Attachment B

Original Agreement with NICE Systems

AGREEMENT FOR SERVICES OF INDEPENDENT CONTRACTOR

THIS AGREEMENT (hereafter "Agreement") is made by and between the County of Santa Barbara, a political subdivision of the State of California (hereafter "COUNTY", "COSB" or "Customer") and NICE Systems, Inc. with an address at 221 River Street 10th Floor Hoboken, NJ 07030 (hereafter "CONTRACTOR" or "NICE" and together with COUNTY, collectively, the "Parties" and each individually a "Party") wherein CONTRACTOR agrees to provide and COUNTY agrees to accept the services specified herein.

WHEREAS, CONTRACTOR represents that it is specially trained, skilled, experienced, and competent to perform the special services required by COUNTY and COUNTY desires to retain the services of CONTRACTOR pursuant to the terms, covenants, and conditions herein set forth;

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein, the parties agree as follows:

1. DESIGNATED REPRESENTATIVE

Onelia Rodriguez at phone number (805) 722-9421 is the representative of COUNTY and will administer this Agreement for and on behalf of COUNTY. Andy Doyle at phone number (801) 502-5608 is the authorized representative for CONTRACTOR. Changes in designated representatives shall be made only after advance written notice to the other Party.

2. NOTICES

Any notice or consent required or permitted to be given under this Agreement shall be given to the respective parties in writing, by personal delivery or facsimile, or with postage prepaid by first class mail, registered or certified mail, or express courier service, as follows:

To COUNTY:

> Aimee Miller, County of Santa Barbara, Information Technology Department, 105 E. Anapamu Street, Room 304, Santa Barbara, CA 93101

To CONTRACTOR: NICE Systems, Inc. 221 River Street , 10th Floor Hoboken NJ 07030

or at such other address or to such other person that the parties may from time to time designate in accordance with this Notices section. If sent by first class mail, notices and consents under this section shall be deemed to be received five (5) days following their deposit in the U.S. mail. This Notices section shall not be construed as meaning that either party agrees to service of process except as required by applicable law.

3. SCOPE OF SERVICES

CONTRACTOR agrees to provide services to COUNTY in accordance with EXHIBIT A attached hereto and incorporated herein by reference.

4. TERM

The term of this Agreement shall commence, and CONTRACTOR shall commence performance hereunder, effective as of the first date that this Agreement is duly executed by all of the parties hereto ("Agreement Effective Date"), and the term of this Agreement shall end, and CONTRACTOR shall complete performance of the Services no later than, the date that is five (5) years after the Initiation Date (defined below), unless earlier terminated in accordance with the provisions of this Agreement ("Term"). The COUNTY may exercise its option to extend the Term for an additional two (2) years

beyond the date that is five (5) years after the Initiation Date by providing written notice to CONTRACTOR of such extension prior to the date that is five years after the Initiation Date; provided, however, that any such extension of the Term must first be approved by the COUNTY Board of Supervisors.

5. COMPENSATION OF CONTRACTOR

In full consideration for CONTRACTOR's services, CONTRACTOR shall be paid for performance under this Agreement in accordance with the terms of EXHIBIT B attached hereto and incorporated herein by reference. Billing shall be made by invoice, which shall include the contract number assigned by COUNTY and which is delivered to the address given in Section 2 (NOTICES), above, following completion of the increments identified on EXHIBIT B. Unless otherwise specified on EXHIBIT B, payment shall be net thirty (30) days from presentation of invoice.

6. INDEPENDENT CONTRACTOR

It is mutually understood and agreed that CONTRACTOR (including any and all of its officers, agents, and employees), shall perform all of its services under this Agreement as an independent contractor as to COUNTY and not as an officer, agent, servant, employee, joint venturer, partner, or associate of COUNTY. Furthermore, COUNTY shall have no right to control, supervise, or direct the manner or method by which CONTRACTOR shall perform its work and function. However, COUNTY shall retain the right to administer this Agreement so as to verify that CONTRACTOR is performing its obligations in accordance with the terms and conditions hereof. CONTRACTOR understands and acknowledges that it shall not be entitled to any of the benefits of a COUNTY employee, including but not limited to vacation, sick leave, administrative leave, health insurance, disability insurance, retirement, unemployment insurance, workers' compensation and protection of tenure. CONTRACTOR shall be solely liable and responsible for providing to, or on behalf of, its employees all legally-required employee benefits. In addition, CONTRACTOR shall be solely responsible and save COUNTY harmless from all matters relating to payment of CONTRACTOR's employees, including compliance with Social Security withholding and all other regulations governing such matters. It is acknowledged that during the term of this Agreement, CONTRACTOR may be providing services to others unrelated to the COUNTY or to this Agreement.

7. STANDARD OF PERFORMANCE

CONTRACTOR represents that it has the skills, expertise, and licenses/permits necessary to perform the services required under this Agreement. Accordingly, CONTRACTOR shall perform all such services in the manner and according to the standards observed by a competent practitioner of the same profession in which CONTRACTOR is engaged. All products of whatsoever nature, which CONTRACTOR delivers to COUNTY pursuant to this Agreement, shall be prepared in a first class and workmanlike manner and shall conform to the standards of quality normally observed by a person practicing in CONTRACTOR's profession. CONTRACTOR shall correct or revise any errors or omissions, at COUNTY'S request without additional compensation Permits and/or licenses shall be obtained and maintained by CONTRACTOR without additional compensation.

EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, (a) NO WARRANTIES, EXPRESS OR IMPLIED, ARE MADE BY NICE TO CUSTOMER, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, WHICH ARE SPECIFICALLY EXCLUDED; AND (b) NICE DOES NOT WARRANT THAT ANY INFORMATION, COMPUTER PROGRAM, NICE'S EFFORTS OR ANY SOFTWARE OR SERVICES PROVIDED BY NICE OR ANY INFRASTRUCTURE PROVIDER WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS, NOR DOES NICE WARRANT THAT THE OPERATION OF THE SOFTWARE OR ACCESS TO THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE

Notwithstanding any provision of this Agreement to the contrary, CONTRACTOR warrants that Services furnished hereunder will comply with the requirements of this Agreement (including without limitation all descriptions, specifications, and drawings identified in the CONTRACTOR's response, and Statement of Work), and:

i.   Services will be performed in accordance with this Agreement; and

ii.   All customer support for Services will be performed with professional care and skill.

8. DEBARMENT AND SUSPENSION

CONTRACTOR certifies to COUNTY that it and its employees and principals are not debarred, suspended, or otherwise excluded from or ineligible for, participation in federal, state, or county government contracts. CONTRACTOR certifies that it shall not contract with a subcontractor that is so debarred or suspended.

9. TAXES

CONTRACTOR shall pay all taxes, levies, duties, and assessments of every nature due in connection with any work under this Agreement and shall make any and all payroll deductions required by law. COUNTY shall not be responsible for paying any taxes on CONTRACTOR's behalf, and should COUNTY be required to do so by state, federal, or local taxing agencies, CONTRACTOR agrees to promptly reimburse COUNTY for the full value of such paid taxes plus interest and penalty, if any. These taxes shall include, but not be limited to, the following: FICA (Social Security), unemployment insurance contributions, income tax, disability insurance, and workers' compensation insurance.

10. CONFLICT OF INTEREST

CONTRACTOR covenants that CONTRACTOR presently has no employment or interest and shall not acquire any employment or interest, direct or indirect, including any interest in any business, property, or source of income, which would conflict in any manner or degree with the performance of services required to be performed under this Agreement. CONTRACTOR further covenants that in the performance of this Agreement, no person having any such interest shall be employed by CONTRACTOR. CONTRACTOR must promptly disclose to COUNTY, in writing, any potential conflict of interest. COUNTY retains the right to waive a conflict of interest disclosed by CONTRACTOR if COUNTY determines it to be immaterial, and such waiver is only effective if provided by COUNTY to CONTRACTOR in writing.

11. OWNERSHIP OF DOCUMENTS AND INTELLECTUAL PROPERTY

COUNTY shall be the owner of the following items incidental to this Agreement upon production, whether or not completed: all data collected, all documents of any type whatsoever, all photos, designs, sound or audiovisual recordings and any material necessary for the practical use of such items, from the time of collection and/or production whether or not performance under this Agreement is completed or terminated prior to completion. CONTRACTOR shall not release any of such items to other parties except after prior written approval of COUNTY.

Unless otherwise specified in Exhibit A, CONTRACTOR hereby assigns to COUNTY all copyright, to all data, documents, reports, photos, designs, sound or audiovisual recordings, prepared or provided by CONTRACTOR pursuant to this Agreement (collectively referred to as "Copyrightable Works and Inventions"). COUNTY shall have the unrestricted authority to copy, adapt, perform, display, publish, disclose, distribute, create derivative works from, and otherwise use in whole or in part, any Copyrightable Works and Inventions. CONTRACTOR agrees to take such actions and execute and deliver such documents as may be reasonably needed to validate, protect and confirm the rights and assignments provided hereunder. CONTRACTOR warrants that any Copyrightable Works and Inventions and other items provided under this Agreement will not infringe upon any intellectual property or proprietary rights of any third party. CONTRACTOR at its own expense shall defend, indemnify, and hold harmless COUNTY against any claim that any Copyrightable Works or Inventions or other items provided by CONTRACTOR hereunder infringe upon intellectual or other proprietary rights of a third party, and CONTRACTOR shall pay any damages, costs, settlement amounts, and fees (including attorneys' fees) that may be incurred by COUNTY in connection with any such claims. This Ownership of Documents and Intellectual Property provision shall survive expiration or termination of this Agreement.

No title or ownership of the Services or Software shall be transferred to COSB by way of this Agreement. NICE has sole right to and ownership of, all intellectual property rights in and to: (a) the Services and Software and Documentation, and all modifications, enhancements, improvements, adaptations, translations; (b) the trademarks, service marks, and trade names associated with the Services or Software; (c) Resulting Information; and (d) all other NICE supplied material developed for use in connection with the Services or Software generally, exclusive of the Content.

COSB shall not: (a) publish, disclose, copy, rent, lease, modify, loan, distribute, sell, resell, transfer, assign, alter or create derivative works based on the Services or Software or any part thereof; (b) reverse engineer, decompile, translate, adapt, or disassemble the Services or Software including to: (i) build or create a competitive product or service, and (ii) build or create a product or services using similar ideas, features, functions or graphics of the Services or Software, nor shall COSB attempt to create the source code from the object code for the Software; (c) permit any third party to access the Services or Software except as expressly permitted herein or under an SOW; or (d) create any unauthorized Internet "links" to the Cloud Services or "frame" or "mirror" any content of the Cloud Services. The foregoing restrictions shall not in any way restrict the COUNTY's rights with respect to extraction and transfer of all Content in accordance with Section 19.D., below.

12. NO PUBLICITY OR ENDORSEMENT

CONTRACTOR shall not use COUNTY's name or logo or any variation of such name or logo in any publicity, advertising or promotional materials. CONTRACTOR shall not use COUNTY's name or logo in any manner that would give the appearance that the COUNTY is endorsing CONTRACTOR. CONTRACTOR shall not in any way contract on behalf of or in the name of COUNTY. CONTRACTOR shall not release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the COUNTY or its projects, without obtaining the prior written approval of COUNTY.

13. COUNTY PROPERTY AND INFORMATION

All of COUNTY's property, documents, and information provided for CONTRACTOR's use in connection with the services shall remain COUNTY's property, and CONTRACTOR shall return any such items whenever requested by COUNTY and whenever required according to the Termination section of this Agreement. CONTRACTOR may use such items only in connection with providing the services. CONTRACTOR shall not disseminate any COUNTY property, documents, or information without COUNTY's prior written consent.

14. RECORDS, AUDIT, AND REVIEW

CONTRACTOR shall keep such business records pursuant to this Agreement as would be kept by a reasonably prudent practitioner of CONTRACTOR's profession and shall maintain such records for at least four (4) years following the termination of this Agreement. All accounting records shall be kept in accordance with generally accepted accounting principles. COUNTY shall have the right to audit and review all such documents and records at any time during CONTRACTOR's regular business hours or upon reasonable notice. In addition, if this Agreement exceeds ten thousand dollars ($10,000.00), CONTRACTOR shall be subject to the examination and audit of the California State Auditor, at the request of the COUNTY or as part of any audit of the COUNTY, for a period of three (3) years after final payment under the Agreement (Cal. Govt. Code Section 8546.7). CONTRACTOR shall participate in any audits and reviews, whether by COUNTY or the State, at no charge to COUNTY.

If federal, state or COUNTY audit exceptions are made relating to this Agreement, CONTRACTOR shall reimburse all costs incurred by federal, state, and/or COUNTY governments associated with defending against the audit exceptions or performing any audits or follow-up audits, including but not limited to: audit fees, court costs, attorneys' fees based upon a reasonable hourly amount for attorneys in the community, travel costs, penalty assessments and all other costs of whatever nature up to a limit of $12,000 in the aggregate. Immediately upon notification from COUNTY, CONTRACTOR shall reimburse the amount of the audit exceptions and any other related

costs directly to COUNTY as specified by COUNTY in the notification.

15. INDEMNIFICATION. LIMITATION OF LIABILITY AND INSURANCE

CONTRACTOR agrees to comply at all times during the Term, without limitation, with the indemnification and insurance provisions as set forth in EXHIBIT C attached hereto and incorporated herein by reference.

15.1   SUBJECT TO SECTION 15.2 BELOW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR: (a) ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OR LOSSES, INCLUDING LOSS OF USE, COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY, LOST REVENUE AND/OR PROFITS, SUSTAINED OR INCURRED REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT OR OTHERWISE; OR (b) DIRECT DAMAGES IN EXCESS OF TWO (2) TIMES THE AMOUNTS PAYABLE UNDER THIS Agreement, PURCHASE ORDER, OR STATEMENT OF WORK UNDER WHICH SUCH LIABILITY AROSE.

15.2   The limitations in Section 15.1 above shall not apply to: (a) damages occasioned by the of either Party, including by such party's Representatives, of its obligations of confidentiality; (b) indemnification obligations under Section 15 above; or (c) matters that cannot be excluded or limited by applicable law. (d) CONTRACTOR shall also indemnify for damages caused by the Gross Negligence of the CONTRACTOR in the performance of this agreement. Gross Negligence is defined as a severe deviation from the standard care and diligence expected, including reckless disregard for user data safety or confidentiality, legal non-compliance, failure in security protocols and neglect of system performance and availability.

NICE Indemnification of COSB. CONTRACTOR shall indemnify, defend, and hold harmless COUNTY from and against any losses resulting from or arising out of a third party claim ("Claim") against COUNTY to the extent that such Claim alleges the infringement of such third party's U.S. patent or copyright by the Services or Software. The foregoing indemnity shall not apply if the infringement arises out of: (a) specifications or designs furnished by COUNTY and implemented by CONTRACTOR at COUNTY's request; (b) the Services or Software being modified by, combined with, added to, interconnected with or used with any equipment, apparatus, device, data, software or service by COUNTY that is not supplied or approved by NICE in writing; (c) the modification to Services or Software by COUNTY; or (d) use of Services or Software other than in accordance with its Documentation. Documentation in this instance means the applicable specifications and user documentation accompanying the Services or Software and is accessible within the Solution, by clicking the Help (?) icon.

If a Claim for which COUNTY is entitled to be indemnified under Section 15 above has occurred, or in CONTRACTOR's opinion is likely to occur, CONTRACTOR shall, at CONTRACTOR's expense, do one of the following: (a) procure for COUNTY the right to continue using the affected Services or Software at no additional cost to COUNTY; (b) replace with functionally equivalent non-infringing alternates or modify the relevant Services or Software so that it becomes non-infringing but functionally equivalent; (c) accept the return of the affected Software, and refund to COUNTY the fees for the affected Software amortized by an equal annual amount over a three (3) year period beginning from the date of shipment of the affected Software; or (d) cease providing the Services and refund all prepaid fees applicable to the period after the Services has ceased .   The collective obligations of CONTRACTOR pursuant to Section 15 state the sole and exclusive liability of CONTRACTOR, and COUNTY's sole and exclusive remedy, with respect to intellectual property infringement or misappropriation

16. NONDISCRIMINATION

COUNTY hereby notifies CONTRACTOR that COUNTY's Unlawful Discrimination Ordinance (Article XIII of Chapter 2 of the Santa Barbara County Code) applies to this Agreement and is incorporated herein by this reference with the same force and effect as if the ordinance were specifically set out herein and CONTRACTOR agrees to comply with said ordinance.

17. NONEXCLUSIVE AGREEMENT

CONTRACTOR understands that this is not an exclusive Agreement and that COUNTY shall have the right to

negotiate with and enter into contracts with others providing the same or similar services as those provided by CONTRACTOR as the COUNTY desires.

18. NON-ASSIGNMENT

CONTRACTOR shall not assign, transfer or subcontract this Agreement or any of its rights or obligations under this Agreement without the prior written consent of COUNTY and any attempt to so assign, subcontract or transfer without such consent shall be void and without legal effect and shall constitute grounds for termination.

19. TERMINATION

A. By COUNTY. COUNTY may, by written notice to CONTRACTOR, terminate this Agreement in whole or in part at any time, whether for nonappropriation of funds, or because of the failure of CONTRACTOR to fulfill the obligations herein.

1. For Non-appropriation of Funds. Notwithstanding any other provision of this Agreement, in the event that no funds or insufficient funds are appropriated or budgeted by federal, state or COUNTY governments, or funds are not otherwise available for payments in the fiscal year(s) covered by the term of this Agreement, then COUNTY will notify CONTRACTOR of such occurrence and COUNTY may terminate or suspend this Agreement in whole or in part, with or without a prior notice period. Subsequent to termination of this Agreement under this provision, COUNTY shall have no obligation to make payments with regard to the remainder of the term.

2. For Cause. Should CONTRACTOR default in the performance of this Agreement or materially breach any of its provisions, and, (unless such default is not reasonable capable of being subject to cure) and such failure is not remedied by CONTRACTOR within thirty (30) days of written notice to CONTRACTOR of such default in the manner specified by COUNTY, COUNTY may, in COUNTY's sole discretion, terminate or suspend this Agreement in whole or in part upon written notice. Upon receipt of such notice, CONTRACTOR shall immediately discontinue all services hereunder (unless such notice directs otherwise) and notify COUNTY as to the status of CONTRACTOR's performance hereunder. The date of termination shall be the date such notice is received by CONTRACTOR, unless such notice directs otherwise.

3. If County terminates this Agreement during the first 12 months after go-live, other than in accordance with Sections 19.A.1 or 19.A.2, above, a termination fee equal to the balance of the amount that would be owed for the rest of that 12-month period would apply (but the County could immediately initiate data porting/transfer and direct wrapping up of services).
   - Thereafter, the County may terminate without cause by providing a minimum of 90 days' notice to NICE (and the County could immediately initiate data porting/transfer and direct wrapping up of services).

B. By CONTRACTOR. Should COUNTY fail to pay CONTRACTOR all or any part of the payment set forth in EXHIBIT B, CONTRACTOR may, at CONTRACTOR's option terminate this Agreement if such failure is not remedied by COUNTY within thirty (30) days of written notice to COUNTY of such late payment.

C. Upon termination, CONTRACTOR shall deliver to COUNTY all data, estimates, graphs, summaries, reports, and all other property, records, documents or papers as may have been accumulated or produced by CONTRACTOR in performing this Agreement, whether completed or in process, except such items as COUNTY may, by written permission, permit CONTRACTOR to retain. Notwithstanding any other payment provision of this Agreement, COUNTY shall pay CONTRACTOR for satisfactory services performed to the date of termination to include a prorated amount of compensation due hereunder less payments, if any,

previously made. In no event shall CONTRACTOR be paid an amount in excess of the full price under this Agreement nor for profit on unperformed portions of service. CONTRACTOR shall furnish to COUNTY such financial information as in the judgment of COUNTY is necessary to determine the reasonable value of the services rendered by CONTRACTOR. In the event of a dispute as to the reasonable value of the services rendered by CONTRACTOR, the decision of COUNTY shall be final. The foregoing is cumulative and shall not affect any right or remedy which COUNTY may have in law or equity.

D. Transition Period.

1) For the period of thirty (30) days after expiration or notice of termination of this Agreement ("Transition Period"), CONTRACTOR shall provide COUNTY the tools necessary to extract all Content in a structured, commonly used and transferable format reasonably acceptable to County at no additional charge ("Content Transition"). The parties will enter into a mutually agreeable SOW to describe any additional Services required to transition to a third party designed by COUNTY , at an hourly rate of $300

2) During the Transition Period, Services and Content access shall continue to be made available to the COUNTY without alteration.

3) CONTRACTOR agrees to compensate COUNTY for damages or losses COUNTY incurs as a result of CONTRACTOR's failure to comply with this Section 19.D. in accordance with Exhibit C.

4) Unless otherwise directed in writing duly executed by COUNTY, CONTRACTOR shall permanently destroy or render inaccessible any portion of the Content in CONTRACTOR's and/or subcontractor(s)'s possession, custody, or control following the later of the expiration of the Transition Period or the completion of the Content Transition. Upon written request by the County after the expiration of the later of the expiration of the Transition Period or the completion of the Content Transition, CONTRACTOR shall deliver to COUNTY a written statement duly executed by CONTRACTOR confirming the destruction of the Content. If no written request is received by the CONTRACTOR within 12 months of the completion of the Transition Period, CONTRACTOR will delete all COUNTY data.

20. SECTION HEADINGS

The headings of the several sections, and any Table of Contents appended hereto, shall be solely for convenience of reference and shall not affect the meaning, construction or effect hereof.

21. SEVERABILITY

If any one or more of the provisions contained herein shall for any reason be held to be invalid, illegal or unenforceable in any respect, then such provision or provisions shall be deemed severable from the remaining provisions hereof, and such invalidity, illegality or unenforceability shall not affect any other provision hereof, and this Agreement shall be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

22. REMEDIES NOT EXCLUSIVE

No remedy herein conferred upon or reserved to COUNTY is intended to be exclusive of any other remedy or remedies, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy given hereunder or now or hereafter existing at law or in equity or otherwise.

23. NO WAIVER OF DEFAULT

No delay or omission of COUNTY to exercise any right or power arising upon the occurrence of any event of default shall impair any such right or power or shall be construed to be a waiver of any such default or an acquiescence therein; and every power and remedy given by this Agreement to COUNTY shall be exercised from time to time and as often as may be deemed expedient in the sole discretion of COUNTY.

24. ENTIRE AGREEMENT AND AMENDMENT

In conjunction with the matters considered herein, this Agreement contains the entire understanding and agreement of the parties and there have been no promises, representations, agreements, warranties or undertakings by any of the parties, either oral or written, of any character or nature hereafter binding except as set forth herein. This Agreement may be altered, amended or modified only by an instrument in writing, executed by the parties to this Agreement and by no other means. Each party waives their future right to claim, contest or assert that this Agreement was modified, canceled, superseded, or changed by any oral agreements, course of conduct, waiver or estoppel.

25. SUCCESSORS AND ASSIGNS

All representations, covenants and warranties set forth in this Agreement, by or on behalf of, or for the benefit of any or all of the parties hereto, shall be binding upon and inure to the benefit of such party, its successors and assigns.

26. COMPLIANCE WITH LAW

CONTRACTOR shall, at its sole cost and expense, comply with all County, State and Federal ordinances and statutes now in force or which may hereafter be in force with regard to this Agreement. The judgment of any court of competent jurisdiction, or the admission of CONTRACTOR in any action or proceeding against CONTRACTOR, whether COUNTY is a party thereto or not, that CONTRACTOR has violated any such ordinance or statute, shall be conclusive of that fact as between CONTRACTOR and COUNTY.

27. CALIFORNIA LAW AND JURISDICTION

This Agreement shall be governed by the laws of the State of California. Any litigation regarding this Agreement or its contents shall be filed in the County of Santa Barbara, if in state court, or in the federal district court nearest to Santa Barbara County, if in federal court.

28. EXECUTION OF COUNTERPARTS

This Agreement may be executed in any number of counterparts and each of such counterparts shall for all purposes be deemed to be an original; and all such counterparts, or as many of them as the parties shall preserve undestroyed, shall together constitute one and the same instrument.

29. AUTHORITY

All signatories and parties to this Agreement warrant and represent that they have the power and authority to enter into this Agreement in the names, titles and capacities herein stated and on behalf of any entities, persons, or firms represented or purported to be represented by such entity(ies), person(s), or firm(s) and that all formal requirements necessary or required by any state and/or federal law in order to enter into this Agreement have been fully complied with. Furthermore, by entering into this Agreement, CONTRACTOR hereby warrants that it shall not have breached the terms or conditions of any other contract or agreement to which CONTRACTOR is obligated, which breach would have a material effect hereon.

30. SURVIVAL

All provisions of this Agreement which by their nature are intended to survive the termination or expiration of this Agreement shall survive such termination or expiration.

31. BUSINESS ASSOCIATE

The parties agree to the terms and conditions set forth in Exhibit D - HIPAA Business Associate Agreement (BAA), attached hereto and incorporated herein by reference.

32. <u>PRECEDENCE</u>

Any conflict or inconsistency between the provisions contained in the foregoing numbered Sections 1 through 31 of this Agreement and this Section 32] (collectively, the "Numbered Sections"), and the provisions contained in the Exhibits attached hereto, shall be resolved by giving precedence in the following order:

A. Exhibit C

B. Exhibit D

C. Exhibit E

D. Numbered Sections

E. Exhibit B

F. Exhibit A

G. Any other exhibits , attachments, and documents incorporated by reference

H. CONTRACTOR Terms (Defined below)

For purposes of this Agreement, "CONTRACTOR Terms" shall mean any of CONTRACTOR's standard terms and conditions, including terms, conditions, or other documents referenced via hyperlink or web address.

//
//
//
//

(Rest of Page Intentionally Left Blank)

//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//

Agreement for Services of Independent Contractor between the County of Santa Barbara and NICE Systems, Inc.

IN WITNESS WHEREOF, the parties have executed this Agreement to be effective as of the first date executed by all of the parties hereto.

ATTEST:

Mona Miyasato
County Executive Officer
Clerk of the Board

By: _____
Deputy Clerk

COUNTY OF SANTA BARBARA:

By: _____
Steve Lavagnino, Chair
Board of Supervisors

Date: 12-17-24

RECOMMENDED FOR APPROVAL:

Chris Chirgwin, CIO
Information Technology

DocuSigned by:
By: *Chris Chirgwin*
D97209A7A68A4A0...
Department Head

CONTRACTOR:

NICE Systems, LLC

DocuSigned by:
D4212C6E49AB4B1...

DocuSigned by:
By: *Ashley Goodwin*
9B18BA4F7E3349E...
Authorized Representative

Name: John Rennie   Ashley Goodwin

Title: General Manager, Public Safety, Americas

APPROVED AS TO FORM:

Rachel Van Mullem
County Counsel

Signed by:
By: *Lauren Wideman*
8E464D822C84458
Deputy County Counsel

APPROVED AS TO ACCOUNTING FORM:

Betsy M. Schaffer, CPA
Auditor-Controller

DocuSigned by:
By: _____
8BAAEA15901943E
Deputy

APPROVED AS TO FORM:

Risk Management

By: Greg Milligan
Signed by:
Greg Milligan
05E555E00269466
Risk Management

10

EXHIBIT A - STATEMENT OF WORK

DEFINITIONS

"Case" means the following for each COUNTY Department:

Sheriff's Office: A new Case is triggered by assignment of a case number in the Computer Aided Dispatch (CAD) system. One Case is one case number. A Case may be comprised of one call for service or multiple calls for service. Evidence will not be pulled into the DEMS without an association with a case number, so some calls for service will not result in the generation of a new Case. A Case may also be created by a manual trigger in Enterprise (Sheriff Office's Record Management System) or manually created within the NICE system.

District Attorney's Office: A new Case is triggered by a referral from law enforcement to District Attorney's Office. A Case is created when the case is received from law enforcement and logged in by District Attorney staff. If charges are filed, the case is considered active. If the case is rejected the case is considered inactive and can be archived.

Public Defender's Office: A new Case is triggered by a referral from District Attorney's Office to Public Defender's Office, or by a manual trigger in eDefender (Public Defender's Office Case Management System) to create a case. One case will be created for each defendant.

* If mutually agreed upon in writing, parties to this agreement may amend these definitions during the planning phase of implementation, or within a reasonable period of time.

"Support **Case**" means a request for support assistance submitted by COSB via the designated support channels outlined in Table A-1 of this Exhibit. Support Case severity levels are classified based upon the definitions outlined in Table A-2 of this Exhibit.

"**Cloud Service(s)**" means a subscription-based service consisting of the ability to use, and receive support in connection with, software in a hosting environment as described in this Agreement.

"**Commencement Date**" means the first day of the calendar month following the Initiation Date.

"**Content**" means the data provided by COSB or authorized by Customers in connection with the Software or Service.

"**Documentation**" means the applicable specifications and user documentation accompanying Software or Services provided to COSB by NICE.

"**Production**" means an operational environment deployed for commercial use (excluding, but not limited to, any test, development, staging, or lab environment).

"**Resulting Information**" means data created by, or resulting from, the use of the Services, including analyses, statistics, reports, and aggregations, all of which shall be considered NICE Confidential Information excluding the Content. For the avoidance of doubt, the term Resulting Information does not include personally identifiable information, such that there is no reasonable basis on which any individual, or COSB itself, could be identified by the Resulting Information. The foregoing shall not in any way restrict the County's rights with respect to extraction and transfer of all Content in accordance with Section 19, above.

"**Availability**" means the monthly availability of a Cloud Service in Production multiplied by the applicable service levels less any Excusable Downtime.

"**Excusable Downtime**" means and includes: (a) maintenance Services performed during the Maintenance Windows, as defined in Exhibit A; (b) maintenance Services performed on an emergency basis to avoid harm to NICE, COSB, or the Cloud Services; (c) any time spent by NICE in its performance of any additional Services requested or agreed to by COSB; (d) COSB-caused outages or disruptions; (e) outages or disruptions caused by, and in no way caused by or attributable to any act or omission by or on behalf of NICE, any of the following that are not provided or controlled by NICE: (i) software, infrastructure, databases, operator error, or hardware not provided or controlled by NICE, (ii) disruptions attributable to Force Majeure Events, or (iii) configuration changes not made by NICE;

"Initiation Date" means the date corresponding to the earlier of: (a) the date of NICE's notice to COSB that the Cloud Services are available to COSB; and (b) the date of COSB's use of the Cloud Services in Production; or (c) Fifteen (15) months following the Effective Agreement Date.
"Minimum Commitment" means the minimum committed amount, whether expressed in units or currency, of Cloud Services as specified in this Agreement.
"Named Agent(s)" means uniquely identified COSB employees, contractors, agents, or traders (each as applicable) who will have one or more interactions that are processed, or were available for processing, by the Cloud Services (not the maximum concurrent user count), with the identities of such persons being capable of variation, such that new agents may be added and old agents may be removed or terminated.
"Service(s)" means the Cloud Services, Professional Services, or other services to be provided by NICE hereunder.
"Variance" means the actual number of licenses, or additional Network Connectivity, used by COSB in excess of the Minimum Commitment.
"Minimum ARC" means the minimum ARC amount that COSB is required to pay for the Cloud Services, for each annual period of the Subscription Term (defined below).
"Minimum MRC" or **"Minimum Technology MRC"** means the minimum monthly MRC amount that COSB is required to pay for the Cloud Services), for the duration of the Subscription Term.
"MRC" means monthly recurring charges.
"Agreement Effective Date" means the first date this Agreement is fully executed by each of the Parties.

SCOPE OF SERVICES

Contractor shall execute the following Tasks as part of this Statement of Work (SOW):

Task 1. Project Management

Contractor shall provide ongoing project management including weekly project plan updates, weekly status reports on a project dashboard that are kept current, and weekly status meetings. Contractor shall prepare a baseline risk management plan and update the plan regularly (biweekly) over the course of the project.

Contractor shall provide project management tools, processes, and techniques to guide the project, measure and monitor progress, identify, and mitigate risks, facilitate completion of tasks, ensure quality, and accommodate and manage changes in scope. Contractor shall provide County access to all Project Management documents. All Project Management documents (e.g., Project Management Plan, Project Schedule, Work Breakdown Structure, etc.) shall be compatible with Microsoft 2010 or later software products.

Contractor shall provide the following project management activities:

- Development and Management of a Project Plan
- Project Document Management
- Resource Management (County and Contractor Staffing)
- Schedule Management
- Communications Management (Status Reporting/Stakeholder Agency/Department Communications)
- Quality Assurance, including Quality Gate Reviews
- Risk and Issue Management and Escalation
- Scope and Requirements Management, including Requirements Traceability
- Cost Management
- Change Request Management
- Performance Management (Project and System)

Contractor shall provide the following Project Management sub-tasks and deliverables:

Task 1: Project Management SubTasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
1.1	**Project Kickoff**	Contractor shall, at minimum, develop a Project Kickoff Presentation to deliver and present to DEMS Stakeholder agencies/departments in a Formal Kickoff Meeting to initiate the project.	A **Project Kickoff Presentation** shall include information to provide the stakeholder agencies/departments an understanding of the process, roles, and responsibilities: • Understanding of the roles of various project stakeholders including the sponsor, Project Management Team, Contractor Project Team, Business staff, IT staff, and any other key project team members • Identification of key stakeholders to be contacted to review and validate information relative to all steps of the project • Understanding the process to provide input to the strategic and tactical reports on a regular basis • Understanding of project performance measurements and critical success factors Any decisions or agreements from the kickoff meeting will be documented by Contractor and submitted to the overall project team for review and acceptance. **This Deliverable includes a Deliverable Expectation Document (DED).**

1.2	Project Management Planning	Contractor shall plan the activities to be conducted in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. Working with the County Project Manager, Contractor shall set up roles, responsibilities, record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.	A **Project Plan and Schedule** shall conform with IEEE/ISO/IEC 16326-2009 Systems and Software Engineering--Life Cycle Processes-- Project Management.
			
			The deliverable shall minimally include the following components:
			· Project Objectives
			· Project Scope Definition
			· Project Schedule / Work Breakdown Structure
			· Project Resources
			  — Contractor's Project Team (e.g., organization, names, role definition and organization reporting lines)
			  — Project roles and responsibilities
			· Resource Management Plan (Staffing Plan)
			· Quality Management Plan
			· Risk Management Plan and Risk Register
			· Scope and Requirements Management Plan
			· Release Management Plan
			· Communications Plan
			· Risk Assessment Baseline
			· Project Schedule / Work Breakdown Structure
			The County acknowledges that some portions of the PMP may require a standalone plan.
			
			This Deliverable shall include a DED.

1.3	Project Status Reporting	Contractor shall establish a project control and reporting system to provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans. Contractor shall advise the County of progress in meeting goals and schedules contained in the work plans. This shall be initiated one week after Contract effective date and applied weekly thereafter and shall consist of weekly progress meetings attended by Contractor and the County. These may include walkthroughs of selected deliverables as requested by the County staff.	Weekly written Status Reports, provided by Contractor to the County one (1) working day before each weekly meeting, and containing items to be discussed at the meeting, including: · Tasks completed for the period · Tasks planned but not completed for the period · Tasks planned for next period · Upcoming County resource needs (90-day forecast) · Issues · Risks · Decision requests

| 1.4 | Project Close- out | Contractor shall provide Contract close-out plans and manage project close-out activities in accordance with the plan. | A **Contract Close-out Plan** Describing Contractor's approach to completing the required activities necessary to close the Contract, minimally including updating and transferring all System documentation to the County Project Team, performing formal Contract closure, and transitioning all System responsibilities over to County Project Team.

This Deliverable shall include a DED. |

Deliverable Expectations Document (DED): NICE

Project Management Plan

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: Project Management Plan
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>
Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose: NICE shall plan the activities to be conducted in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. NICE shall establish a project control and reporting system to provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans. Collaborating with COSB Project Manager, NICE shall set up roles, responsibilities, record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

Deliverable Scope / Content Expectations:

NICE will provide full project management documentation. The deliverables will include:

PROJECT KICKOFF

- Understanding of the roles of various project stakeholders including the sponsor, Project Management Team, Contractor Project Team, Business staff, IT staff, and any other key project team members
- Identification of key stakeholders to be contacted to review and validate information relative to all steps of the project throughout the SDLC
- Understanding the process to provide input to the strategic and tactical reports on a regular basis • Understanding of project performance measurements and critical success factors

PROJECT MANAGEMENT PLANNING

- Project Objectives
- Project Scope Definition
- Project Schedule / Work Breakdown Structure
- Project Resources
  — Contractor's Project Team (e.g., organization, names, role definition and organization reporting lines)
  — Project roles and responsibilities
- Resource Management Plan (Staffing Plan)
- Quality Management Plan
- Risk Management   Plan and Risk Register
- Scope and Requirements Management Plan
- Release Management Plan
- Communications Plan
- Risk Assessment Baseline
- Project Schedule / Work Breakdown Structure **PROJECT CLOSE-OUT**
- Contract Close-out Plan **Sample Enclosed:**

Preliminary Project Plan

Enclosed in MS Project Format. It follows the standardized planning method that is used with all customers deploying NICE DEMS.

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** The document is in full compliance with the approved DED and required content areas documented above.
	Rework Required: The document in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.
	Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

Introduction to NICE Project Charter & Methodology

NICE shall plan the activities to be carried out in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. NICE shall establish a project control and reporting system to provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans. Working with the COSB Project Manager, NICE shall set up roles, responsibilities, recordkeeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

NICE will follow project management methodologies consistent with the standards and guidelines of the Project Management Institute (PMI) Project Management Methodologies

stated in the Project Management Body of Knowledge (PMBOK) or similar industry standard.

NICE shall provide on-going project management including regular (weekly) project plan updates, weekly status reports and weekly status meetings. NICE shall prepare a baseline risk management plan and update the plan regularly (bi-weekly) over the course of the project.

NICE shall provide the following project management activities:

- Development and Management of a Project Management Plan (PMP)
- Resource Management (COSB and NICE Staffing)
- Schedule Management
- Communications Management (Status Reporting/Stakeholder Communications)
- Quality Assurance, including Quality Gate Reviews
- Risk and Issue Management and Escalation
- Scope and Requirements Management, including Requirements Traceability
- Cost Management
- Change Request Management
- Performance Management (Project and System)

The NICE DEMS Project Management Plan for COSB includes the following components and subsidiary plans (at a minimum): • Project Objectives

- Project Scope definition
- Project Resources/Resource Management
- Quality Management Plan
- Risk Management Plan/Risk Register
- Scope and requirements Management Plan (requirements traceability matrix)
- Release Management Plan
- Communication Plan
- Project Schedule/work breakdown schedule

Project Overview – Project Objectives

NICE Statement of Work ("SOW") sets forth the professional services (collectively, the "Services") to be provided to COSB ("Customer"), to implement a new **NICE DEMS Digital Evidence Management and Investigations solution**.

This SOW is an arrangement for NICE and COSB to complete the scope of deliverables defined herein, after which NICE believes COSB can confidently perform its business activities with/in the new system.

The purpose of this document, and all its associated documents, is to describe the implementation of a solution which shall fully meet or exceed all the requirements as stated and maintained within the stated and agreed to 'requirements'.

NICE PROJECT TEAM – KEY PERSONNEL, ROLES, AND RESPONSIBILITIES

The following NICE personnel, as specified in greater detail in the Qualifications table set forth further below, shall be assigned to this NICE DEMS project:

- LeslieAnn A Nicholas – Project Manager
- Stephen Benwell – Senior Architect (Technical Lead)
- Danielle Cummins – Software Integrations Manager
- John Lally – Digital Evidence Management Subject Matter Expert

The minimum requirements for the NICE Project Team Key Personnel must meet are as follows:

1. **Project Manager**

LeslieAnn A Nicholas meets the below qualifications and will be filling the role of Project Manager for this Implementation.

Experience	Minimum	Ideal
Experience directing and overseeing all phases of a software integration project including, but not limited to, projects involving developing multiple business views, integration with third party software (i.e. e-mail, calendaring, etc.), interfacing with other systems and databases and training, customer service	5 Years	8 Years
Worked as the Project Manager on comparable projects	5 Years	10 Years
Project experience, in the PM role for county, state, or federal government systems	N/A	3 Years
Project Management Institute (PMI) Project Management Professional (PMP) Certification	Yes	N/A
Education: Baccalaureate from an accredited college/university. Additional qualifying experience may be substituted for the required education on a year-for-year basis.	Yes	N/A

2. **Senior Architect (Technical Lead)**

Stephen Benwell meets the below qualifications and will be filling the role of Senior Architect for this Implementation.

Experience	Minimum	Ideal
Experience in the role of Senior Architect (Technical Lead) as defined in Section V. Project Team	3 Years	5 Years
Senior Architect experience, defined as performing tasks defined in the Project Management Body of Knowledge, for a similar system integration project(s)	2 Years	3 Years
Worked as the Senior Architect in the design and development of comparable projects deployed to production for end users, which are equal or greater than listed in the project requirements.	2 Years	3 Years
Configuration design experience with the hardware/software defined by the Contractor	2 Years	5 Years
Implementation and tuning experience with the solution proposed by the Contractor	2 Years	5 Years
Database design experience with the solution proposed by the Contractor	2 Years	5 Years
Customization and configuration experience with the solution proposed by the Contractor	2 Years	5 Years
Project experience, in the Senior Technical Architect role for county, state or federal government systems	N/A	2 Years
Education: Baccalaureate from an accredited college/university. Additional	Yes	N/A

qualifying experience may be substituted for the required education on a year-for-year basis.

3. <u>Software Integration Manager</u>

Danielle Cummins meets the below qualifications and will be filling the role of Software Integration Manager for this Implementation.

Experience	Minimum	Ideal
Experience in the role of Software Integration Manager as defined in Section V. Project Team	3 Years	5 Years
Worked as the Software Integration Manager in the design and development of comparable projects deployed to production for end users, which are equal or greater than listed in the project requirements.	2 Years	3 Years
Experience leading development teams of a system integration project	2 Years	6 Years
Implementation and tuning experience with the solution proposed by the Contractor	2 Years	6 Years
Customization and configuration experience with the solution proposed by the Contractor	2 Years	6 Years
Project experience, as the Software Integration Manager for county, state or federal government systems	N/A	2 Years
Education: Baccalaureate from an accredited college/university. Additional qualifying experience may be substituted for the required education on a year-for-year basis.	Yes	N/A

4. <u>*Digital Evidence Management Subject Matter Expert*</u>

John Lally meets the below qualifications and will be filling the role of DEMS SME for this Implementation.

Experience	Minimum	Ideal
Operational experience in multiple roles within a digital evidence management and office management setting	5 Years	10 Years
Experience in the use of digital evidence management systems in a large volume criminal justice system with multiple office locations	2 Years	3 Years
Experience in a county, state or federal government criminal justice system.	N/A	Yes
Education: Baccalaureate from an accredited college/university. Additional qualifying experience may be substituted for the required education on a year-for-year basis.	Yes	N/A

In addition, NICE personnel will conduct the following:

Project Manager	- Plans and monitors project activities and action items per the project contractual obligations. - Communicates progress to COSB and NICE Systems management. - Identifies and mitigates risk. Resolves potential risks and ensures that tasks are done on time and as committed. - Schedules and coordinates all in-house activities at NICE HQ. This includes R&D, Marketing, Sales, Field Services, Training and Technical Writing.

	• Works closely with COSB and the NICE local team.
	• Assures that quality control activities are implemented as planned and agreed in line with company policy.
	• Plans and tracks the project budget.
Solution Engineer, Professional Services	• Provides technical services for all activities connected to project deployment. This includes staging, acceptance testing, installation, integration, assimilation, and transition.
Education Specialist and Consultant	• Prepares customized training plan that reflects specific needs of COSB • Prepares associated resources required to conduct the training • Delivers training to users and administrators appointed by COSB • Performs associated quality control • Serves in a system application consulting role, guides COSB in use of the solution in a manner that targets specific needs and requirements as communicated by COSB and uncovered in the initial status analysis

NICE shall provide and use management tools, processes, and techniques that shall be employed to guide the project, to measure and monitor progress, to identify and mitigate risks, facilitate completion of tasks, ensure quality, and to accommodate and manage changes in scope.

NICE shall conduct workshops with COSB during project initiation and planning to determine the best solution design and deployment approach for rolling out the NICE DEMS solution, including possible phasing strategies, site specific considerations, as well as benefits and risks of strategy alternatives.

NICE shall apply industry best practices and work with COSB to determine recommendations for managing organizational change required for the solution to meet the project objectives. Such recommendations shall be developed considering business impact on each of the key stakeholder groups.

NICE shall manage requirements as defined within the 'Requirements Management Plan' defined within the detailed Project Management Plan (PMP). NICE shall review the requirements included in this scope and work with COSB to confirm, update and finalize the list of requirements/deliverables to be provided by the DEMS solution; inputs to this review shall include the requirements included in this scope and capabilities of the out-of-box DEMS product. NICE shall ensure that all confirmed functional and technical requirements are provided by the DEMS solution and document how such requirements are realized in a 'Requirements Traceability Matrix'. NICE shall update the matrix as the project proceeds.

The deliverable processes are outlined below unless otherwise mutually agreed upon between NICE and COSB in a 'Deliverable Expectations Document' (DED):

• NICE shall deliver all agreed items to COSB by the delivery date as established in the Project Management Plan. If NICE is unable to meet the established delivery date, it must provide COSB with written notice at least one (1) week prior to the delivery date. Such notice must specify the proposed new delivery date.

• Unless otherwise noted, COSB shall review the deliverable within ten (10) Business Days of receipt of the Document Deliverable ("Acceptance Review Period") and provide a written response which either:

— Indicates that COSB has (accepted) the deliverable; or

— Documents the COSB's comments on where and how the deliverable fails to conform to the relevant specifications.

21

Should COSB not accept the deliverable, or if no changes or comments are requested within the Acceptance Review Period, the NICE Project Manager will escalate the delay in deliverable acceptance to COSB's Project Manager for follow-up and action. The NICE Project Manager shall assess any potential delays and provide this information as a part of the escalation process.

- If the Review Record indicates that COSB has not accepted the deliverable, NICE shall, within three (3) Business Days from the time COSB delivers the Review Record, respond in writing addressing the points raised by COSB in the Review Record and, as appropriate, amend the deliverable.

- COSB shall, within ten (10) Business Days of receiving written response to the points raised in the Review Record and/or the amended deliverable, notify NICE in writing that COSB considers that:

  — All the points raised have been addressed and/or amendments have been incorporated into the deliverable and that COSB accepts the deliverable; or

  — Not all the points raised have been addressed and/or not all the amendments have been incorporated into the deliverable, in which case COSB shall provide an update to the original request, documenting its further comments on the deliverable.

- The parties shall repeat the above processes until COSB accepts the deliverable per the acceptance process for deliverables.

NICE shall prepare and submit a Deliverable Identification Document (DID) for each deliverable identified within this SOW. The DID shall include deliverable purpose, approach/key activities, table of contents, and acceptance criteria. NICE shall provide the DID to COSB for approval prior to providing the subject deliverable. Upon receipt of DID, COSB will have ten (10) business days to review and either accept and approve the DID, or request revisions.

Project Scope Overview

This SOW is for the implementation of NICE DEMS SaaS instance for COSB. The NICE DEMS solution scope will encompass the following services, platform functionality and user capabilities.

- NICE shall develop, install, implement and maintain a Digital Evidence Management System (DEMS) solution for COSB.

- The NICE DEMS shall provide a common infrastructure and an enterprise Countywide platform for digital evidence management.

- The NICE DEMS will integrate with existing content management solutions and/or digital evidence management solutions to fully support the lifecycle of digital content (e.g., video, audio, images, and digital files) which may be submitted to courts as digital evidence.

- The NICE DEMS shall store, manage, and protect all data regardless of file content or format. This includes digital evidence captured by Body Worn Cameras (BWC), patrol cameras, closed circuit television (CCTV), crime scene video and images, 911 calls or other audio recordings, video that is captured by the general public, private businesses or the media, documentation that is scanned and converted to digital files, and digital content from computers, cellular phones, and other electronic devices.

- The NICE DEMS shall manage all types and forms of digital evidence in line with the agreed to business requirements of all the stakeholder agencies and departments in the COSB criminal justice system.

- The NICE DEMS solution shall be scalable to support varying data files sizes for photograph images, voice, and video recordings on different cases.

- The NICE DEMS and the Disaster Recovery (DR) solution shall contain quality control components to best support error-free storage and management of digital evidence.

- The NICE DEMS shall support the ingestion of COSB's current catalog of digital evidence consisting of digital video, photographs, audio recordings, third-party video and documents formatted in Portable Document Format (PDF) as well as future uploads, downloads, storage, retrieval of digital assets.

- The NICE DEMS shall provide a streamlined approach for requesting and viewing digital evidence along with the tracking of all requests.

- The NICE DEMS shall track the chain of custody of evidence collection through disposition.

- The NICE DEMS shall meet the application functionality requirements of each of the stakeholder agencies/departments in the criminal justice system. These include receive and classify digital evidence, exchange digital evidence, review digital evidence, maintain the integrity of digital evidence, generate derivative content, and archive and dispose digital evidence.

- The NICE DEMS shall support granular role-based content security and access control.

- The NICE DEMS shall support Chain of custody and cyber security requirements which mandate that the System supports audit logs for all access.

- The NICE DEMS solution shall allow individual stakeholder agencies/departments in the criminal justice system to have a private repository to manage content that they own

- The NICE DEMS solution shall allow the sharing of digital evidence from one entity to another.

- The NICE DEMS solution shall include an option for a deployment with a geo-redundant failover environment.

- The scope of services for this NICE DEMS solution offering includes technical documentation, project management, installation, engineering, configuration, testing, implementation, training and deployment of the NICE DEMS and DR solution.

- The NICE DEMS solution shall include all necessary hardware and software components and maintenance support.

- The NICE DEMS solution will be deployed as a cloud-based Software-as-a- Service (SaaS), hosted within Microsoft's Azure Government cloud.

- End user access to NICE DEMS is over the HTTPS protocol, with end users connecting via their Web browser from any LAN connected PC, Wi-Fi/Cellular connected laptop including smartphones of COSB personnel.

- The NICE DEMS solution shall function in a heterogeneous systems environment, providing standards-based integration opportunities between NICE DEMS and existing deployed technologies including existing agency/department-owned Enterprise Content Management and Case Management Systems, and future BWC video systems.

- NICE shall be responsible for the implementation of the integrations as detailed in this statement of work.

‧COSB shall be responsible for ensuring any third-party vendors provide the information necessary to complete any works on the integrations. NICE shall assist with all technical discussions with third parties where applicable.

NICE DEMS INTEGRATIONS WITH EXISTING COSB/STAKEHOLDER DATA SOURCES

The NICE DEMS solution shall integrate with the following identified existing agency/department case management and content management solutions to automate the collection of case related information and digital evidence from these connected data sources.

‧"Integrate" includes export out of NICE to a 3rd party vendor in a usable format

‧Detailed requirements for the integrations will be agreed to and documented during the DEMS Planning and Design Phases of this project.

‧All Integrations are subject to the participation from the 3rd party vendor in providing the necessary API or technical information necessary to support the integration effort.

‧It is the responsibility of the COSB/stakeholder owner of the system to work with 3rd party vendors to obtain the necessary technical support required for the Integration.

‧NICE will design and develop all software connectors required for the listed integrations in the Requirement Traceability Matrix attached as Attachment A to this Exhibit A – (RTM) .

Technical Overview

NICE DEMS is a cloud-based Software-as-a-Service (SaaS), hosted within Microsoft's Azure Government cloud solution. All access is over the HTTPS protocol, with end users connecting via their Web Browser, and the Data Source Gateway (DSG) connecting to Web APIs. Azure Government data centers provide enhanced security policies for access control and maintenance, sufficient to meet CJIS security policy requirements (https://www.fbi.gov/services/cjis/cjis-security-policy-resource- center/view).

A detailed technical description document, the NICE DEMS Site Readiness Document is attached hereto as Attachment C, and provides technical aspects and key architectural points within the NICE DEMS suite of products.

ARCHITECTURE

The architecture for NICE DEMS consists of items deployed within the COSB Sheriff Infrastructure and items deployed within the Microsoft Azure cloud subscription.

The Microsoft Azure cloud components shall host the evidential data store and the software components required to service the DEMS client web interfaces.

Within the COSB Sheriff Infrastructure, a Virtual Machine(s) shall be deployed as the DEMS Data Source Gateway(s) (DSG). The DSG(s) shall connect to COSB data sources for indexing and collection of the evidential data to be stored within NICE DEMS. A diagram detailing the high-level architecture is shown below.
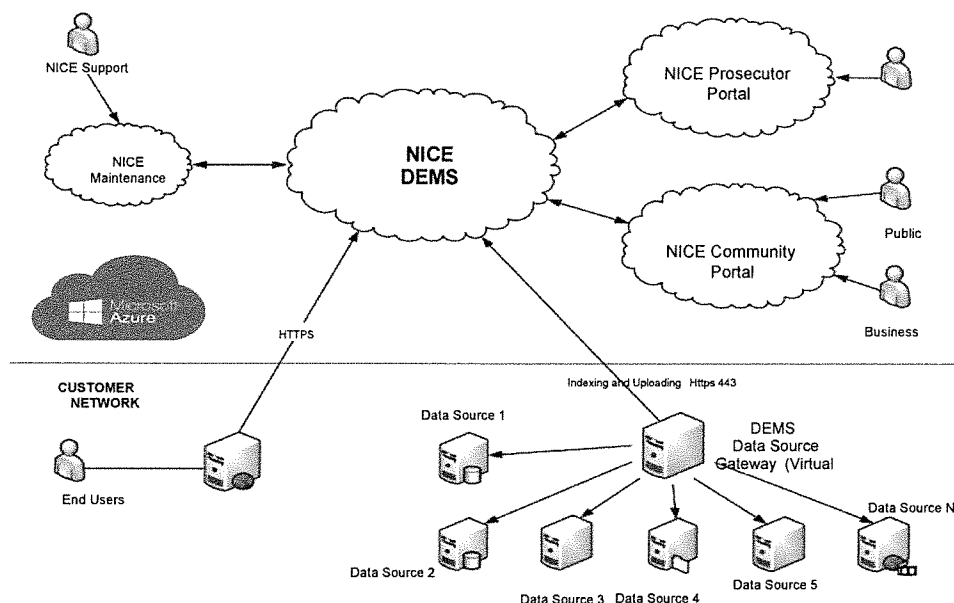
The data sources shown are those required for the delivery. Further data sources may be added during the service period as required.

DEMS PORTALS

The NICE DEMS SaaS solution consists of a number of portals to provide access for public bodies, Investigators, and criminal justice organizations. The portals which shall be deployed on the DEMS instance are:

- Main DEMS Portal
- DEMS Download Portal
- DEMS Administration Portal
- DEMS Community portal
- DEMS Public Portal
- DEMS Business Portal

NICE DEMS shall be deployed with the most current version of released software.

STORAGE

NICE DEMS shall be deployed with initial storage capacity per the COSB requirements.

DATA SOURCE GATEWAY (DSG) SPECIFICATION REQUIREMENTS

The DEMS Data Source Gateway provides the integration point between the data sources and the NICE DEMS platform. A number of virtual servers shall be deployed within the COSB network infrastructure. These servers shall host the integration software required to connect to the data sources and transfer the data to the DEMS platform. All connections of the DSG are outbound only, using secure browser protocols (i.e., HTTPS).

The recommended specification of the virtual servers which shall run the DSGs is as follows:

Item	Specification
CPU	4 vCPUs @2GHz
System RAM	16GB
HDD	200GB
Network Interface	Ethernet TCP/IP: minimum speed 100 Mbps, 1Gbps recommended configured as Full Duplex

Operating System	MS Windows Server 2019 or MS Windows Server 2016

COSB shall be required to provide 1 or more VMs to host the number of recommended DSG connectors. The exact number of VMs shall be determined during the Planning Phase for this project.

EXTERNAL CONNECTIONS REQUIREMENTS

Communication between the DSG and Client workstations to the NICE DEMS platform are made over a standard internet connection via TCP network ports. COSB Sheriff are required to ensure that suitable firewall rules are in place to allow these communications. The required network ports are detailed in Table 1 below.

Table 1: Network port requirements for DSG and client workstations

Application	DEMS End Point	Destination Network Port	Protocol
DSG to NICE DEMS			
DSG	DEMS DSG API	TCP 443	HTTPS
Azure Storage (blob)	Azure Storage (blob)	TCP 443	HTTPS
Client PC to NICE DEMS			HTTPS
Web browser	DEMS client APIs	TCP 443	HTTPS

IMPORTANT: Internet access is paramount to the correct working of the system and should be always available.

External HTTPS connections use FIPS 140-2 security algorithms.

No incoming connections are required from the internet.

INTERNAL CONNECTIONS REQUIREMENTS

The DSGs connect to the data sources for indexing and collection of evidential data using standard network connections. These connections are made via standard TCP ports.

Defined DSG network port requirements to connect to data sources shall be determined during the detailed technical design phase.

DSG MAINTENANCE AND CONNECTIONS

Maintenance of the DSG virtual machines up to operating system level is the responsibility of COSB Sheriff. NICE are responsible for the configuration and maintenance of the NICE DSG software. To facilitate this maintenance, NICE shall require the ability for authorized users to access and monitor the DSG virtual machines from outside using VPN and remote access.

Access to the DSGs shall be initiated only from approved secure locations within NICE, by authorized personnel.

CLIENT CONNECTIONS

NICE DEMS is accessed using any standard web browser, although the best performance is achieved with Google Chrome or Edge. No software is needed to be installed on the client workstation.

The NICE Data Source Gateway (DSG) is installed on the COSB Sheriff network and provides the secure connection point between local data sources, (e.g., CAD, Records, etc.), and the NICE DEMS cloud service. It uses a selection of custom integrations, called

"DSG connectors", for searching and retrieval of the meta data and media from each individual data source.

The DSG periodically queries each data source for any new records, or changes to existing records and transfers the data up to the NICE DEMS cloud to allow the Authorized users to build a holistic view of any Cases and evidence available to them. Any multi-media evidence that can be directly linked to a Case (e.g., supplemental reports, Crime scene photos, etc.), shall also be automatically pushed securely up to the cloud to remove the burden of retrieval from the Authorized users

Figure 2 – High Level Architecture Overview
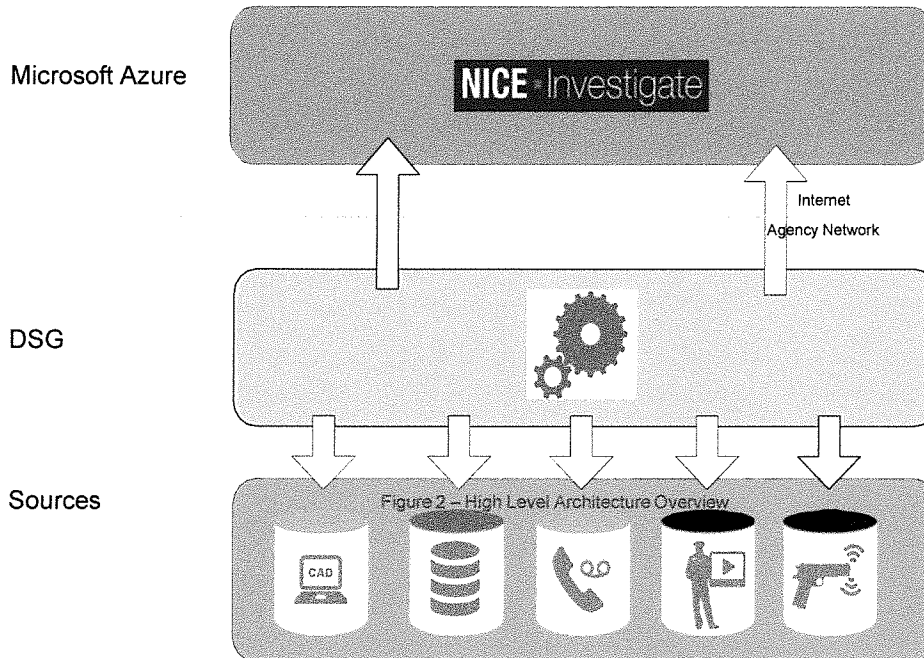
BANDWIDTH REQUIREMENTS

Operation of NICE DEMS requires defined internet access bandwidth both for users to access the system and for the DSG to upload and index any media data. Any network management tools on site need to be adjusted to allow for the requirements of NICE DEMS.

The bandwidth requirements shall vary during the initial deployment of the system.

NICE DEMS shall be uploading all digital evidence related to a Case; hence the key bandwidth drivers shall be video, photos and audio.

COSB shall be required to make sufficient bandwidth available to enable NICE DEMS to upload and download data to meet the requests of the DEMS platform and the users.

RESILIENCE AND REDUNDANCY

NICE DEMS is based upon Microsoft Azure Technologies and leverages their resilience features. Microsoft Azure provides transparent resilience for storage and queues which form the core of the NICE DEMS infrastructure. All data is synchronously replicated across three different storage nodes within the same Azure data center.

The NICE DEMS specific code runs as multiple load balanced instances of each of the front and back-end services and is designed to handle short term connection outages with automated retry policies.

Project Approach: Project Charter and Methodology

NICE shall plan the activities to be carried out in the project, the assignment of County and NICE resources to those activities, the dependencies among those activities, and their timing. NICE shall establish a project control and reporting system to provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans. Working with COSB Project Manager, NICE shall set up roles, responsibilities, record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

NICE shall follow project management methodologies consistent with the standards and guidelines of the Project Management Institute (PMI) Project Management Methodologies stated in the Project Management Body of Knowledge (PMBOK) or similar industry standard. For details regarding the PMI, please refer to www.pmi.org.

NICE shall provide on-going project management including regular (weekly) project plan updates, weekly status reports and weekly status meetings. NICE shall prepare a baseline risk management plan and update the plan regularly (bi-weekly) over the course of the project.

NICE shall provide the following project management activities:

- Development and Management of a Project Management Plan (PMP)
- Project Document Management
- Resource Management (COSB and NICE Staffing)
- Schedule Management
- Communications Management (Status Reporting/Stakeholder Communications)
- Quality Assurance, including Quality Gate Reviews
- Risk and Issue Management and Escalation
- Scope and Requirements Management, including Requirements Traceability
- Cost Management
- Change Request Management
- Performance Management (Project and System)

To deliver a quality deployment, NICE Project Management uses a five-step delivery approach: Initiation, Planning, Execution (includes training), Closure and COSB Rollout.

Project Assumptions

The following assumptions have been used to develop this SOW. Any deviation from these assumptions may cause changes to the project schedule, fees and expenses, tasks, and the level of effort required to perform the Services covered by the SOW.

GENERAL ASSUMPTIONS

- COSB shall be responsible for the responsiveness and performance of any third-party vendor and/or subcontractor engaged by COSB in connection with the Solution described in this SOW.

- COSB shall provide reasonable access to the necessary COSB facilities, and suitable workspace for all NICE project team members when working at the COSB's site when necessary. Suitable workspace includes, but is not limited to, desks, telephones, access to the system and meeting rooms.

- COSB shall identify and schedule training class attendees and facilities in connection with any training to be provided by NICE hereunder.

·All training and consulting Services to be provided by NICE under this SOW must be used by COSB within twenty-four (24) months following the date of completion of the installation Services to be performed hereunder, signified by NICE's notification to COSB of its completion of the NICE installation test procedure. If COSB fails to use the consulting/training Services within the aforementioned twenty-four (24) months period: (a) COSB shall forfeit its right to receive and use such Services; and (b) NICE shall invoice COSB for the fees for such training and consulting Services, which shall be paid by COSB in accordance with the payment terms set forth in the Agreement.

·If there is a need for an escort across the site facility, COSB shall allocate a dedicated security person as needed.

·Installation of Products and application migration and testing shall be performed during NICE normal business hours (Monday-Friday 8:00 a.m. – 5:00 p.m PST.).

TECHNICAL AND FUNCTIONAL ASSUMPTIONS

·NICE shall provide the NICE Site Preparation Checklist at the project kickoff meeting as outlined in Attachment A. COSB shall complete all items on the NICE Site Preparation Checklist approximately two (2) weeks prior to the commencement of installation.

·COSB understands that all site readiness activities shall be completed no later than two (2) weeks prior to scheduled implementation date including formal review and agreement of Site Preparation Checklist.

·COSB shall confirm and provide network IP addresses, firewall access, and required open ports per NICE's specifications.

— COSB shall provide a lab (staging area) that is ready to be used for a testing environment.

Deliverable #	Deliverable Name
Deliverable 1	Project Kickoff Presentation
Deliverable 2	Project management Plan and Schedule
Deliverable 3	Project Status Updates
Deliverable 4	Solution Implementation Plan
Deliverable 6	Solution Design
Deliverable 7	Requirements Traceability Matrix
Deliverable 8	Application Configuration Document
Deliverable 9	DSG Integration Design Document(s)
Deliverable 10	Test Plan
Deliverable 11	User Acceptance Testing Results and Remediation Processes
Deliverable 12	Training Plan
Deliverable 13	Production Cutover Plan

Roles and Responsibilities

NICE RESOURCES

Following the execution of this SOW by both parties, NICE shall assign a project manager ("NICE PM") in connection with its performance of the Services to be performed hereunder. The NICE PM shall serve as the primary point of contact for NICE in connection with the Services and shall be responsible for working with the COSB team, including the development of a project plan, and NICE's coordination of the Services to be performed by it hereunder.

STANDARD NICE ROLES AND RESPONSIBILITIES

NICE Project Manager – Responsibilities of the NICE PM include:

- Be a proactive and customer-centric interface between COSB and NICE, while determining that internal customers, technical staff and upper management are kept aware of project status, issues, and escalations.

- Plan, estimate and organize overall implementation of NICE products while being applied in COSB environments.

- Provide daily direction, motivation, and support to project team.

- Plan for project contingencies and anticipate variations that may affect resources, successful implementation, and revenue recognition.

- Serve as the communication link between COSB and NICE throughout the entire project, and act as liaison with other NICE departments.

NICE Professional Services Engineer ("PSE")

- The NICE PSE shall verify site prerequisites, install and configure the Solution, and conduct the Installation Test Procedure ("ITP").

NICE Education Specialist ("NICE ES")

- The NICE ES shall implement all aspects of the training as required by the purchased Solution, including preparing and conducting training classes.

Appendix A: Sample NICE DEMS Project Plan
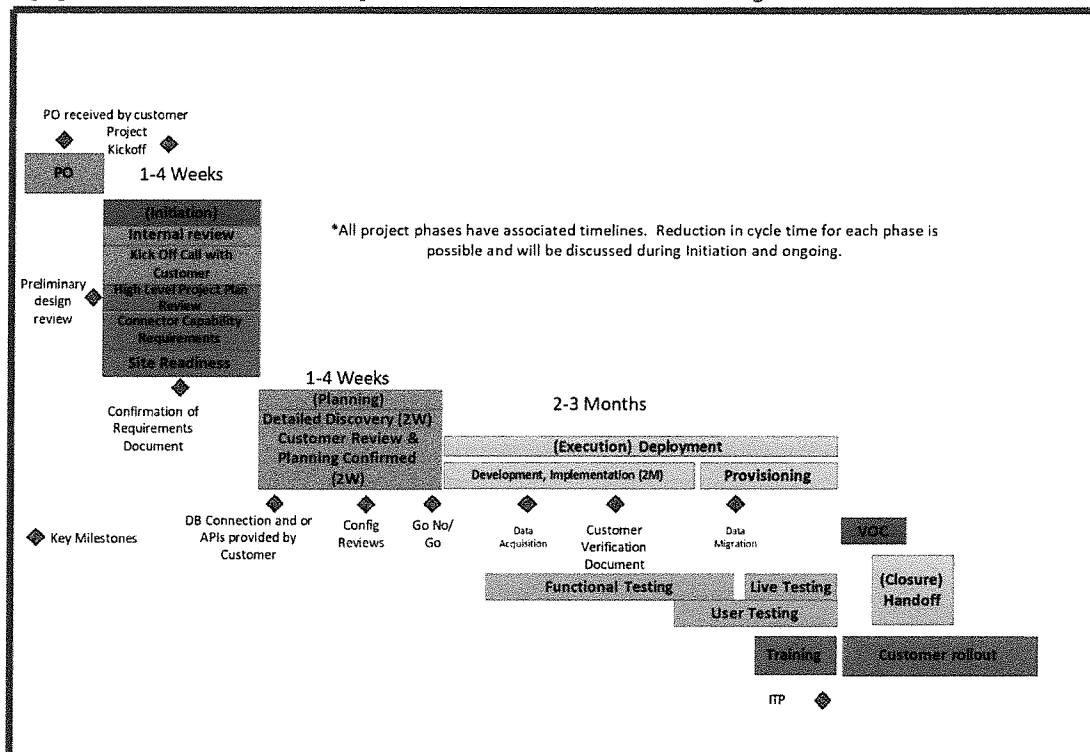
Appendix B: Description of Services

PROJECT ACTIVITIES

NICE follows industry standard PMI implementation methodology. The Solution shall be implemented in accordance with the following phases and activities:

Activity	Description	Responsibility	Output
Initiation Phase			
Project Validation	• NICE Project Manager reviews purchased solution.	NICE	NICE Project team created
Sales to Services Handover	• NICE Project Manager conducts Post-PO Sales to Service ("S2S") internal call with NICE Account Team to review SOW, Pricing and Solution Design relative to COSB's business need.		
Planning Phase			
Internal Kickoff Meeting	• Preparation for COSB Kickoff Meeting • Preliminary Project Plan is developed	NICE	Preliminary Project Plan
COSB Kickoff Meeting Conducted	• Review and finalize proposed Project Plan • Review executed Statement of Work • Review NICE Site Preparation Checklist.	NICE/ COSB	Final Project Plan

COSB Technical Discovery Sessions Held	· Discovery Sessions for each DSG connector · Discovery session for security/access controls and retention configurations · DSG design documents created · Security/Retention/Access Control policy documents reviewed and approved.	NICE/ COSB	Approved DSG design documents Approved Security/ Retention /Access Control policy documents
Execution Phase			
DSG Connector Development	· NICE development of DSG connectors · NICE testing of DSG connectors with COSB test databases · COSB approves functionality of DSG connectors · DSG solution software released	NICE/ COSB	
Site Preparation Checklist Completed	· COSB completes all items on the Site Preparation Checklist at least two (2) weeks prior to the installation date. · The NICE PM receives the completed NICE Site Preparation Checklist ("SPC") from COSB.	COSB NICE	Site Preparation Checklist completed by COSB
System Installed	· Remote software installation and hardware verification shall be completed by the NICE Professional Services Engineer ("PSE") in collaboration with COSB. An COSB representative shall be available for the NICE Professional Services Engineer ("PSE") to contact for support. · System includes components as described in the Project Scope Overview section of this SOW.	NICE	
System Configured	· Security policy configured · Retention policy configured · Access Control policy configured	NICE	
Execution Phase			
Installation Test Procedure ("ITP")	· While NICE conducts the ITP, a COSB representative shall be available to actively participate in the process. Upon completion of the tests set forth in the ITP, NICE shall provide a copy of the ITP to COSB. NICE, COSB shall retain a copy of the document, signifying the completion of the installation.	NICE/ COSB	Completed ITP

The COSB point of contact is responsible for notifying all COSB parties that the ITP has been completed.

Training Conducted	· Training includes sessions as defined in Attachment B of this SOW.	NICE
Closure Phase		
Solution Begins Working	· Solution begins working in COSB · environment(s). · Outstanding issues are addressed. Transition of support to NICE Customer Support Center ("CSC") takes place.	NICE/ COSB

COSB RESOURCES

COSB shall assign a project manager ("COSB PM") in connection with the Services to be performed hereunder. The COSB PM shall serve as the primary point of contact for COSB in connection with the Services and shall be responsible for working with the NICE team, including the development of a project plan, and COSB's internal coordination of the Services to be performed by NICE hereunder.

COSB PROJECT MANAGER

The NICE PM and COSB PM shall work together to act as the main vehicle for all communications and implementation-related activities.

SYSTEM ADMINISTRATOR

This person shall be familiar with all operational aspects of the NICE Solution that is installed. They shall understand the basic functional components of the Solution and how they should be deployed within the COSB contact center infrastructure. The System Administrator shall have the most technical responsibility within the project.

IT SPECIALIST

This person shall be needed to address network infrastructure needs, specifically providing the VMs for the DSG, the bandwidth to connect the DSG to the cloud, and administering security certificates.

Task 2. System Design, Development and Configuration Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
2.1	**System Implementation Planning**	Contractor shall describe its preliminary System Implementation Methodology Plan (e.g., implementation and/or development methodology and plan) for system analysis, design, build and deployment. Clearly identify the timing of each stage and key milestones, including the rationale for Contractor's proposed timeline and any assumptions. The plan shall align the stages, milestones, and deliverables in the project plan with this Statement of Work.	The **System Implementation Plan** shall ude (at a minimum): • Description of the implementation methodology and plan for delivering DEMS, including: — Installation and/or setup — System Analysis and Design — System Configuration — System Build (e.g., data import, interfaces) — Testing (e.g., unit testing, system, UAT) — Training Production Deployment (e.g., including • possible phasing strategies, site specific considerations, and benefits and risks of strategy alternatives) • Production Go-Live Support • Post Production Go-Live Support Identification of stages and key milestones, including any assumptions. Aligns the stages, milestones, and deliverables in the Project Plan within this Statement of Work. — Description of dependencies on DEMS project activities and any external constraints or dependencies. — Organization change management recommendations **The Deliverable shall include a DED.**

2.2	System Design	Contractor shall use a structured, iterative methodology for incremental deployment of functionality between environments. This approach allows both Contractor and the County frequent feedback as to the progress of the Project with opportunities to make corrections in interpretation and will result in a better understanding of the challenges of the Project at an earlier date. Contractor shall conduct workshops with the County during project initiation and planning to determine the System production deployment approach for rolling out DEMS. Contractor shall incorporate the design and development approach into a comprehensive System Design and Development Plan complying with IEEE 12207.2, Section 5.3.3 - System Architectural Design.	The System Design and Development Plan deliverable shall minimally include: • se cases, business process flows or a similar mechanism describing how DEMS will be used in the context of each County business process • DEMS security and privacy controls Key business processes and/or policy changes required to conform with DEMS capabilities • Summary level descriptions of DEMS configuration changes needed to meet County requirements **This Deliverable shall include a DED**

2.3	Requirements Traceability Management (Exhibit A Attachment A – RTM)	Contractor shall validate, update, and manage the functional and technical requirements to ensure traceability throughout the life of the project.	The **Requirements Traceability Plan** shall, at a minimum, address the following areas: • Establish a baseline for existing requirements • Manage versions of requirements • Establish and maintain the County's requirements traceability matrix that will be used for requirements management, and map where in the software a given requirement is implemented • A requirement change control process • A methodology for managing requirements in an iterative development lifecycle or each requirement, the **Requirements Traceability Matrix (RTM)** shall include: • Reference to Exhibit A Attachment A - RTM • The specific DEMS component (e.g., screen, report, workflow, data field) where the requirement is met • The test scenario(s) where the requirement is tested • The training module where instruction is provided for the requirement **The Deliverable shall include a DED.**

| 2.4 | Configuration Management | Contractor shall document the system configuration, including references to system tables where appropriate. | The Application Configuration Report shall include history of configuration changes, including references to system provided change logs if available. In addition, the Deliverable shall include detailed specifications for all system changes/customizations and shall also include information regarding the configuration needed to scale and expand within and across other agencies/departments, potentially including those outside of criminal justice.
The Configuration Management Plan deliverable shall minimally include:
• Platform-specific Hardware and Software solution components.
• Descriptions including Architecture or Configuration updates, new functionality introduced, defects fixed, modifications to interfaces with other systems, other changes to existing code, and any software and hardware configuration changes.
• Detailed hardware and software configuration information including any software and hardware dependencies and instructions at a level of detail that will enable System administration staff to rebuild and configure the hardware environment.
• Detailed configuration information for any 3rd party hardware and software.
The Deliverable shall include a DED. |

Deliverable Expectations Document (DED):

NICE SYSTEM IMPLEMENTATION PLAN

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: System Implementation Plan
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>

Deliverable Owner (County):	Deliverable Author (Vendor):
<Name, Role – TBD, as mutually agreed >	<Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose:
The NICE Professional Services organization has fine-tuned and refined the proven Project Management Institute (PMI) System Implementation Planning and Delivery methodology to provide a NICE DEMS delivery approach that ensures shortest time to value for COSB. This is reflected in the System Implementation Plan and associated sub-plans under System Design and Development Plan.

Deliverable Scope / Content Expectations:
NICE will provide full documentation for System Implementation Planning for agreed-upon solution and its phased deployment. The deliverables will include: NICE System Implementation Plan Project Management Initiation and Preparation Execution Sample: The following plan is based on repeatable, consistent processes utilized with all NICE Public Safety solution deployments.

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.

NICE System Implementation Plan

The NICE Professional Services organization has fine-tuned and refined the proven Project Management Institute (PMI) delivery methodology to provide a NICE DEMS delivery approach that ensures shortest time to value for COSB.

NICE's approach is focused around the intent to have COSB on-boarded in a timely fashion—educated and equipped for the daily use of the NICE DEMS solution.

NICE shall conduct workshops with SBCO during project initiation and planning to determine the solution design and deployment approach for rolling out the DEMS solution, including possible phasing strategies, site specific considerations, as well as benefits and risks of strategy alternatives.

NICE shall apply industry best practices and work with COSB to determine recommendations for managing organizational change required for the solution to meet the project objectives. Such recommendations shall be developed considering business impact on each of the key stakeholder groups.

The below methodology walks you through what to expect so you can be well prepared for the deployment.

PROJECT MANAGEMENT – EXPERT PLANNING, COORDINATION AND CONTROL

To oversee your deployment, a NICE project manager will be the single point of contact for COSB. The NICE project manager will work with COSB's own project management team and will take full responsibility for all NICE- related activities — from inception and planning to the final handover to your team.

To deliver a quality deployment, NICE Project Management uses a five-step delivery

approach: Initiation, Planning, Execution (includes training), Closure and COSB Rollout. This process has been refined over scores of projects.

Since NICE project managers work exclusively with NICE solutions, they are well versed in all the contingencies, dependencies, and requirements of even the most complex NICE implementations. That experience can dramatically streamline the process for your team and help avoid needless delays and complications.

Throughout the project from inception through closing NICE and COSB will document identified and known risk areas and mitigation steps for each. Thus, a well thought out project kick off involves the communication, explanation, and a detailed sharing of the expectations, best practices, team responsibilities, identified high risk areas, and desired outcomes of the engagement, enables a highly efficient and successful implementation with a high probability of exceeding the project implementation objectives of providing the client with the capability to mitigate any of the identified risk areas, actively engage the solicited technology solution, and realize the larger stated organizational objectives. NICE's mitigation tools and established best practices and methodologies are complemented by NICE's continuous communication, strong documentation and ongoing cooperative validation of the proven strategic steps NICE and the COUNTY completed in each phase of the phased, risk-based approach for implementation, planning, training, testing, delivery, and client feedback, During each phase of the project NICE and COSB collectively look for opportunities to improve the timeline and compress the schedule to bring the solution to its useful intent at the fasted possible opportunity.

INITIATION AND SYSTEM IMPLEMENTATION PLANNING

Preparation for Successful Deployment of NICE DEMS

The NICE project manager will review with the internal NICE customer engagement team the overall objective and details of the solution design as prepared and purchased by COSB.

The NICE project manager will schedule a Kickoff call with the COSB project manager and relevant stakeholders to review the objectives, design and scope of the solution as sold to ensure all parties are on the same page. During the Initiation discussion, the NICE project manager and COSB project manager will review the overall project delivery scope, high level project plan, connector capability requirements and COSB site readiness. The respective project managers will also establish the communication cadence for the project. They will review all the project documentation that is associated with each phase of the project to ensure all stakeholders are receiving status updates and project control details throughout the project. At each step in the process COSB will have a complete understanding of the status, next steps, and a timing confirmation to reduce and eliminate risks.

The First Critical Path Phase - Pre-requisites for COSB Data Readiness

This will include but not be limited to the technical infrastructure, remote access and all the associated APIs and Database access for the preparation of the DSG connection and set up.
This is an area of significant risk to the success of the project timeline. The NICE project manager and team will work with COSB to establish a clear understanding for the secure remote connectivity required for the project and solution on an ongoing basis. Second, from the earliest discussions around the third-party systems NICE will capture data from through the workshop conducted. The immediate access to the data structures, DB access and or APIs is a critical milestone.

This area can have a two-fold impact on the project and solution. Short term it will impact all the timelines and planned activities. If the access to the source data are not understood or available the solution and data within will not be accurate, useful, or provide value. NICE will

discuss this with the COUNTY further during planning.

Keeping the success and timely completion of the project in mind, it is always very useful for all stakeholders to have visibility into steps along the timeline in order to understand what to expect along the way. NICE takes pride in partnering with COSB during all phases of solution delivery, understanding that it will be COSB's first time with an engagement of this type.

PLANNING STAGE

After all Parties have reviewed and agreed to the scope, the next step is **Planning**.

At this stage, the respective project managers will refine the high-level project plan and lock down the detailed project plan with timelines for the Execution which includes development of the DSG to handle the third-party data, provisioning the instances in the cloud, data collection of the historical Case data, and migrating the historical data for reference, while testing these multiple areas along the way. The Execution phase wraps up with the training and then transitions to COSB for your planned Rollout of the solution to the users. The first major activity of the Planning phase is a detailed discovery session with the COSB teams.

A key element to success is the connections to COSB third party systems that feed data to the NICE DSG. As per the Initiation phase where the requirements were shared for this milestone, the NICE and COSB teams will complete a detailed design and respective review over the course of approximately two weeks. This will contribute to the development of the detailed overall project deployment plan.

As previously shared, this is a significant milestone and risk area to the project timeline and the solution itself. Historical data will also be reviewed and taken into consideration as a deliverable and milestone COSB is responsible for.
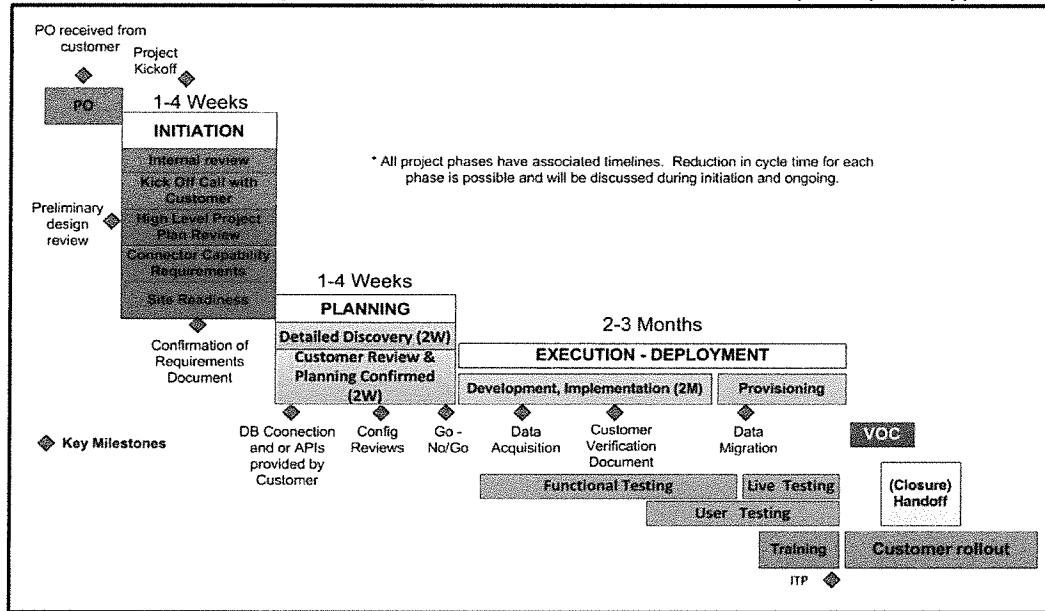
Once NICE has the identified data, the planning for acquisition, migration of the data and testing will be in the plan and associated tasks.

With the detailed project plan and timeline agreed to, the respective project managers will review specific tasks required to deliver the implementation or Execution phase flawlessly. The respective project managers will identify the specific resources needed from both organizations to accomplish each task.

With the tasks identified, the respective project managers will build out the detailed work breakdown structure for each task with the associated timelines and dependencies. The site preparation task will have a "go - no go" milestone two weeks prior to the planned execution phase.

Below, is a high-level example of a DEMS project plan showing the key phases of the plan and associated timeframes for delivery. NICE has created a COSB specific plan with a representative start date of January 1, 2025. NICE will update this baseline plan to accurately reflect the project timelines as NICE and the COUNTY move forward with project planning. (please see the attached MS Project Plan)

4.2   *NICE Project Delivery Phases & Estimated Duration (Example only)*

EXECUTION

Deploying NICE DEMS, Testing & Training

The deployment of your NICE DEMS solution is performed by specialist NICE installation technicians via secure remote access provided by COSB. Under the coordination of your NICE project manager, the NICE resource(s) are responsible for everything from the development of the connectors to your third-party systems (DSG), provisioning of the NICE DEMS application, testing and training, to final hand-off to your users and the NICE operations and support organization.

As agreed during the Planning phase, the NICE resources under the direction of the project manager will remotely install the software for the DSG on COSB's premise environment. The NICE DEMS pre-production instances will be set up in MS Azure as a unique instance for COSB.

The NICE resource will establish connectivity between your third-party source system(s) as outlined in the detailed design and scope plan, then test the connection(s). Once the DSG environment is established and tested, NICE resources will connect the DSG via secure link to the COSB instance in MS Azure. The DSG connection to MS Azure along with the NICE DEMS pre-production instance will be tested by the NICE resources to confirm the data in the NICE DEMS application.

As part of the use of NICE DEMS, historical data will be very useful and helpful as a compliment to the current Case data. Another key milestone is the identifying and acquisition of the historical data and then the migration of this data.

Module Title	Outline
DEMS Portal Overview	By the end of this module, you will be able to: • Describe the NICE DEMS Solution • Log in to the NICE DEMS Portal • Reset your password • Configure your notifications • Configure your user settings • Use Help
Case and Evidence Items	By the end of this module, you will be able to: • Create a New Case and Upload Evidence Items • Navigate an Existing Case • Case Item Actions • Navigate Case Evidence Items • Case Evidence Item Actions
Case and Evidence Views	By the end of this module, you will be able to: • Describe the views available for Case and Evidence Items • Work with Grid and List view • Work with the Timeline View and Playback Video & Audio • Work with the Map View and Playback Video & Audio
Filtering and Ordering Cases	By the end of this module, you will be able to: • Describe Filtering and Ordering • Filter Cases and Evidence Items • Filter using the Refine by Option • Filter using Keywords • Filter using Configurable Fields • Create a Saved Filter • Use the Ordered by Option
Search Evidence	By the end of this module, you will be able to: • Search for Cases and Case Evidence Items using Search Criteria • Add Searched Evidence to a Case • Perform a Document Search • Perform an Audio Search
Evidence Suggestions	By the end of this module, you will be able to: • Navigate the Suggestions Page • View Suggestion Information • View Suggestion on the Map View • Add Suggestions to a Case
Evidence Requests	By the end of this module, you will be able to: • Submit a Request to a Business • Submit a Request to a Citizen • Submit a Request to a Business using Map View • Track Requests • Add Media Items to a Case

Audio and Video Evidence Items	By the end of this module, you will be able to: • Use Playback Controls • Clip Audio and Video Files • Create a Snapshot • Redact Audio from Media • Redact Video from Media • Use Zoom Controls • Add a Bookmark
Sharing a Case	By the end of this module, you will be able to: • Overview of Sharing Case and Evidence • Share a Case and Case Evidence Items with Users • Share a Case and Case Evidence Items via Download with Users • Manage Shares using the Sharing Page

Validation and communication are critical path items to the success of the deployment. At each step in the deployment process, the NICE project manager will be communicating with the COSB project manager to provide status updates of the progress and completion of each task and validate. **The validation is a two-step process where it first confirms delivery of an execution task in the delivery process.** The second step is that the task is confirmed and tested by COSB. This ensures both parties are on track for the overall project delivery timelines as set forth during the Planning phase.

The testing and validating of the NICE DEMS solution will be conducted by the NICE resource using the NICE Implementation Test Plan to verify that your solution is ready for training and COSB rollout.

They also provide full documentation of the details including all test results, the set up, and configuration of your solution are documented. NICE and the County are now ready for training.

Training

Training is a critical path item and the key to the last step of a successful project. To help gain maximum return on your investment in NICE DEMS as quickly as possible, NICE's Customer Education Services team provides users with the knowledge and skills needed to take full advantage of its capabilities right from the start.

NICE crafts their training approaches as carefully as NICE develops their award-winning solutions, using the most effective state-of-the-art training platforms and techniques.

During the Planning phase the dates for the Training were established and confirmed as the ongoing deployment was underway and as part of the validation communication.

Key User Application Courses

NICE hands-on training covers the full functionality and capability of NICE applications for Key Users and Administrators, conducted at COSB's site. The entire curriculum requires one day of education. Depending on the number of sessions and students, the appropriate training plan and schedule will be determined during the Planning phase. NICE understands it is difficult for staff to be away from their work for an entire day thus NICE provides a level of flexibility to deliver in half day segments. This also allows for some practice time as well away from the classroom.
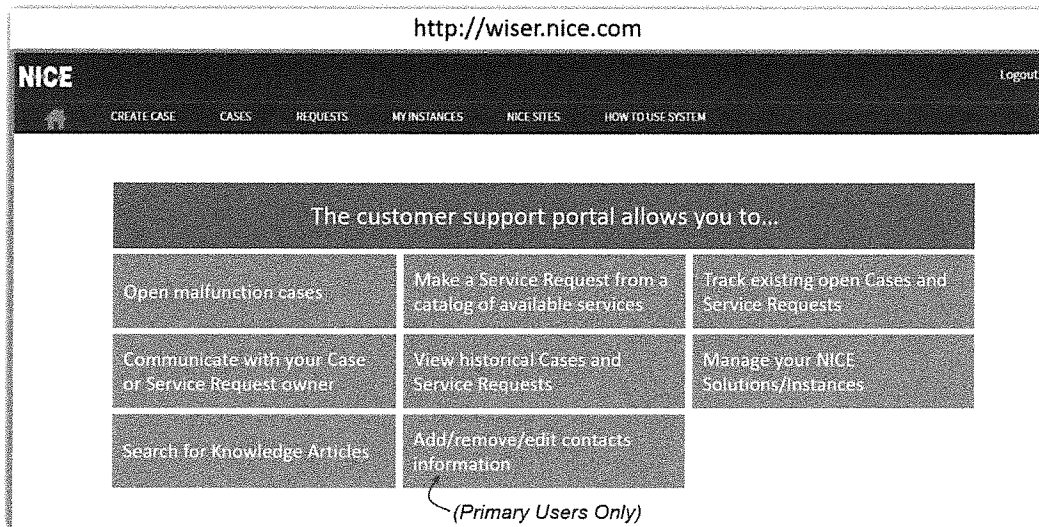
Train-the-trainer Courses

NICE provides a specialized program that enables in-house trainers to conduct internal courses for NICE users, all based on the techniques and content NICE's own trainers have found most effective. This will help extend NICE solution skills throughout the organization and maintain high levels of proficiency over time. The learning experience NICE has found

to be most effective is a three-pronged approach. First, NICE delivers the course material to the COSB education specialist. Second, NICE will co-deliver the class with your education specialist and lastly, NICE will observe the COSB education specialist deliver the class. The course Trainer Guide along with the education material will be provided to the COSB education specialist.

CLOSURE AND HAND-OVER

At this stage, closure, the technical delivery of your DEMS solution is complete and the Training has been delivered. The NICE project manager will conduct an introduction for COSB to NICE's Customer Support organization and processes. COSB will be set up in NICE's Wiser Customer Case Management system and COSB will be shown how to open up a support case via the Wiser Portal in the event that COSB needs to raise a case for support.

During the review of the Wiser Portal, the NICE project manager with the assistance of the NICE Support Manager will review the COSB support process, severity definitions and associated SLAs to ensure COSB is aware of the process and support delivery obligations of the NICE Customer Support organization.

VOICE OF COSB

Upon closure the NICE project manager will remind the COSB project manager that a member of the NICE Voice of COSB organization will reach out to them to schedule a live phone interview to capture valuable feedback on the project and the NICE resources who participated in the project. NICE thanks COSB in advance for taking the time with this last step in the critical path to a successful COSB experience.

Deliverable Expectations Document (DED):

NICE SYSTEM DESIGN & CONFIGURATION MANAGEMENT PLANS

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: System Design & Configuration Management
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>

44

Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>
Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose: NICE System Design Plan details the customizations that will be installed and configured for COSB's NICE DEMS deployment. It does not describe the functionality of NICE DEMS as that is covered elsewhere.

Deliverable Scope / Content Expectations: NICE will provide full documentation for System Design Planning for agreed-upon solution and its phased deployment. The deliverables will include: •   NICE DEMS Deployment Overview •   DSG Connectors to all relevant evidence data sources • NICE DEMS Field Configurations Sample: The following NICE System Design Plan is taken from a specific NICE customer design and deployment. Since it is based on an actual plan used with a specific NICE customer, it includes integrations that are presently not applicable to COSB.

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.

NICE DEMS Solution

<u>**Design Document**</u>

Example from actual customer documentation – customer and 3rd party product brand names have been redacted

---

SOLUTION DESIGN DOCUMENT REVISION INFORMATION

Revision: **0.2 Draft**
Date: **04 Mar 2019**
Updated by: **Steven Leavens**

DOCUMENT HISTORY

Revision	Date	Author	Details
0.1	04-03-19	Steven Leavens	Initial Version
0.2	29/03/2019	Steven Leavens	Add detail for ports, connectors and detail layouts

INTRODUCTION

About This Document

This document details the customizations that have been installed and configured for the COSB NICE DEMS deployment. It does not describe the functionality of NICE DEMS as that is covered elsewhere.

REFERENCES

This section defines other referenced documentation relating to the Solution.

Ref	Document Type	Title	Reference
1	Technical description	NICE DEMS R1.6 Technical Description	TD884-101-01-06-00-03
	Site readiness	NICE DEMS Site Readiness	
2	Release Note	NICE DEMS Data Source Gateway – Software Release Note	RN884-401-02-06-0001-XR
	Discovery	NICE DEMS R1.6 - Customer Discovery	
	Integration Description	COSB Connector IDD	
3	COSB workflow diagram	Visio-CCTV Import process Part 1 (To Be) V5	

OVERVIEW

Description

The NICE DEMS Solution for CUSTOMER consists of

- NICE DEMS
- NICE Community Portal
- NICE Data Source Gateways:

Niche RMS (Occurrence data and users), Fotoware Images, Capita ControlWorks CAD (phase 2), Axon BWV (phase 2)
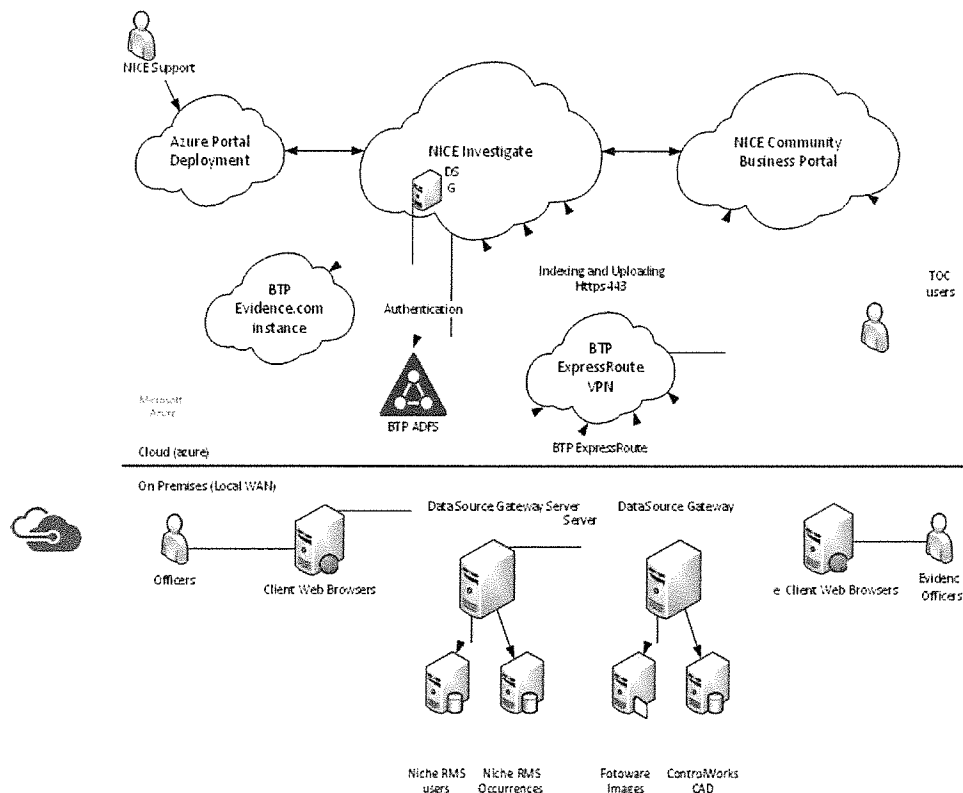
4.3   System Block Diagram

Figure 1: NICE DEMS system components

SYSTEM OVERVIEW

The DEMS solution consists of the cloud-based components of the DEMS, Admin and Community business portals and the on premises DSG components. These integrate with the COSB network infrastructure.

NICE DEMS is deployed in NICE's Azure subscription as a separate instance of DEMS just for COSB . NICE DEMS Community portals are deployed in NICE's Azure subscription as a shared instance with other forces.

DSGs are installed in Virtual Machines, or physical servers, on COSB 's premises with network access to the data sources that are ingested into DEMS. A further DSG is installed within NICE's Azure subscription for COSB to access the Axon API for BWV.

COSB are installing Azure ExpressRoute or another VPN client that provides a dedicated network link to the Azure cloud, this includes a VPN for COSB within Azure. All network traffic from the CUSTOMER] network goes via the ExpressRoute link. NICE DEMS is deployed outside of this VPN and so provision is made on the COSB ExpressRoute configuration to allow routing out of the VPN to the NICE DEMS deployments.

Authentication of users into NICE DEMS is to COSB 's ADFS presence.

4.4   Points to be resolved

- **Configuration of COSB ExpressRoute to allow connection to NICE DEMS.** Routing needs to be configured to endpoints for the NICE DEMS portals, Community portals and DSG API and DMZ storage.

- **Access to COSB 's instance of Axon BWV data source.** The instance of Axon's BWV data source is hosted in Azure. It is proposed that a DSG is hosted in NICE's

47

subscription to access the API. However, this solution may not work depending on the access controls to the instance.

CCTV WORKFLOW

The NICE DEMS Solution for COSB integrates within existing workflows and processes for the collection of CCTV video media with some minor alterations. NICE DEMS is used as the primary store for CCTV media and its metadata and so there needs to be a controlled workflow for request and retrieval of the media.

COSB are split into 4 divisions A, B, C and D. The workflow process will differ between divisions A/B and C/D in the manner that the requests are submitted, and media retrieved. There are also differences between requests to Train Operating Companies (TOCs) and other third parties. Thereafter once the media is held within NICE DEMS they are handled the same.

Retrieval Workflow

The workflow for request and retrieval of CCTV falls into the following main actions:

- CAD / Occurrence
- Request
- Retrieval
- Share to officer

Divisions A/B

- CAD incident is created, If it is a crime then a Niche occurrence will also be created
- In DEMS a case folder will be created for each occurrence, a case folder will be created for some CAD incidents based on what type of incident it is and other metadata values.
- Officer/OIC determines that CCTV media is required.
- Request is made into existing e-service system.
- Request is triaged at Ebury and a corresponding request is made in DEMS within the 'Requests' top level menu.
- Continue workflow at section 3.3.1.3.

Divisions C/D

- CAD incident is created, If it is a crime then a Niche occurrence will also be created
- In DEMS a case folder will be created for each occurrence, a case folder will be created for some CAD incidents based on what type of incident it is and other metadata values.
- Officer/OIC determines that CCTV media is required.
- Request is made directly in DEMS within the 'Requests' top level menu.
- Continue workflow at section 3.3.1.3.

All Divisions

Continued from 3.3.1.1, 3.3.1.2 or 3.3.1.4.

- The request is annotated and sent with the following information:
  — The CCTV reference number is entered into the request details.
  — If a Niche occurrence has already been created the Occurrence file number is entered into the request at creation.
  — If this is a CAD only request (non-crime) the incident number is added to the

48

request. The incident number can be added in addition to the occurrence number if required.

— If no Niche occurrence or CAD exists the request is created without the number; they can be added later, or the returned request media directly added to the DEMS case.

— A document is sent with the request for the recipient to read and assert that the upload is a true recording. A checkbox has to be ticked before the request is returned to indicate the statement has been read.

— If the TOC has signed up for submitting requests via the Business portal then the request is sent directly to the TOC. Otherwise, the request is sent to an 'Evidential Officer' to collect the media, this includes collection from other 3rd party entities.

▪ The request is received by the TOC or Evidential Officer.

— The TOC extracts the requested CCTV media and uploads into the Business portal and completes the request. The Evidential Officer goes to the TOC and gets the requested CCTV media. They upload the media into the Business portal and completes the request at a suitably equipped COSB regional office.

▪ The media is returned with the request to DEMS. The media goes through the DEMS processing workflow including the following actions: virus check, transcode to playable format and thumbnail extraction. A notification is sent to indicate the request was completed. ▪ The Officer/OIC can review the completed request and add to the DEMS case if one already exists. If the occurrence file number and/or incident number was added to the request when created it will show the corresponding case when adding the media.

— The Niche occurrence, if linked, can be updated to put an entry in the OEL and/or create property items for each media item.

▪ At this point the media is now available to all DEMS users with access to the DEMS case.

— The case or content can be shared with other DEMS users by giving the explicit contributor or reader access.

— The case or content can be shared with other, non-DEMS e.g. CPS, users by sending to it to the DEMS sharing portal. Here a user can be given a time limited code to access the shared media.

Request from third party

Requests for CCTV can come from third parties where no incident has occurred. In this situation no DEMS case folder will have automatically been created.

▪ Request from third party (on a form) this would come to Ebury.

▪ In DEMS manually create a case folder for the request, the case can be given the request reference as its name.

▪ Create an DEMS request from within the created DEMS case for CCTV.

▪ Continue workflow at section 3.3.1.3.

Processing workflow

After media has been retrieved and added to an DEMS case folder other processing actions may need to be performed on the media. Some processing is available within the DEMS such as clipping, frame capture, redaction etc. This can be suitable for initial sharing to other users, however for other purposes such as taking to court more enhanced processing is required. The following workflow outlines how this is achieved whilst keeping the media and any versions within DEMS.

- Item is selected within DEMS and the download action selected.
- Media is downloaded to the client workstation. The original can be downloaded at the
- same time if required, otherwise just the transcoded copy.
- The media is processed by other third-party tools creating one or more output files.
- In DEMS the processed files are uploaded to the case as new evidence items. They are tagged using keywords and comments.

  - The uploaded items can be of a different media type to the original. E.g. the court playbook could be uploaded as a pdf document.

- At each stage comments and keywords can be added to the item to log why the item was downloaded and what has subsequently been uploaded. The comments are time stamped and show in the comments tab for the item, keywords can be used to filter results easily to show items with the same keyword tags.

Sharing

Evidence items within an DEMS can be viewed by any user of DEMS with the appropriate permissions. Explicit permissions can be given to DEMS users if their default profile does not allow by giving them reader or contributor access to the case or individual evidence items.

For third party users, e.g. CPS or court, evidence items can be shared to the sharing portal with an access code. From there the user can view the items online or download them as required.

NICE DEMS DEPLOYMENT

The deployment uses the following deployment settings:

Setting	Value
Agency (Force) Name	COSB
AgencyId	COSB
Agency Short Name (DEMS)	COSB in
Microsoft Data center location	UK West/South (UKW, UKS)

LINKED PORTAL

The following portals are linked to COSB 's DEMS system. The communication between DEMS and these portals is direct from one portal to the other via the internet.

Portal	Comment
Community UK (Public)	In UKW, UKS data centers
Community UK (Business)	In UKW, UKS data centers

Business portal CCTV cameras

CCTV cameras can be registered by Business portal businesses and be the subject of requests for video media.

Suggestions

Suggestions are shown in the suggestions tab for a case and list other items in DEMS that might be related or useful for the current case. The items listed are ranked in an order of precedence based on configurable rules for each type of case or evidence item. Each rule can take the time and/or the location of the case or another evidence type within the case to find and rank the suggestion list. A match with either rule will return the item.

Registered cameras are selected and ranked according to the following rules:

Type	Rule
Distance rule	Within 2km of current case location OR Within 2km of matched CAD record location
Time rule	-

SECURITY POLICY RULES

The COSB DEMS system uses IP whitelisting to control access to the NICE DEMS portal; access is restricted to a list of source IP addresses.

Access to data held in DEMS is controlled by an Access Control Policy that is defined in coordination with COSB . The following policies are defined:

- NICE DEMS honors any viewing restrictions applied by the individual data sources, where available, as described in each connector section below.

- There is a general policy that shows a restricted view of ACLd case and evidence items in the search and suggestions pages, this just shows the name of the item and the OIC contact for the item.

- OICs are able to view and edit their occurrences (DEMS cases) and any evidence they contain.

- Others TBD

4.5 Points still to be resolved

- What roles are required by COSB

- Are the roles to be read from the COSB ADFS

- What access does each role have to the features of DEMS

- What access does each role have to the data held in DEMS

NICE DEMS PORTAL ENDPOINTS

See the Site readiness document for general details.

The NICE DEMS and its linked portals have the following endpoints:

DEMS endpoint	Address	Port
NICE DEMS. 6 endpoints	<TBD>.digital-olicing.co.uk	443
NICE DEMS Community Portal. 5 endpoints	<TBD>.digital-olicing.co.uk	443
NICE DEMS Prosecutor Portal. 3 endpoints	<TBD>.digital-olicing.co.uk	443

AUTHENTICATION

Users are authenticated in NICE DEMS with COSB 's ADFS presence. Other user details such as the user's name, various Ids, email address etc. are extracted from data imported from the Niche RMS system. Common information between the Azure user account and the Niche user data is used to join the two sources of data together. **Points still to be resolved**

inking the COSB ADFS users to the Niche and other data source user representations. DEMS holds the different representations for a user required to correlate a user with a particular evidence item. For COSB the data source representations include the Niche ID (number starting 150...), the officer's FIN or collar number and the officer's Niche UserID. These need to be linked to the DEMS login used to authenticate with COSB 's ADFS.

DSG

The DSG is deployed on two VMs or physical servers provided by COSB as a Windows service. Each DSG accesses a subset of data sources. In addition, a DSG is hosted on a VM in the DEMS subscription to access the Axon API for BWV.

Setting	Value
Hosting DSG servers	PVM-SVR-000010 PVM-SVR-000011
DSG service account	

DSG VM REQUIREMENTS

See DSG release note.

CONNECTION TO DEMS

See the Site readiness document for general details.

The DSG connects out to endpoint hosted by DEMS in the Azure cloud. The DSG only initiates outgoing connections to these endpoints, no incoming connections are required.

DEMS endpoint	Address	Port
NICE DEMS DSG API	<TBD>.digital-olicing.co.uk	443
Microsoft Azure Storage (DMZ)		443

DSG CONNECTORS

This section contains the specific details of each connector at COSB

The connector configurations are defined in the COSB connector Integration Description Document. The sections below detail anything particular to the DSG or a connector that are not contained in the IDD.

NICHE RMS USERS' CONNECTOR

This Connector synchronizes the current Niche User logins with NICE DEMS, so that the users can use the same Username for login. It also informs NICE DEMS of the other identities that each user has, e.g., Collar number, Niche Person Id, Niche User Id, for matching users on other data sources.

CONNECTION

The Niche User Connector connects to an employee view populated from the Niche DB. This view is provided by COSB for use by NICE.

Setting	Value

Hosting DB server	
Hosting DB credential	

ITEM INDEXING

The Connector monitors the view "modified" datetime field for changes to the records and fields of interest within a time range. The records returned from the query are returned to DEMS to create/update the items it holds.

The connector runs once per hour to find changes.

BANDWIDTH

Each person record is typically between 1-2kB. Only updates to persons are sent to DEMS once per hour.

- Initial user ingestion = Number of Users * 1.5kB

- Ingestion rate = approx. 1 user per second => ~15kbit/sec.

OUTPUT

The provider generates/updates user records in NICE DEMS. Users' usernames are the same as their Niche users' User Id.

- Users are disabled in DEMS if their Person Classification is not "A" (not active). Users' emails are constructed by convention: <>@COSB .pnn.police.uk.

- Users' display names are constructed by the convention: <collar number> <family name>

- Users' passwords are NOT synchronized with Niche. Users must use the forgotten password feature to first access NICE DEMS.

MATCHING/CORRELATION

The Niche User Provider does not require specific matching/correlation rules.

ACCESS CONTROL

No Access Control is required for this connector.

RETRIEVAL

No media retrieval is required for this connector.

SUGGESTIONS

No suggestion rules are required for this connector.

DELETION

No deletion is required for this connector.

POINTS STILL TO BE RESOLVED

Where to get user details has not been decided. DEMS holds the different representations for a user required to correlate a user with a particular evidence item. DEMS will require the IDs for a user in the different data sources these include the Niche ID (number starting 150…), the officer's FIN or collar number, the officer's Niche UserID and the user's AD username. Where to get this information has not been decided.

NICHE RMS CONNECTOR

This Connector synchronises Occurrences and linked entities between Niche and NICE DEMS.

Occurrences ingested from Niche generate the Case folders into which all other digital media are attached. Associated entities are shown as lists within the details of the case with the exception of reports that are created as evidence items attached to the case.

- Most data is read from the Niche API. Other data is read from views and tables populated from the Niche DB.
- See the IDD for full details of the fields and records returned.

CONNECTION

The Niche RMS Connector retrieves information from two sources, the Niche RMS WebAPI, and additional DB all_ChangedIds_7d_vw view and ACLOccurrencesonNiche table provided by COSB for use by NICE.

Setting	Value
Hosting DB server	
Hosting DB port	1433
Hosting DB credential	
API server	
API port	80
API credential	
API domain	-

ITEM INDEXING

The Connector monitors all changed Ids. View for rows that have been added within a query time range. In addition, the connector performs a time based search on the Creation time for occurrences on the NicheWeb API for the same time range. Duplicate Ids are removed. The resultant list of Occurrence IDs is then used to perform detailed queries.

The details are returned to DEMS to create/update the items it holds. The connector runs once every 30 minutes to find changes.

BANDWIDTH

The bandwidth requirements are a combination of the metadata indexing for occurrences

and reports and the media retrieval for reports.

Occurrence metadata varies depending on the number of associated entities such as property or involved persons etc. A typical size is approx. 2kB for an occurrence with no associated entities to 50kB for an occurrence with 100 associated entities.

- Indexing rate = approx. 10 items per second.
- For an average item size of 20kB => ~2Mbit/sec. This is the burst rate until all items have been sent every half hour.
- Report media are uploaded in parallel with the occurrence indexing. Document uploads can be throttled.

For an average document size of 300kB and throttled to 5 documents every 10 seconds =>

~1.5Mbit/sec.

OUTPUT

The Connector generates/updates Case Folders within NICE DEMS based on the Occurrences. The type of occurrence is limited to just crime ("Niche '903...') from COSB with an Owning Agency of TBD.

The details of the Occurrence will contain the latest information for the following occurrence and associated entities:

- Occurrence basic details
- Involved Officers (With classifications of ARR, CAU, CHA, VDR, FWC, KHT, FPN, IUC, CM1, SUS, SUD, SUC, SVA, SUN, VOL, VIC, WIT)
- Associated Occurrences
- Court Folders
- Auxiliary IDs
- Addresses (With classifications of OLC, FDA, CSI)
- Persons (With classifications of ARO, SCO, IOF, OIC, WIT, INV)
- Vehicles
- Property (With classifications of DAM, EVD, REC, SWW, SEZ, STO, USD) The retrieved information is described in the IDD.

The Connector also uploads Documents from Niche into NICE DEMS that have been locked.

MATCHING/CORRELATION

Correlation rules cause metadata fields to be copied from one item to another based on a set of criteria to allow matching of the item to a case. The following correlations occur:

This Field	Is copied to this Field	When
Occurrence File Number	Case.MatchId	Always (populated by DSG claim)

Matching rules define when cases are created and when evidence will be added to cases, based on a set of criteria.

The following **case** matching occurs:

hen this Field	Is equal to this Field	The result will be
MediaType = Case And Media Subtype = RMS Record	-	Case created

The following **RMS** evidence matching occurs (for **Documents only**):

When this Field	Is equal to this Field	The result will be
Evidence.RMSID	Case.RMSID	RMS document evidence added to case.

ACCESS CONTROL

The hosted DB table ACL Occurrences on Niche contains a list of all occurrences that are ACL d or have been ACL d. The DEMS folder is then marked as Case Closed. This flag is used in the Access Control Policy to set user access to the case. See Security policy rules. •
If an occurrence is not available to the account used by NICE when querying the Niche API,

- then the occurrence is also marked as Case Closed.

- If any associated entity is not available to the account used by NICE when querying the Niche

- API it is removed from the details shown in DEMS.

If any report is not available to the account used by NICE when querying the Niche API, then the item is marked as ItemAclSet. This flag is used in the Access Control Policy to set user access to the item. See Security policy rules.

RETRIEVAL

Documents are retrieved from the Niche API and ingested into NICE DEMS when the document is matched to the case.

SUGGESTIONS

Suggestions are shown in the suggestions tab for a case and list other items in DEMS that might be related or useful for the current case. The items listed are ranked in an order of precedence based on configurable rules for each type of case or evidence item. Each rule can take the time and/or the location of the case or another evidence type within the case to find and rank the suggestion list. A match with either rule will return the item.

Cases are selected and ranked according to the following rules:

Type	Rule
Distance rule	Within 250 meters of current case location OR Within 250 meters of matched CAD record location
Time rule	Within 2 hours of current case StartTime

Setting	Value
API server	
API port	80
API credential	Fotoware Account and key, created by COSB
Archive(s)	

DELETION

Occurrences are ingested with their MOPI level as set in Niche. This is used as part of the deletion rules configured in NICE DEMS to set the retention of a case.

There are standard backstop rules configured as follows:

- NICE RMS media is deleted after xx years.

- NICE DEMS will purge RMS media records that are xx years old at midnight each night.

WRITE BACK EVENTS

The connector can listen for certain events from NICE DEMS and take action when those events are received:

POINTS STILL TO BE RESOLVED

- **How to get change data.** Change data is required to keep the metadata held in

- **DMS current.** The exact method to get this has not been defined.

- **Niche writeback not defined.** DEMS can write back to the Niche OEL and create property items on specific DEMS events. The events what to write back are undefined.

Event	Action

Case Created	OEL entry created
Evidence From New Connector	OEL entry created (not for Niche and CAD items)
Evidence Created	None
Evidence Deleted	None

FOTOWARE CONNECTOR

This Connector synchronises images between the Fotoware image repository and NICE DEMS.

The metadata is read from queries against the Fotoware FotoWeb API and ingested into " NICE DEMS. When it is matched to an Occurrence, the NICE item is 'added' to the occurrence case folder and the media retrieved via the API.

See the IDD for full details of the fields and records returned.

CONNECTION

The Fotoware Image Connector connects to the Fotoware FotoWeb API.

ITEM INDEXING

The Connector queries the API "uploaded" and "file modified time" datetime fields for changes within a time range. The records returned from the query are returned to DEMS to create/update the items it holds.

BANDWIDTH

The bandwidth requirements are a combination of the metadata indexing for Fotoware images and the media retrieval.

- Fotoware metadata is typically 2kB. Indexing rate = approx. 10 items per second.
- For an average item size of 2kB => ~200kbit/sec. This is the burst rate until all items have been sent every half hour.
- Media are uploaded in parallel with the indexing when an item is matched to an occurrence. Media uploads can be throttled.
- Assuming all images are matched and for an average document size of 10MB and throttled to 5 documents every 10 seconds => ~50Mbit/sec. This is the burst rate until all items have been sent every half hour.

OUTPUT

The Connector generates Image evidence items within NICE DEMS, for all items from configured Fotoware archives.

The details of the Incident will contain the latest information for the following items:

- Fotoware image asset details
- Fotoware image metadata details

The retrieved information is described in the IDD.

MATCHING/CORRELATION

Correlation rules cause metadata fields to be copied from one entity to another based on a set of criteria. **No correlations occur for Fotoware.**

Matching rules define when cases are created and when evidence will be added to cases, based on a set of criteria. The following **Fotoware** evidence matching occurs:

When this Field	Is equal to this Field	The result will be

Evidence.CADIDs (Fotoware)	Case.CADIDs	Fotoware evidence added to case.

The Fotoware CADIDs is extracted from the "TBD" field of the Fotoware record. If this number is not present, then no match can occur.

ACCESS CONTROL

There is no specific Access Control that is followed by the Fotoware connector.

The Access Control Policy defines how the images are accessed. See Security policy rules.

RETRIEVAL

The media is retrieved from the FotoWeb API when the Image item is matched to a case.

SUGGESTIONS

Suggestions are shown in the suggestions tab for a case and list other items in DEMS that might be related or useful for the current case. The items listed are ranked in an order of precedence based on configurable rules for each type of case or evidence item. Each rule can take the time and/or the location of the case or another evidence type within the case to find and rank the suggestion list. A match with either rule will return the item.

Fotoware Images are selected and ranked according to the following rules:

DELETION

Occurrences are ingested with their MOPI level as set in Niche. This is used as part of the deletion rules configured in NICE DEMS to set the retention of a case.

Type	Rule
Distance rule	Within 1km of current case location OR Within 1km of matched CAD record location
Time rule	Within 6 hours of current case StartTime OR Within 6 hours of matched CAD record StartTime OR Within 6 hours of matched CAD record EndTime

Fotoware records are deleted when their matched case is deleted. There are standard backstop rules configured as follows:

- NICE Fotoware media is deleted after xx years.
- NICE DEMS will purge Fotoware media records that are xx years old at midnight each night.

POINTS STILL TO BE RESOLVED

- Is the FotoWeb API or File share scanning to be used
- Is a datetime field mapped in Fotoware that updates if metadata is changed in Fotoware

CONTROLWORKS CAD CONNECTOR

This Connector synchronises Incident information between ControlWorks CAD and NICE DEMS.

The metadata is read from queries against the CAD DB and ingested into NICE DEMS. When it is matched to an Occurrence, the NICE item is 'added' to the occurrence case folder. The CAD record is used to match other items, such as BWV, into the occurrence as well.

There is an integration between ControlWorks and Niche so that if a Niche occurrence is

created the CAD incident number is pushed as a reference into the auxiliary Ids for the occurrence.

See the IDD for full details of the fields and records returned.

CONNECTION

The ControlWorks CAD Connector connects to the CAD reporting database.

Item indexing

Setting	Value
ControlWorks DB server	
ControlWorks DB port	1433
ControlWorks DB credential	

The Connector queries the database on the "modified" datetime fields for changes to the records and fields of interest within a time range. The records returned from the query are returned to DEMS to create/update the items it holds.

BANDWIDTH

The bandwidth requirements are a combination metadata indexing for CAD records and any media retrieval.

- CAD metadata varies depending on the number of dispatch comment entries. A typical size is approx. 30kB with 100 dispatch comments.

- Indexing rate = approx. 10 items per second.

- For an average item size of 30kB => ~3Mbit/sec. This is the burst rate until all items have been sent every half hour.

- CAD media are uploaded in parallel with the CAD record indexing. Media uploads can be throttled.

For an average media size of 1MB and throttled to 5 items every 10 seconds => ~5Mbit/sec. This is the burst rate until all items have been sent every half hour.

OUTPUT

The Connector generates CAD evidence items within NICE DEMS. In addition, DEMS case folders are created for specific CAD incidents based on the values of CAD fields such as the incident type. Typically, these CAD generated cases will be where a Niche occurrence will not be created.

The details of the Incident will contain the latest information for the following items:

- Incident basic details
- Events
- Linked incidents
- Units (units dispatched for the incident)
- Personnel (personnel dispatched for the incident including dispatched, arrival and cleared times)

The retrieved information is described in the IDD.

Additionally documents and images are indexed if the incident has a path set for retrieval from a file share.

MATCHING/CORRELATION

Correlation rules cause metadata fields to be copied from one item to another based on a set of criteria to allow matching of the item to a case. The following correlations occur for CAD:

This Field	Is copied to this Field	When
Case.MatchId (Which is equal to Niche Occurrence file Number)	Evidence.MatchId	Case.CADIDs = CAD.CADID (COSB CadRmsCADIDs)

Matching rules define when cases are created and when evidence will be added to cases, based on a set of criteria. The following **CAD** evidence matching occurs:

When this Field	Is equal to this Field	The result will be
Evidence.MatchId	Case.MatchId	CAD evidence added to case.
MediaType = CAD/RMS And Media Subtype = CAD Record	-	Case created

ACCESS CONTROL

he ControlWorks CAD DB indicates that an Incident has been secured when the *TBD* column of the *TBD* table is set to '*TBD*' for the incident. When the DSG reads this incident it is marked as ItemAclSet. This flag is used in the Access Control Policy to set user access to the item. See Security policy rules.

RETRIEVAL

Documents and images are ingested into NICE DEMS from a file share, when the CAD item is matched to a case. The incident contains a path to the file.

SUGGESTIONS

Suggestions are shown in the suggestions tab for a case and list other items in DEMS that might be related or useful for the current case. The items listed are ranked in an order of precedence based on configurable rules for each type of case or evidence item. Each rule can take the time and/or the location of the case or another evidence type within the case to find and rank the suggestion list. A match with either rule will return the item.

CAD records are selected and ranked according to the following rules:

Type	Rule
Distance rule	Within 250 meters of current case location OR Within 250 meters of matched CAD record location
Time rule	Within 2 hours of current case StartTime

DELETION

Occurrences are ingested with their MOPI level as set in Niche. This is used as part of the deletion rules configured in NICE DEMS to set the retention of a case.

CAD records are deleted when their matched case is deleted. There are standard backstop rules configured as follows:

- NICE CAD media is deleted after xx years.
- NICE DEMS will purge CAD media records that are xx years old at midnight each night.

AXON BWV CONNECTOR

TBD

NICE DEMS FIELD CONFIGURATION

The metadata displayed within NICE DEMS are customized to the needs COSB in the different views. The fields available from each data source metadata is detailed in the connectors IDD. The following data can be customized:

- User display name.

- Fields shown in the Case cards. Which fields to show, their alias (if any) and in which order.

- Fields shown in the Evidence cards. Which fields to show, their alias (if any) and in which order.

- Detail metadata views for each type of case and evidence item. Which fields to show, their alias (if any) and where in the panel.

- Field position in forms. (The name used is the same as the case or evidence alias.) The following sections detail the views for each item type.

USERS

The display name for a user can be customized from any of the user attributes available. The set username is: <Collar Number> <Surname>"

CARD LAYOUTS

The cards are the summary view of any item in DEMS in the case or evidence lists. They consist of 6 fields that can be displayed at once in two areas of the card known as the 'chip fields' and 'preferred fields. The fields can be given an order of precedence so that the top 6 fields available for an item will be shown. Those numbered 1 to 3 are chip fields those numbered 4 and above are preferred fields. For the preferred fields the first 3 fields with a value for the item are shown.

The configuration for the case and evidence cards is fully configurable via the System Admin portal.

DETAIL VIEWS

The detail views are shown when the 'Details' tab for a case or evidence item is selected.

Each type of evidence can have a different defined view, if an item does not match a specific view then a default is used for the media type.

Details views consist of one or more panels that can be used to group fields together. There are two types of panes for displaying individual fields, such as the item name, or lists, such as the list of occurrence addresses.

Each field panel can have a title and any number of available fields displayed in two columns. Each field can have an alias or use the alias applied for the cards, if configured. A field can be repeated in any panel.

Each list panel can have a title and a single list. The fields are shown as columns and which fields to show can be configured. Each field can have an alias.

Below the details views are defined for each item type with the label and in parentheses the fieldname the value is taken from. This field name can be referenced back to the source system in the IDD.

NICE Digital Evidence Management System

Requirements Traceability Document

This is Attachment A to Exhibit A – Requirement Traceability Matrix

(Section on Next Page)

Introduction

This document describes a list of basic checks that can be used to validate that the NICE DEMS system has been correctly installed and provisioned.

The NICE Data Source Gateway will be fully provisioned by NICE Professional Services and as such is not directly covered in the scope of this document (although it does cover the data sent by the DSG).

HOW TO USE THIS DOCUMENT

The following points should be noted while following this document:

- Some sections are optional
- NICE DEMS comprises a number of different portals and external connection, not all sections will be relevant to the COSB configuration.
- Certain functions will rely upon data being present in the system
- If a DSG is connected, then some sections will rely upon data having been sent from the DSG to NICE DEMS.
- If no DSG is connected, then a test Case and Evidence should be created to facilitate some of the tests.

Provisioning Verification

This section checks that the Data Source Gateway and DEMS provisioning has been completed and is operating as expected.

DSG CONNECTOR VERIFICATION

RMS Connector provisioned correctly [optional]

For each NICE DEMS entity ingested from the RMS data source (e.g. Cases, vehicles, property etc), ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	
Cases correctly created	Pass / Fail	Cases in DEMS are created correctly from underlying data source.
Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.

DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

CAD Connector provisioned correctly [optional]

For Evidence ingested from the CAD data source, ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	
Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.
DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

4.6   BWV Connector provisioned correctly [optional]

For Evidence ingested from the BWV data source, ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	
Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.
DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

4.7   Audio Connector provisioned correctly [optional]

For Evidence ingested from the Audio data source, ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	
Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.
DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

For Evidence ingested from the Photograph data source, ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	
Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.
DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

4.8 Interview Room Connector provisioned correctly [optional]

For Evidence ingested from the Interview Room data source, ensure that data is received and displayed correctly.

Result	Result	Comment
Data sent to DEMS	Pass / Fail	

Evidence items correctly created	Pass / Fail	Evidence items in DEMS are created correctly from underlying data source.
Evidence entities correctly matched to Case	Pass / Fail	Evidence items successfully matched to Case, where applicable.
Evidence media can be viewed/played	Pass / Fail	If the item has associated media.
Data in DEMS is as expected	Pass / Fail	Ensure data is correctly representing the underlying data source information.
Access control operating as expected	Pass / Fail	If COSB specific access control is configured, ensure it is operating as expected.
DSG "write back" to data source	Pass / Fail	If configured, ensure any data written back to the data source is correct.

Application Function

This section checks that NICE DEMS has been installed and is operating correctly.

NICE DEMS PORTAL OPERATION

NICE DEMS portal operating correctly

NOTE: Requires a login with suitable credentials to access DEMS Portal.

Result	Result	Comment
DEMS Login successful	Pass /	
Case list page is displayed	Fail	
User can reset their password	Pass /	
though the forgotten password link	Fail	
	Pass /	
	Fail	

Cases displayed in Case list

NOTE: Requires either a test case or case created by the DSG.

Ensure cases are displayed in the Case list.

Result	Result	Comment
Cases displayed in case list	Pass / Fail	

Cases displayed and details correct

NOTE: Requires either a test case or case created by the DSG and requires that evidence is contained within the case.

Open the case and ensure the details displayed are as expected and that evidence is shown.

Result	Result	Comment
Case opens	Pass / Fail	
Case details displayed as expected	Pass / Fail	
Evidence items are displayed as expected-	Pass / Fail	

66

Case can be downloaded	Pass / Fail	
Case can be shared via download	Pass / Fail	

4.9 Case shown on map view

NOTE: This requires that a Case has a location; either a valid resolved address entered by the user or should be a DSG created case that has location information.

Navigate to a case

Result	Result	Comment
Map tiles displayed	Pass / Fail	
Case displayed on map at correct location	Pass / Fail	

4.10 Evidence displayed and details correct

NOTE: Requires either a test case or case created by the DSG and requires that evidence is contained within the case.

Navigate to a case or multiple cases (either test case if previously created or case created by a DSG connector), open an evidence item of each type and check the details are as expected; if case and evidence creation is managed by the DSG, ensure all expected types are checked.

Result	Result	Comment
Evidence of each expected type displayed	Pass / Fail	
Evidence details display as expected	Pass / Fail	

4.11 Evidence item media display/replay

Navigate to a case (either test case if previously created or case created by a DSG connector), then to an evidence item; confirm that any media can be viewed or replayed correctly in DEMS.

Result	Result	Comment
Video item uploaded and playable	Pass /	
Image item uploaded and viewable	Fail	
Document item uploaded and viewable	Pass / Fail	
Evidence item can be downloaded	Pass /	
Evidence item can be shared via downloaded	Fail	
	Pass / Fail	
	Pass / Fail	

4.12 Evidence item map view

NOTE: This requires that an evidence item has a location; either a valid resolved address entered by the user, or should be a DSG item that has location information.

67

Navigate to a case and select the map view.

Result	Result	Comment
Evidence item displayed on map at correct location	Pass / Fail	

4.13 Searching

Navigate to the Search page, enter a valid search term that will return known results. Confirm that results are displayed.

Result	Result	Comment
Search page displayed	Pass /	
Items displayed correctly	Fail	
Search works with user entered text	Pass /	
Evidence can be added to case from	Fail	
search results	Pass /	
	Fail	
	Pass /	
	Fail	

4.14 Notifications

Configure specific notification settings (for portal and email) and make a change that will trigger a Notification to occur.

Result	Result	Comment
Notification displayed in DEMS Notification received in email	Pass / Fail Pass / Fail	

4.15 User Case creation [Optional]

NOTE: Perform this step if the user will be creating cases manually in the system, and it is acceptable to have a test case.

Create a test case, and check that it is created without error, and appears correctly in the case list, and search page.

esult	Result	Comment
Case created ok Details are as expected	Pass / Fail Pass / Fail	

Task 3. Security Planning

Contractor shall provide the following Security sub-tasks and deliverables:

Task 3. Security Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
3.1	System Security Management	Contractor shall provide a System Security Plan that describes the security approach for DEMS. In addition, because of the expected interactivity with other entities, a comprehensive plan shall explain how DEMS will respect and coordinate, when necessary, with the security constraints of other entities.	The System Security Plan shall address, at a minimum, the following areas: • General Information about System Environment, Interconnections/Information Sharing, Applicable Laws or Regulations, Information Sensitivity, Responsible Parties, General System Description • Security Controls pertaining to Risk Assessment and Management, User Rules or Behavior, Implementation Phase, Operation and Maintenance Phase • Technical Controls pertaining to User Identification and Authentication, Logical Access Controls, Audit Trails **The Deliverable shall include a DED.**
3.2	System Security not user security (ongoing – as changes are made)	Establish Patch management processes and procedures that are transferred to the County after successful completion of DEMS installation.	Provide documentation and training on system and patch management including regular maintenance, upgrades, and response to zero-day exploits.
3.3	Third Party Compliance Attestation (ongoing – annual)	Complete a third-party compliance review and provide attestation that security compliance controls are followed.	The Third-Party Compliance Attestation will address at a minimum: • What they did • What they remediated • The Vendor will remediate anything that is non- compliant at no cost to County

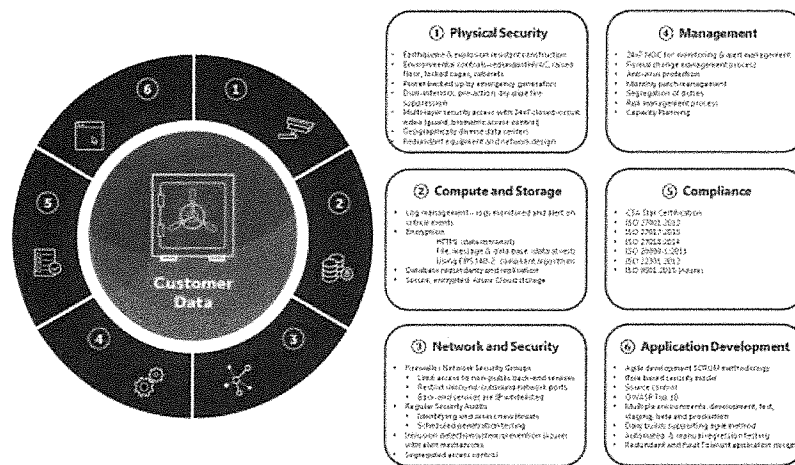# Deliverable Expectations: NICE System Security Plan

Project Deliverable Number:	Title of Deliverable: System Security Plan	
<Insert - TBD>		
Draft Submission Due Date:	County Draft Review & Comment Period:	
<Insert – TBD, as mutually agreed >	*<Insert - TBD>*	
Final Submission Due Date:	County Final Review & Comment Period:	
<Insert – TBD, as mutually agreed >	*<Insert - TBD>*	
Reviewed By Required:	Deliverable Document Format:	
<Yes/No – by whom –TBD as mutually agreed >	*< Word / PDF>*	
Deliverable Owner (County):	Deliverable Author (Vendor):	
<Name, Role – TBD, as mutually agreed >	*<Name, Role - – TBD, as mutually agreed >*	

Deliverable Description and Purpose:	
NICE designed NICE DEMS from the ground up with security in mind, with Microsoft Azure Government as NICE's cloud provider. The combination of NICE DEMS and the Microsoft Azure Government cloud offers law enforcement agencies a comprehensive, scalable, CJIS- compliant cloud-based investigative software solution for managing investigations, and storing and safeguarding digital evidence. The plan provides details of CJIS compliance.	

Deliverable Scope / Content Expectations:	
NICE will provide full documentation of Security related to your solution. The deliverables will include:	
CJIS REQUIREMENTS AND NICE DEMS STEP-BY-STEP COMPLIANCE	
13 POLICY AREAS	
CJIS AUDIT READINESS	
ANTIVIRUS, DATA BACKUP, PHYSICAL SECURITY	
SECURE EVIDENCE MANAGEMENT SECURITY MANAGEMENT	
ACCESS CONTROL AND USER AUTHENTICATION ACCESS TO EVIDENCE Sample	
Enclosed:	
NICE DEMS CJIS COMPLIANCE WHITE PAPER IS A STANDARDIZED DOCUMENT APPLICABLE TO ALL CUSTOMERS. IT WAS USED AS A SOURCE FOR THE INFORMATION PROVIDED HEREIN.	

References / Standards	FBI CJIS standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.	
Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above.	
	Rework Required: The document is substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.	
	Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.	

Security Management Plan

NICE designed NICE DEMS from the ground up with security in mind. And, this is why NICE chose

Microsoft Azure Government as NICE's cloud provider. The combination of NICE DEMS and the Microsoft Azure Government cloud offers COSB stakeholder agencies a comprehensive, scalable, CJIS-compliant cloud-based investigative SaaS solution for managing investigations, and storing and safeguarding digital evidence.

Details of the security designed into the NICE DEMS SaaS offering is provided in the following sections. At a high level, this Security Plan for COSB addresses all aspects of the DEMS solution including physical security, security of compute resources and storage, network security, security management, and security of the application development process. All security processes are in compliance with Industry Standards bodies guidelines.

NICE

PHYSICAL SECURITY

- Earthquake & explosion resistant construction
- Environmental controls–redundant HVAC, raised floor, locked cages, cabinets
- Pow er backed up by emergency generators
- Dual-interlock, pre-action, dry-pipe fire suppression
- Multi-layer security access with 24x7 closed-circuit video (guard, biometric access control)
- Geographically diverse data centers •   Redundant equipment and network design

COMPUTE AND STORAGE SECURITY

- Log management – logs monitored and alert on critical events
- Encryption
- HTTPS (data in transit)

— File, message, and database (data at rest)

— FIPS 140-2 compliant algorithms

- Database redundancy and replication

- Secure, encrypted Azure Cloud storage

NETWORK SECURITY

- Firewalls / Network Security Groups

- Limit access to non-public back-end services

- Restrict inbound/outbound network ports

- Back-end services are IP whitelisted

- Regular Security Audits are conducted

- Identifying and assess new threats

- Scheduled penetration testing

- Intrusion detection system/prevention (Azure) with alert mechanisms

- Segregated Access Control

SECURITY MANAGEMENT

- 24x7 NOC for monitoring & alert management

- Formal change management process

- Anti-virus protection

- Monthly patch management

- Segregation of SaaS duties with access controls

- Risk management process

- Capacity Planning

SECURE APPLICATION DEVELOPMENT

- Agile development SCRUM methodology

- Role based security model

- Source control

- OWASP Top 10

- Multiple environments: development, test, staging, beta and production

- Daily builds supporting agile method

- Automated & manual regression testing

- Redundant and Fault Tolerant application design

COMPLIANCE

- CSA Star Certification

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 20000-1:2011
- ISO 22301:2012
- ISO 9001:2015 (Azure)

Microsoft Azure Government – A Secure Foundation

Already used by more than a hundred government agencies, the Microsoft Azure Government platform is the trailblazer in the government cloud market. It was the first hyperscale infrastructure cloud platform contractually committed to meeting the FBI's Criminal Justice Information Services (CJIS) requirements for federal, state and local governments. The Microsoft Azure Government platform is inherently secure, as its use is restricted to qualified federal, state, local and tribal government agencies and their screened providers.

Additionally, Azure Government addresses the stringent security and compliance requirements for other key government regulations, such as the United States Federal Risk and Authorization Management Program (FedRAMP), the Department of Defense Enterprise Cloud Service Broker (ECSB), and the Health Insurance Portability and Accountability Act (HIPAA).[i]

Law enforcement agencies looking to take advantage of NICE DEMS's powerful digital policing and investigative capabilities delivered through the Microsoft Azure Government cloud platform can be confident in the solution's ability to protect sensitive case evidence.

This DEMS Security Plan outlines the many aspects of the integrated NICE DEMS/Microsoft Azure Government solution designed to keep your case evidence secure, while helping you comply with the FBI's CJIS requirements.

13 AREAS OF DEMS SECURITY CJIS: 13 KEY POLICY AREAS

The FBI Criminal Justice Information Services (CJIS) Security Policy includes a number of technical safeguards designed to protect and secure FBI Criminal Justice Information. But CJIS compliance is not just about technology, it's also about processes and people. Hosted software solutions cannot achieve CJIS compliance on their own merits; they must be operated within and by organizations that adhere to prescribed CJIS policies, processes and procedures.

The FBI defines 13 key areas that cloud service providers must address to be aligned with CJIS requirements which are summarized in more detail below.

More detailed information on these key policy areas can be found in the FBI CJIS Security Policy Resource Center on the FBI website at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

NICE has commissioned an independent consultant, Diverse Computing, Inc., whose team of Audit and Compliance Experts (ACEs) is working with NICE to ensure that NICE DEMS supports each of key FBI CJIS requirement areas.

ADDRESSING THE 13 KEY FBI CJIS POLICY AREAS

As noted above the FBI's Criminal Justices Information Services (CJIS) Policy covers 13 key areas which cloud service providers must address: 1) Information Exchange Agreements; 2) Security Awareness Training; 3) Incident Response; 4) Auditing and Accountability; 5) Access

Control; 6) Identification and Authentication; 7) Configuration Management; 8) Media Protection; 9) Physical Protection; 10) Systems and Communications Protection and Information Integrity; 11) Formal Audits; 12) Personnel Security; and 13) Mobile Devices.

The purpose of FBI CJIS security policies is to establish minimum security requirements to protect and secure various types of FBI Criminal Justice Information.

NICE not only adheres to these policies, it has taken a conservative approach (based on the recommendations of the International Association of Chiefs of Police) by applying CJIS policy to all data collected, analyzed and shared through NICE DEMS, including data that by definition falls outside of the scope of CJIS security policy.

More information on how NICE and Microsoft Azure Government address each of the key 13 policy areas is included in the detailed table in Appendix A, starting on page 18.

NICE's hosting partner, Microsoft, has already signed CJIS Security agreements in many states.

Upon request, NICE can provide documentation to show how NICE DEMS complies with your state's specific CJIS security requirements.

MINIMIZING OPEN FIREWALL PORTS AND SECURITY RISK

Your agency's firewall serves a vital purpose – it protects your trusted, secure internal network from outside security risks. The more ports (holes) you open on your firewall, the more vulnerable your network is, and the easier it is for hackers to penetrate holes in firewalls are also directional. Generally speaking, inward holes (that allow inbound connections) present a higher security risk than outward holes (that enable outbound connections between your network and some external source). Any nefarious individuals wanting to breach your network from outside need to find an inward hole to launch an attack.

For this reason, NICE DEMS *does not require any inward firewall holes* to access any systems on your network. All communications are initiated from within your network, outward to the NICE DEMS cloud, and those communications are encrypted.
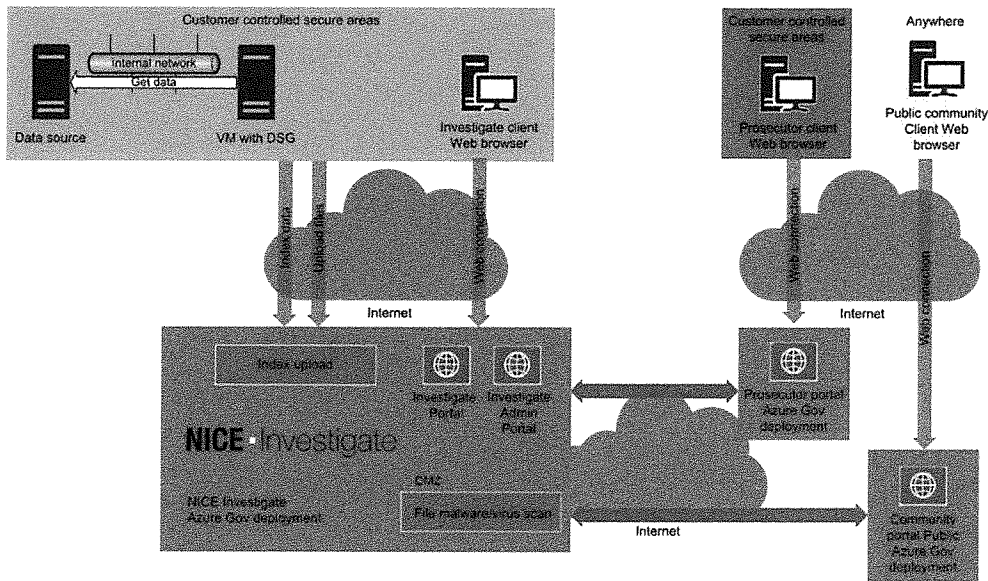
STRONG ENCRYPTION PROTECTS YOUR DATA

NICE DEMS ensures that all data in transit outside of secure areas is encrypted using TLS 1.2 256 bit encryption (FIPS 140-2 standard). Similarly, all case evidence that agency investigators share with prosecutors via NICE DEMS's Prosecutor Portal is secured by encryption as well. Data at rest is encrypted and secured by NICE's hosting partner, Microsoft, at ultra-secure data center locations within the Azure Government network.

Below is a schematic that illustrates this concept. It shows the agency secure areas and the Microsoft Azure Government cloud secure areas with encrypted data transfer between them. In addition, public and community-generated data (for example crowdsourced data or uploaded third party video) is stored in the Microsoft Azure public cloud, and is virus scanned before it's transferred to the Microsoft Azure Government cloud. This ensures that all information entering the Microsoft Azure Government cloud is virus-free and doesn't pose a danger to the secure system.

In this NICE DEMS solution architecture, the colored rectangles are secure, and the blue interconnects are encrypted.

Public uploads reside in the public cloud initially until they are transferred into a secure cloud via DMS and virus scan. The main blue rectangle – NICE DEMS – is where all stored data is encrypted.

LOCKING DOWN ACCESS TO SENSITIVE CASE EVIDENCE

• **Account Management, Access Enforcement and Access Control Criteria** – Only agency officials with administrator rights to NICE DEMS can establish and activate user accounts. If specific users leave the agency, or their roles changes, administrators can modify, disable, and remove those user accounts accordingly. NICE DEMS user rights/access privileges are based on a Policy-Based Access Control (PBAC) model. This model allows flexible rules to be created to configure security access for specific users and groups, based on their roles (e.g. homicide detective, etc.) and rights (owner of a case or contributor). Also referred to as Attribute Access Control, this feature of NICE DEMS allows administrators to also set up rules that control which material can be accessed by which users (compliant with NIST Special Publication 800-162).

• **Access Control Mechanisms** – Pre-established user rights in NICE DEMS dictate what cases and evidence items a user can access and the specific things the user can do (e.g. add evidence, create bookmarks, contribute comments, or simply view what's inside a virtual case folder). NICE DEMS also ensures that all data in transit is protected through encryption.

• **Unsuccessful Login Attempts** – The NICE DEMS system offers a customizable setting to automatically and temporarily lock a user out of his/her account following a pre- specified number of failed login attempts.

• **Session Lock** – Similarly, there is a customizable session timeout setting that will lock a user out after a pre-specified number of minutes of inactivity to prevent inadvertent viewing when a device is left unattended.

• **Remote Access & Publicly Accessible Computers** – Agencies can restrict access to defined IP ranges, so users can only access NICE DEMS from approved office locations.

Additionally, any device accessing NICE DEMS requires a X.509 device security certificate (this feature can be disabled where agencies have existing network access control systems in place), thus ensuring that NICE DEMS can only be accessed from authorized devices. Each agency can control which devices are issued certificates and limit access to only those mobile devices with suitable protection (e.g. encryption). All remote connections occur via an encrypted (FIPS 140-2 certified) path. All remote users accessing DEMS must be identified prior to access and authenticated prior to or during the session.

- **Identification and Authentication** – All users attempting to access NICE DEMS must have a valid user profile, and access to NICE DEMS is controlled by a user name / password combination, with FBI CJIS-compliant complex password enforcement rules. If required, NICE DEMS can also support two-factor authentication (also known as Advanced Authentication) in two manners. NICE DEMS supports two-factor authentication and single sign on by using your agency's ADFS SSO, or Active Directory Federation Services Single Sign-on, *which already provides two-factor authentication),* as the NICE DEMS login. When a user with an active profile in NICE DEMS signs on to ADFS, NICE DEMS will automatically transfer any claims assigned to the user from the ADFS to NICE DEMS. If your agency does not use ADFS SSO then NICE DEMS can support two-factor authentication in an alternate manner. As noted above, NICE DEMS provides agencies with the option to limit which devices access the service by means of client certificates. Clientside certificates can be used with TLS to prove the identity of the client to the server. As a second level of authentication, the user using the device would have to enter a valid user credential and password.

— Users, user groups, and user roles are created and managed in the DEMS Administration Portal by a COSB assigned DEMS System Administrator(s).NICE recommends a minimum of one System Administrator per Stakeholder Agency.

— Users can be created by synching with the county's Active Directory database. Rules and roles can also be obtained by interfacing with the county's Active Directory database or other identified HR database.

— Users access shall be authenticated using X.509 certificates and a username and password. IP whitelisting can also be implemented as required.

WORKING WITH INTEGRATIONS AND SECURITY ISSUES WITH 3RD PARTY VENDORS

There are several ways that NICE DEMS can collect information from your core systems. The first method is via integration API, where the vendor of the core system provides an API so that NICE DEMS can access the system in a manner approved by the vendor.

NICE DEMS can also pull data from read-only copies of databases, or database warehouses. This eliminates the need to interface with live production systems. NICE DEMS can also pull data from views provided on live databases.

Finally, NICE DEMS can pull data from file shares (for example folders containing crime photos). Agencies may choose to implement different methods for different core systems.

A successful implementation will require integrations with many data sources from different vendors. Each data source may bring its own security issues to be addressed. NICE will work with COSB and if necessary other vendors to work through these security issues to identify and deploy a solution.

SECURE EVIDENCE MANAGEMENT

NICE DEMS provides a baseline set of security controls providing appropriate protection against typical threats such as unauthorized access to the service; upload of malicious content to DEMS; unauthorized access and distribution of assets in DEMS.

All information is handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack.

- Hosted in the Microsoft Azure Government data centers. This cloud platform and application are CJIS certified and provide enhanced security policies for access control and maintenance.

- Encryption at rest of all collected digital evidence along with any metadata using strong AES256 encryption.

- Virus checking of all data uploaded to DEMS to protect against malicious content being uploaded.

- User access is via secure HTTPS browser connections with 2-factor authentication for login

- Attribute based access controls for accessing digital evidence

- Chain of custody reports proving the authenticity of collected evidence

PROTECTION FROM POTENTIAL OUTSIDE THREATS

The NICE DEMS platform is comprised of three main application portals: The Public Portal, the Investigation Portal and the Prosecution Portal.

The Public Portal allows citizens to electronically and securely share photos and video with police departments. It also provides businesses and residents with a virtual place to easily register their private CCTV cameras so that investigators have a better understanding of what cameras are located within the area of an incident. Knowing where the cameras are and who owns them, an investigator can send out an electronic request to have the video footage uploaded to the secure portal.

Crowdsourced evidence can offer some of the best leads in investigations. But because these files come from outside your secure network environment, they can contain malware or viruses, thus posing a threat to other secure digital evidence in the Microsoft Azure Government cloud.

NICE DEMS solves this problem by making sure that all crowdsourced public content is staged outside of the Microsoft Azure Government secure cloud, where it is automatically virus scanned. Only then can it be selected by a detective and uploaded to the secure Microsoft Azure Government cloud.

ADDRESSING ACCESS CONTROL THROUGH USER ROLES/RIGHTS

Policy-based Access Control Model

FBI CJIS Access Control Policy (5.5.2.1) notes that, in order to mitigate the risk to CJI, agencies should adhere to a "Least Privilege" approach which limits access to CJI to only authorized personnel with the need and the right to know.   Essentially this means that the agency should enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.

Limiting access to case evidence to those who have a need to know is absolutely critical. When evidence gets into the wrong hands it can compromise a case. Additionally, in high profile cases, prematurely disclosing evidence through the media can victimize a victim all over again.

NICE DEMS's user rights/access privileges are based on a Policy-Based Access Control (PBAC) model which restricts access based on a specific user's role within the organization, and his/her need to access specific data (e.g. as the owner of a case, contributor to a case, or supervisor). Access can be further restricted based on specific cases (e.g. homicide case ABC), or specific types of cases (e.g. all homicide cases).

77

NICE DEMS implements an attribute-based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know".

The control of access rights is established in DEMS via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.

It is also possible to create a connection to synchronize and inherit access control rules with COSB's existing records management system as a custom integration.

The NICE DEMS System Administrator is responsible for working with the NICE system engineer to implement access rules for users.

The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in DEMS.

User access to cases, evidence, and features within NICE DEMS is controlled by a Security Access Control Policy. Access control rules shall be defined by COSB during the Planning Phase of the project.

LOCKING DOWN SENSITIVE CASE FILES

In many states, there are laws governing confidentiality for cases involving certain types of crimes, particularly those involving children/juveniles and sex crimes. High profile cases involving celebrities may also be sensitive.

Case owners have the ability to mark any case they are managing as 'sensitive.' This will lock down the case, restricting access solely to the case owner. So even if the agency had designated all homicide detectives as contributors to all homicide cases, they would not be able view or contribute to any cases marked as 'sensitive' based on the NICE DEMS user access rules engine.

Finally, individuals from the subscribing agency can also be designated as administrators of the NICE DEMS system. Administrators are able to add users to the system, assign roles and rights, change roles and rights, and delete users. Police departments are highly dynamic environments and it's not uncommon for investigators to transfer in or out, or even transition to other divisions with completely different geographies. NICE DEMS enables your administrator to update user roles and rights as needed.

SHARING EVIDENCE WITH EXTERNAL USERS

The final step in the process of building a case typically involves sharing the case and its evidence (or in the early stages portions of the collected evidence) with a prosecutor for case direction advice, and ultimately for filing consideration. In NICE DEMS this is done through the Share Portal.

As a registered user, external users such as outside counsel can log in to the Share Portal and set up a user name and password to view all shared evidence.

NICE DEMS users can share entire cases or selected case evidence with external users by emailing a link to a secure portal which they can then open and review. NICE DEMS internal users can choose to include or withhold the "Download" option for evidence shared to external users.

Finally, all user activity on the NICE DEMS system, involving both internal and external users, is thoroughly tracked by NICE DEMS and can be audited if necessary.

PROTECTING CHAIN OF CUSTODY

In a legal context, chain of custody refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

To maintain chain of custody, you must preserve evidence from the time it is collected to the time it is presented in court. To prove the chain of custody, and ultimately show that the evidence has remained intact, prosecutors generally need service providers who can testify: 1) that the evidence offered in court is the same evidence they collected or received; 2) to the time and date the evidence was received or transferred to another provider; 3) that there was no tampering with the item while it was in custody.

A chain of custody ensures that the data presented is "as originally acquired" and has not been altered prior to admission into evidence.

Chain of custody is especially important for electronic evidence because it can be more easily altered.

Chain of custody is the foundation the prosecution needs to establish for certain types of exhibits to be admitted into evidence. Defense strategies often rely on bringing the chain of custody into question. If the strategy's successful, the case could be compromised or thrown out.

Whether physical or digital evidence, it's essential to track chain of custody. Today, when physical evidence is booked into the evidence room, all the details surrounding who recovered it, where, when, etc., are entered, documented and tracked in your agency's evidence tracking system. Digital evidence copied onto CDs, DVDs or USB drives is handled the same manner.

NICE DEMS does not replace your evidence tracking system for logging and tracking physical evidence, but it does simplify the process of handling and securing digital evidence and tracking its chain of custody. Here's how.

Instead of copying digital evidence onto CDs, DVDs, and USB drives, and locking it in an evidence room, with NICE DEMS, digital case folders and their digital evidence contents are securely stored in the Microsoft Azure Government Cloud.

The NICE DEMS system automatically tracks whenever any authorized system users access a digital case folder or any of its digital evidence contents in an event log. It also tracks what they did and when they did it – for example if they viewed a piece of evidence, downloaded it, copied it, annotated it, or shared it, and even who they shared it with.

The chain of custody event logs can be viewed online or printed in a report format for court if needed. Only someone who has been assigned access to a case (e.g. case owner or contributor) can access the chain of custody report for an evidence item in the case.

NICE DEMS's chain of custody event logs are tamper-proof. Event logs are protected by block chains which link and lock data (for each instance where evidence was viewed /touched/etc.) to the next instance in a chronological sequence. This ensures chain of custody event logs can't be edited.

Furthermore, when digital evidence is added to DEMS NICE, there is no way for an investigator to edit or modify the original digital evidence. Instead, NICE DEMS creates working copies of the evidence that the investigator can work with as he/she builds the case. For example, an

investigator can insert comments, redact video/audio, and annotate working copies of digital evidence. NICE DEMS tracks chain of custody for all working copies, as well as tracking the chain of custody for the original digital evidence.

DETAILED AUDIT TRAILS AND ACTIVITY LOGS

The FBI Criminal Justice Information and other sensitive evidence used in investigations can be highly sensitive and confidential. Your agency must be able to audit exactly who has accessed data, when, how, and for what purpose.

NICE DEMS's Chain of Custody function tracks all user actions related to a digital case folder or any of its digital evidence contents to ensure evidence integrity. The NICE DEMS Audit Trail, on the other hand, tracks and logs *all* activity on the system.

CJIS Security Policy (5.4.1 Auditable Events and Content - Information Systems), specifies that audit records must be generated and logged for specific types of events, including:

- Successful and unsuccessful system log-on attempts;

- Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource;

- Successful and unsuccessful attempts to change account passwords;

- Successful and unsuccessful actions by privileged accounts;

- Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

NICE DEMS automatically logs and maintains a record of all of these activities. These records can be reviewed by a designated administrator or security officer within the agency.

This individual can review the audit records to look for indications of inappropriate or unusual activity or to DEMS suspicious activity or suspected violations, and then report their findings to appropriate officials, who can then take necessary actions. According to CJIS Security Policy 5.4.3 (Audit Monitoring, Analysis and Reporting), this audit review/ analysis should be conducted at a minimum once a week.

If a security concern comes up outside of the ongoing audit review/analysis process, a designated security officer with proper system access can use NICE DEMS 's audit logs to retrace any related activity necessary to complete his/her investigation.

CJIS Security Policy 5.4.5 (Protection of Audit Information) also stipulates that the audit information should be protected from modification, deletion and unauthorized access. NICE DEMS's audit logs are secured in a password-protected database with no way for users to edit the logs.

CJIS AUDIT READINESS

As noted above, agencies with access to FBI CJIS systems and information are subjected to formal audits. NICE DEMS tracks and logs all user activity and provides audit trail reporting that can help your agency demonstrate its compliance with specific CJIS requirements.

For example, one CJIS requirement states that user accounts be disabled when a user is no longer employed with the agency. Your agency can use the NICE DEMS audit trail to demonstrate that the user's account was disabled on the day that individual left the organization.

The audit log can also demonstrate that all required auditable events (per CJIS 5.4.1) have in fact been logged.

ANTIVIRUS SOFTWARE AND OTHER BUILT-IN PROTECTION MECHANISMS

As noted earlier, NICE DEMS leverages both the Microsoft Azure "public" and Microsoft Azure Government clouds to manage data at various stages of an investigation. NICE uses third-party anti-malware software to scan, identify and remove viruses, spyware and other malicious software and provide real time protection. All data is virus scanned before it is transferred to a secure area.

Other built-in protection mechanisms include:

- **Automatic & transparent security updates** – As your Software as a Service (SaaS) providers, NICE and its hosting partner, Microsoft, are responsible for managing all software and security updates. Integrated deployment systems manage the distribution and installation of security patches.

- **Intrusion detection & DDoS** – To protect the Microsoft Cloud, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the continuous monitoring and penetration-testing processes of Azure. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks.

- **Penetration testing** – NICE and its hosting partner Microsoft conduct regular penetration testing to improve NICE DEMS security controls and processes. By constantly challenging the security capabilities of the service, NICE stays ahead of emerging threats.

DATA BACKUP AND INHERENT DISASTER RECOVERY

NICE's hosting partner, Microsoft, protects your agency's data through Geo-Redundant Storage (GRS) which replicates the data across two geographically distributed Microsoft Azure Government datacenters (located over 500 miles apart). Geo-replication ensures the digital evidence crucial for investigations will always be available, even in the most unpredictable of circumstances. This level of disaster recovery is difficult if not impossible for most individual agencies to achieve on their own.

In addition to ensuring business continuity, there are other inherent advantages to using a Software as a Service Provider instead of self-hosting on-site, including: fewer headaches *(think of endless rolling hardware upgrades; and the additional real estate, operational, maintenance, and security costs/challenges that come with managing your own data center)*, and think about paying for everything up front vs. the ability to "pay as you go," and only for what you need.

STATE-OF-THE-ART PHYSICAL SECURITY

Finally, the Microsoft Azure Government data centers are physically constructed, managed, and monitored to protect data and services from unauthorized access and other threats, via:

- **24-hour monitored physical security** – Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

- **Monitoring and logging** – Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.

81

- **Security** – Datacenters are secured using physical, logical and procedural controls. Important controls include secured access control to the datacenter, second person screened escorts, aisle cameras, and secured cabling. All security controls are audited and logged.

- **Screened personnel** – Operations and support are performed by personnel in the United States, who have been background screened.

- **Continental United States** – All COSB data, content, and organizational data (both at rest and in transit); all hardware, networking and other physical infrastructure; and all personnel reside in the Continental United States (CONUS).

PLANNING TOGETHER FOR A SECURE SERVICE OFFERING

Digital evidence is growing every day and becoming increasingly difficult for police departments to manage. The combination of NICE DEMS and the Microsoft Azure Government cloud can provide your County Agencies with a comprehensive, scalable, CJIS- compliant cloud-based investigative software solution for managing investigations, and storing and safeguarding digital evidence.

This DEMS Security Plan has detailed the many aspects of the integrated NICE DEMS/Microsoft Azure Government solution designed to keep your case evidence secure, while helping your agency comply with the FBI's CJIS requirements.

During the Project Planning Phase, the DEMS Security representative will review this information with the designated COSB Security representative(s) to ensure a through understand of all security aspects of the DEMS SaaS solution. Areas of concern with respect to potential gaps in this security plan will be documented, mitigation plans will be developed and tracked to resolution.

NICE has included a Security Test Plan from a previous customer project to show the various security aspects tested prior to system turnover to COSB.

Task 4. Systems Integration Expectations

Contractor shall provide an overview of integration capabilities and inventory of interfaces available with DEMS. Contractor shall work with the County to identify existing APIs or other methods for DEMS to receive or provide data for each DEMS interface.

For each DEMS interface, Contractor shall provide API(s) or other method(s) for DEMS to provide data to or receive content from the integrated application. As appropriate, Contractor shall extend DEMS to provide the required functionality, including working directly with the interfacing application to design, develop and test direct interfaces. County shall provision services from third party providers of the interfacing systems, if support activities or third-party system modifications are required. Contractor shall additionally support County testing of all interfaces.

NICE is developing an Enhanced API that provides additional functionality that is currently not available to customers in Production. Once the Enhanced API is developed and available for customers, COSB developers will develop an integration with Box.com using the Enhanced API and work with NICE support to build out the required Box.com integration (Item #15 on Attachment A – RTM, Integrations Tab).

COSB reserves the right to continue with the Public Defender implementation if the Box.com integration meets the following requirements:

1. The integration is running in a Production environment and supported currently by NICE

2. The integration is able to transfer the required data to and from Box.com, placing the information in the specific location within a case file in Box.com and following the desired naming convention by the Public Defender's office.

3. Perform the transfers in line with COSB's Public Defender's requirements included as Attachment D Box.com Integration Functionality Requirements

Contractor shall provide the following System Integration sub-tasks and deliverables:

Task 4. Systems Integration Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables

4.1	Systems Integration Management	Contractor shall provide a Systems Integration Plan that describes the integration and interoperability approach for DEMS. In addition, because of the expected interactivity with other entities, a comprehensive plan shall explain how DEMS will respect and coordinate when necessary within the constraints of other entities.	The Systems Integration Plan shall address, at a minimum, the following areas: • General Information about System Environment, Interconnections/Information Sharing, Information Sensitivity, Responsible Parties, General System Description • Business processes and workflows between systems • System capabilities for validation, transformation and routing of information and data • Adherence to and integrity of security requirements across systems • Interface and Protocol Management (APIs, WebServices, etc.), Enterprise Adapters, Semantic Mapping, File Transfers, Data Federation and Replication, Message and Event Generation and Brokering • Contractor shall ensure accurate design and function, and where needed, to allow DEMS to accept case content **The Deliverable shall include a DED**.
4.2	Interface Design	Contractor shall provide interface design services by providing API(s) or other methods for DEMS to provide and receive data from stakeholder agency/department systems.	For each interface, the Interface Design Document shall include (at a minimum): • Integration flow • DEMS adapter/connector type (e.g., web service, file, etc.) • Interface content (field level) • Interface trigger event or frequency • Validations and exception processing • Testing considerations • Security needs/requirements **The Deliverable shall include a DED.**
4.3	Complete System Interfaces and Integrations	Contractor shall build the system integrations specified in the Systems Integration Plan.	A Notice of Completion shall at minimum provide a list and description of all completed interfaces. **The Deliverable shall include a DED.**

Deliverable Expectations Document:
NICE Systems Integration Management Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Systems Integration Management
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*

Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
A key part of the NICE DEMS Project Planning Phase are the technical discovery sessions that are held with COSB.   During these sessions, representative subject matter experts from COSB meet with NICE technical personnel to discuss and document data migration requirements from existing COSB databases to NICE DEMS. Requirements identified from these sessions are documented in an Integration Design Document (IDD) which serves as the Systems Integration Management Plan. There will be a detailed list of requirements that will be documented and agreed to for each project integration. The IDD is then used by the NICE DEMS R&D team when developing the DEMS DSG connectors.

Deliverable Scope / Content Expectations:
NICE will provide full integration management documentation including integration design for a comprehensive collection of integration parameters and their delivery for agencies in scope of this Agreement. The deliverables will include: • NICE DEMS SYSTEMS INTEGRATION MANAGEMENT PLAN o DATA CONVERSION AND DATA MIGRATION PLAN o INTEGRATION DESIGN DOCUMENTATION   • INTERFACE DESIGN AND INTEGRATIONS PLAN Sample Enclosed: SAMPLE INTEGRATION DESCRIPTION DOCUMENT

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above. Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

NICE DEMS Systems Integration Management

FLEXIBLE INTEGRATION OPTIONS

NICE DEMS's flexible integration options put your agency in control. For police investigators, evidence collection is a very manual and tedious process. It typically involves logging on to a dozen or more systems. NICE DEMS streamlines this process by providing a one- stop shop for gathering evidence – the investigator doesn't have to spend time logging on to all of the individual systems, such as CAD or RMS, to gather evidence.

NICE DEMS can do the work for the investigator because it's able to connect to and collect

data from your agency's siloed systems.

NICE DEMS has been uniquely designed to require minimal end user action for evidence collected and managed in the platform. A NICE DEMS Data Source Gateway (DSG) is installed on the Agency Network and provides the secure connection point between any local electronic data sources, (e.g. CAD, Records, 911 recordings), and the NICE DEMS cloud service. It uses a selection of custom integrations, for searching and retrieval of the metadata and media from each individual data source.

Once the NICE DEMS DSG connectors are properly configured and connected to data sources, no further intervention from the end user is required. NICE DEMS case folders are automatically created through an integration with the agency's RMS. All data ingested into NICE DEMS is automatically populated with the applicable metadata.

There are several ways that NICE DEMS can collect information from your core systems.

- The first method is via integration API, where the vendor of the core system provides an API so that NICE DEMS can access the system in a manner approved by the vendor.

- NICE DEMS can pull data from read-only copies of databases, or database warehouses. This eliminates the need to interface with live production systems.

- NICE DEMS can pull data from views provided on live databases.

- NICE DEMS can pull data from file shares (for example, folders containing crime photos).

Agencies may choose to implement different methods for different core systems.

Data Conversion and Data Migration Planning and Tracking

A key part of the NICE DEMS Project Planning Phase are the technical discovery sessions that are held with COSB.

During these sessions, representative subject matter experts from COSB meet with NICE technical personnel to discuss and document data migration requirements from existing COSB databases to NICE DEMS. Requirements identified from these sessions are documented in an Integration Design Document (IDD). There will be a detailed list of requirements that will be documented and agreed to for each project integration. The IDD is then used by the NICE DEMS R&D team when developing the DEMS DSG connectors.

The following shows an IDD detailing the data migration requirements of 911 call recordings from a customer's NICE Inform database to NICE DEMS. As, you can see, IDDs are very detailed and specific in nature. NICE documents every data field that will be migrated and show how it will be used and shown in NICE DEMS. (See the attached IDD for details on all integrations for the project)

All IDDs must be reviewed and approved by COSB SMEs before any connector development work can begin.

Deliverable Expectations Document: NICE Interface Design Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Interface Design Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
The Interface Design Plan includes a list of all planned integrations as well as the purpose of each integration, methodology of data collection, as well as the description of access to such information. A full list of integrations and details of each integration and the data to be collected will be defined in the NICE DEMS Solution Design document that is created during the technical design phase of the project.

Deliverable Scope / Content Expectations:
NICE will provide a complete document relevant to Interface Design Planning related to the agreed upon solution. The deliverables will include: •   DETAILED INTERFACE DESIGN PLAN •   INTERFACE DESIGN SUB-PLAN FOR EACH INTEGRATION Sample Enclosed: SAMPLE INTEGRATION DESCRIPTION DOCUMENT

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above. Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

Interface Design

Following is an example list of commonly supported integrations – it is not comprehensive but provided only to illustrate the solution's flexibility.

A full list of integrations and details of each integration and the data to be collected shall be defined in the NICE DEMS Solution Design document that is created during the technical design phase of the project.

DEMS INTEGRATION TO RMS

This shall be a direct integration to a copy of the COLBALT RMS SQL database to provide RMS case information and incident details in DEMS. It shall be a one-way integration, reading information from the Cobalt RMS. This shall be a synchronized connection, updating in real time as information is updated in the Cobalt RMS.

The NICE Integration shall provide:

- The ability for NICE DEMS to create a digital case folder based on the creation of a case folder in the Cobalt RMS.

- The ability for NICE to extract key incident related information such as CAD incident ID, RMS case ID, incident type, status information, etc and populate key information in the DEMS case folder.

- The ability to search all key information in the Cobalt RMS database from within NICE DEMS

NICE DEMS INTEGRATION TO CAD

This shall be a direct integration to a copy of MPD's Intergraph CAD SQL structured database to provide CAD incident information in DEMS. It is a one-way integration, reading information from CAD. This shall be a synchronized connection, updating in real time as information is updated in the CAD.

The NICE Integration shall provide:

- The ability for NICE to extract key incident related information such as CAD incident ID, dispatched officers, incident type, etc and populate key information in the DEMS case folder.

- A CAD incident summary report generated from the available CAD information and included in the DEMS case folder.

- The ability to search all key information in the CAD database from within NICE DEMS

- Police reports collected from the RMS and added to DEMS case folders

NICE DEMS integration to BWV & INTERVIEW ROOM RECORDINGS

This integration provides BWV meta-data and media to NICE DEMS. It is a read-only integration. The DSG connector shall integrate directly with the Axon database via a customer provided API or via direct access to the SQL database.

BWV records are matched to the NICE DEMS Case using the CAD incident ID or by using data from the CAD incident to determine incident time and dispatched officers, this is then correlated to the BWV camera owner at the incident time.

Interview room recording shall also be collected via this integration. Metadata tagging associated with the Interview Room recordings will be used to correlate and match the recordings with the proper DEMS case folders.

This shall be a synchronized connection, updating in real time as information is updated in the Axon database.

NICE DEMS INTEGRATION TO CRIME SCENE PHOTOS DATA STORE

This integration shall support the collection of crime scene photos that are currently stored in

MPD's DIMS. The photos shall be placed into the appropriate DEMS case folders based on the metadata provided in DIMS which identifies the MPD case. This shall be a synchronized connection, updating in real time as information is updated to DIMs.

<u>NICE DEMS integration to 911 call recording platform</u>

This integration provides the 911 call audio and meta-data to NICE DEMS. It is a read- only integration. CAD Incident information is used to locate matching calls and place in the associated NICE DEMS case folder.

<u>Lessons learned from other conversions and data migrations</u>

A critical part of any project is completing a session on Lessons Learned. This is where the team members discuss what worked well and what areas of the process need improvement. This step is critical because it provides the foundation for continuous improvement as NICE moves forward in their customer/vendor relationship as well as for other customer deployments. It is also important to note that the initial customer deployment is often just the beginning, as projects are typically multi-year commitments. So, continual improvements guarantee NICE's commitment to COSB that your overall satisfaction is NICE's number #1 priority. Examples from Previous Projects, Resolutions and Lessons Learned

- **Accessing database structure or needed API for data connectors**

  The challenge NICE identified is that some data/media source vendors do not support open access to data stored in their platforms or the database structure is not known by COSB. In such cases, vendor involvement is required to support the NICE Investigation integration.

- **Lessons & Mitigation** – Early in the project, NICE will request copies of the database structure or copy of the APIs for each database to which NICE DEMS will connect. This improves the quality of planning for integration phases of the project and provides visibility into needed actions that can be handled concurrently with other tasks, as well as their prioritization.

- **Hidden, inaccessible data in customer database/s**

  Another challenge was limited or lacking customer clarity concerning technical requirements for data access. Not all data required by COSB was actually exposed by the COSB database to NICE's data connector. This caused weeks of schedule delay and required rework for both COSB and NICE project team.

- **Lesson & Mitigation** – NICE have increased the granularity of data tracking in IDD documentation. NICE now requires mitigation checkpoints with COSB during connector development, with proactive field-by-field analysis.

Sample Integration Description Document

Integrations		Sample Integration Description Document

		System	Interface	Notes
Vendor				A consolidated view of all the IDDs of the required Integrations for Customer solution
Versions				

DSD version	2.4

Revision	3/13/2019

Purpose	A record of all the details of the case within the RMS.						
Provider template	RmsDataProvider/RmsOccurrenceDataProviderEvidencePerInvolvement	Investigate		Data source			Comments
Base Record	Description	Investigate claim	Native claim	Dataset	Entity	Field	
							Only return '903' occurrences AND Occurrence_

							_OwningAgency = 'NWP'
Fields							
Unique ID	An ID in the record that is unique to the record and can be used to link the CAD collections to this base record.	id Hash of the value	Occurrenceld	Occurrence	Occurrence	Occurrence__Id	
Name	A field or fields that are used to create a readable name for the record	name		Occurrence	Occurrence	Occurrence__Occurrence FileNoG	
Incident date	The date and time of the incident for which the RMS record was created.	StartTime If StartTimeTZV2G != null then	StartTimeTZV2G	Occurrence	bsl_nice_occurrence	Occurrence__StartTimeTZV2G	Field is Local time
		StartTimeTZV2G else ReportedTimeTZV2G	ReportedTimeTZV2G	Occurrence	bsl_nice_occurrence	Occurrence__ReportedTimeTZV2G	Field is Local time
RMS ID	The ID or number of the case or RMS record so that other records can be linked to the RMS case.	RMSID		Occurrence	Occurrence	Occurrence__OccurrenceFileNoG	
Update date/time	A field or fields that can be monitored to detect if the record has been updated. The provider will send a new copy of the record if one of the monitored dates falls within the continuous search window.	UpdateDate	TriggerTime	Database: RMSRepl	View: ChangedIds_vw	TriggerTime	Obtained from the ChangedIds database view for forward search

92

			CreTime	Occurrence	Occurrence	Occurrence__CreTime	For backwards search
Case status	The status of the case	Status		Occurrence	Occurrence	Occurrence__UCRClearanceStatusG	
Case type	The type of case	CaseType		Occurrence	Occurrence	Occurrence__OccurrenceType	
Assigned officer	The officer assigned to the case. This is used to map to a user within Investigate as the case 'owner'	owner Set to "Unknown" if no person matches OIC		GOccInvGPerson;GPerson	GPerson Select person where GOccInvGPerson__Classification contains: OIC	GPerson__Id	Value is converted to the Investigate login username
Assignment date	The date and time the officer was assigned to the case.	AssignmentDate		GOccInvGPerson;GPerson	GOccInvGPerson Select person where GOccInvGPerson__Classification contains: OIC	GOccInvGPerson__CreTime	
Deleted	A flag to indicate if the item was deleted from the data source or access removed		Deleted Set to "1" if the entity is not returned from API query	Occurrence	Occurrence		Inferred from whether any data is returned when querying for an occurrence

93

	the case according to the status is closed)						TimeTZV 2G	
ReportedDate	The date and time the of the incident was reported for the occurrence		ReportedTim eTZV2G	Occurrence	Occurrence	Occurren ce__Rep ortedTim eTZV2G	Field is local time
DateEntered	The date and time the occurrence was created		CreTime	Occurrence	Occurrence	Occurren ce__CreT ime	
Summary	A summary for the occurrence	Summary		Occurrence	Occurrence	Occurren ce__Sum mary	
Remarks	Any remarks for the occurrence		Remarks	Occurrence	Occurrence	Occurren ce__Rem arks	
Matching field	A field that can be copied to correlated records to further copy to correlated records so they match to the case	MatchId		Occurrence	Occurrence	Occurren ce__Occ urrenceFi leNoG	
Label			Label	Occurrence	Occurrence	Occurren ce__Lab el	
ChangedId	The ID that triggered the occurrence update		ChangedId	Database: NicheRMSR epl	View: ChangedIds_ vw	ChangedI d	Obtained from the ChangedIds database view for forward search
Contributing Officers Collection	(optional) The list of contributing officers to the case		nicheInvestig atingPersons				

Fields							
Unique ID	An ID in the record that is the same as the unique ID from the RMS base record.		OccurrenceId	GOccInvGPerson;GPerson	GOccInvGPerson	GOccInvGPerson__LId	
Case relation	The field or fields that contain information about how the officer is related to the case.			GOccInvGPerson;GPerson	GOccInvGPerson	GOccInvGPerson__Classification	Only return rows where GOccInvGPerson__Classification CONTAINS (ARO, SCO, IOF, OIC, WIT)
			LinkClassificationG	GOccInvGPerson;GPerson	GOccInvGPerson	GOccInvGPerson__ClassificationG	
Associated date/time	The date and time this record was associated		LinkCreTime	GOccInvGPerson;GPerson	GOccInvGPerson	GOccInvGPerson__CreTime	
Officer name	Field or fields that identify the officer.		PersonId	GOccInvGPerson;GPerson	GPerson	GPerson__Id	Value is converted to the Investigate login username
			PersonEmployeeNumber_cache	GOccInvGPerson;GPerson	GPerson	GPerson__EmployeeNumber_cache	
			PersonLabelEmployClassificationG	GOccInvGPerson;GPerson	GPerson	GPerson__LabelEmployClassificationG	

95

			PersonLabel Name	GOccInvGPe rson;GPerso n	GPerson	GPerson _LabelN ame	
Person's unit	The unit the person belongs to		PersonLabel Unit		GPerson	Gperson_ _LabelUn it	
Associated Cases Collection	(optional) The list of associated cases		nicheAssocO ccurrences				
Fields							
Unique ID	An ID in the record that is the same as the unique ID from the RMS base record.		OccurrenceId	GOccAssoc GOcc;Occurr ence	GOccAssoc GOcc	GOccAss ocGOcc_ _Lid	
Case relation	The field or fields that contain information about how the officer is related to the case.		LinkClassific ationG	GOccAssoc GOcc;Occurr ence	GOccAssoc GOcc	GOccInv GPerson __Classifi cationG	
Associated date/time	The date and time this record was associated		LinkCreTime	GOccAssoc GOcc;Occurr ence	GOccAssoc GOcc	GOccAss ocGOcc_ _CreTim e	
AssociatedCas eID	Internal or other unique ID of the accociated case		AssocOccurr enceId	GOccAssoc GOcc;Occur rence	Occurrence	GOccurre nce__Id	
RMS ID	The ID or number of the associated case or RMS record.		AssocOccurr enceFileNoG	GOccAssoc GOcc;Occur rence	Occurrence	GOccurre nce__Oc currence FileNoG	
Creation date/time	The date and time the RMS record was created.		AssocOccurr enceCreTim e	GOccAssoc GOcc;Occur rence	Occurrence	GOccurre nce__Cr eTime	

96

Case type	The type of linked case		AssocOccurr enceType	GOccAssoc GOcc;Occur rence	Occurrence	GOccurre nce__Oc currence Type	
Description	A description or summary of the associated case		AssocOccurr enceLabel	GOccAssoc GOcc;Occur rence	Occurrence	GOccurre nce__La bel	
Associated Court files collection	(optional) The list of associated court files		nicheCaseFil es				
Fields							
Unique ID	An ID in the record that is the same as the unique ID from the RMS base record.		OccurrenceId	CFlvGOccur rence;Court Folder	CFlvGOccurr ence	CFlvGOc currence_ _RId	
Associated date/time	The date and time this record was associated		LinkCreTime	CFlvGOccur rence;Court Folder	CFlvGOccurr ence	CFlvGOc currence_ _CreTime	
Court Folder ID	Internal or other unique ID of the accociated court folder		CourtFolderI d	CFlvGOccur rence;Court Folder	CourtFolder	CourtFold er__Id	
Creation date/time	The date and time the RMS record was created.		CourtFolderC reTime	CFlvGOccur rence;Court Folder	CourtFolder	CourtFold er__CreTi me	
Description	A description or summary of the associated court folder		CourtFolderL abel	CFlvGOccur rence;Court Folder	CourtFolder	CourtFold er__Label	

97

Associated IDs Collection	(optional) The list of associated auxiliary IDs		nicheAuxiliar yIDs				Contains CAD incident Ref
							Required to match CAD
Fields							
Unique ID	An ID in the record that is the same as the unique ID from the RMS base record.		OccurrenceId	GOccID	GOccID	GOccID_ _WId	
ID	Internal or other unique ID of the accociated ID		GOccIDId	GOccID	GOccID	GOccID_ _Id	
Creation date/time	The date and time the ID record was created.		GOccIDCreTi me	GOccID	GOccID	GOccID_ _CreTime	
Associated ID	The ID associated with the occurrence		GOccIDIDNu mberG	GOccID	GOccID	GOccID_ _IDNumb erG	
Description	A description or summary of the associated ID		GOccIDEntit yDisplayNam e	GOccID	GOccID	GOccID_ _EntityDi splayNam e	
Remarks	Any remarks for the associated ID		GOccIDRem arks	GOccID	GOccID	GOccID_ _Remark s	
Associated Addresses Collection	(optional) The list of associated addresses		nichePhysica lAddresses				
Fields							

Unique ID	An ID in the record that is the same as the unique ID from the RMS base record.		OccurrenceId	GOcclvPA;P hysicalA ddress	GOcclvPA	GOcclvP A_LId	
Associated date/time	The date and time this record was associated		LinkCreTime	GOcclvPA; PhysicalAd dress	GOcclvPA	GOcclvP A_CreTi me	
Case relation	The field or fields that contain information about how the address is related to the case.			GOcclvPA; PhysicalAd dress	bsl_nice_occ _GOcclvPA	GOcc lvPA_ _Clas sificati on	Only return rows where GOcclvPA_ _Classificati on CONTAINS (OLC, FDA, CSI)
			LinkClassific ationG	GOcclvPA; PhysicalAd dress	bsl_nice_oc c_GOcclvP A	GOcclvP A_Class ificationG	
Address ID	Internal or other unique ID of the accociated address		PhysicalAddr essId	GOcclvPA; PhysicalAd dress	PhysicalAd dress	PhysicalA ddress_ Id	
Address	The field or fields that contain the address information		PhysicalAddr essLabel	GOcclvPA; PhysicalAd dress	PhysicalAd dress	PhysicalA ddress_ Label	
			PhysicalAddr essLatitude G	GOcclvPA; PhysicalAd dress	PhysicalAd dress	PhysicalA ddress_ Latitude G	Field is converted to decimal from dd:mm:ss
			PhysicalAddr essLongitud eG	GOcclvPA; PhysicalAd dress	PhysicalAd dress	PhysicalA ddress_ Longitud eG	Field is converted to decimal from dd:mm:ss
			PhysicalA ddressOr dnanceS	GOcclvPA; PhysicalAd dress	PhysicalAdd ress	Physical Address_ _Ordnan ceSurvey	

			urveyLoc ationG			Location G	
Static mappings	Static values mapped to Investigate claims		Level			Value	
Media Type	What media type this is	MediaType	Case			"Case"	
Media Sub Type	A refinement of the media type	MediaSubTy pe	Case			"RMS record"	
Media Source	Text to indicate where the item came from	MediaSource	Case			"RMS"	
User ID Fields	List of fields that contain user identifiers	UserIDFields _NicheId	Native			"owner", Investigat ingPerso ns[*].Per sonId	

Task 5. Deliverable Expectations: Testing

Contractor shall prepare test plans and conduct testing needed to ensure that all System components are complete, integrated, error free, and meet system requirements and specifications. Progressive test cycles shall be repeated until all bugs and anomalies are resolved and DEMS components are demonstrated to meet all applicable criteria, specifications, and system requirements.

Contractor shall conduct unit/module and systems integration testing, as specified in the Test Plan.

Contractor shall develop test plans and perform tests to ensure that the production system will meet all response-time requirements when deployed to all users and used during peak workloads. Contractor shall tune, and otherwise, update the production system to resolve noted issues. Contractor shall repeat stress-test cycles until all issues are resolved.

The County shall conduct User Acceptance Testing (UAT) as specified in the Test Plan. Contractor shall support UAT.

Testing and Development shall have their own environments, separate from Stage and Production environments. Testing or development shall not be performed in the production environment. Contractor shall provide and prepare system environments, including configuration and loading of test data, required to support all testing as specified in the Test Plan.

Contractor shall record all tests conducted, defects discovered, defects resolved and retests. Contractor shall provide regular status reporting of all testing.

In addition, Contractor shall use a single Problem Resolution Tracking tool that Contractor and the County shall use collaboratively for the tracking of System defects. The County is open to using a NICE application for Problem Resolution Tracking. The Problem Resolution Tracking tool shall, at a minimum, include:

- All defects in the System identified during any testing phase or in production shall be recorded, prioritized, tracked, and resolved in a timely manner. Each shall be assigned a "Defect Level" based on the following definitions:

  - **Critical** - Results in a complete system outage and/or is detrimental to the majority of the development and/or testing efforts. There is no workaround.

  - **Serious** - System functionality is degraded with severe adverse impact to the user and there is not an effective workaround.

  - **Moderate** - System functionality is degraded with a moderate adverse impact to the user but there is an effective workaround.

  - **Minor** - No immediate adverse impact to the user.

- Contractor shall allow the County full access to the Problem Resolution Tracking tool.

- The processes and management of the Problem Resolution Tracking tool shall be addressed as part of the Quality Control Plan.

- Contractor shall comply with the "Defect Level" approach as described above, including the requirement that the County's Project Management shall designate the level of severity to all defects.

- Contractor shall provide the following Testing sub-tasks and deliverables:

Task 5. Testing Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
5.1	Test Planning	Contractor shall prepare test plans and conduct testing needed to ensure that all system components are complete, integrated, error free, and meet system requirements and specifications. Progressive test cycles shall be repeated until all bugs and anomalies are resolved and DEMS components are demonstrated to meet all applicable criteria, specifications, and system requirements.	Contractor shall provide a comprehensive Test Plan that meets the IEEE Std. 829-1998 Standard for Software Test Documentation. The Test Plan shall include the procedures for documenting the completion of each test phase, test scripts, test conditions, test cases, and test reports. Detailed Test Plans shall be created for the following: • Unit/module testing approach • Systems integration testing approach • County user acceptance testing approach with support from Contractor • Performance and stress testing approach • Security testing approach • Test data creation approach, including data refresh processes • Automated test usage (optional) • Defect remediation release strategy • Defect reporting and tracking **The Deliverable shall include a DED**
5.2	Test Scenarios and Test Cases	Contractor describes the scenarios required to fully test all requirements of DEMS.	For each test scenario, the **Test Scenarios and Test Cases** shall minimally include: • Traceability to requirements and business processes • Dependencies and data preconditions • Test instructions • Expected results **The Deliverable shall include a DED.**
5.3	Systems Integration Testing	Contractor shall conduct and record the results and remediation steps of the integration system testing.	For each test scenario during Systems Integration Testing, the **Systems Integration Testing Results** shall include (at a minimum): • Date scenario was executed • Person executing the scenario • Test result status (pass/fail) — Defects discovered — Retest dates and results **The Deliverable shall include a DED.**

5.4	User Acceptance Testing	Contractor shall support the County in UAT testing and record all associated results and remediation steps.	For each test scenario during User Acceptance Testing, the User Acceptance Testing Results and Remediation Processes shall include (at a minimum): • Date scenario was executed • County Person performing executed test scenario • County determined test result status (pass/fail) • Defects discovered and proposed resolution from Contractor Team • County Retest dates and results **The Deliverable shall include a DED.**

Deliverable Expectations Document: NICE Implementation Test Plan

Project Deliverable Number: *<Insert - TBD>*	**Title of Deliverable:** Test Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Draft Review & Comment Period:** *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Final Review & Comment Period:** *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	**Deliverable Document Format:** *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	**Deliverable Author (Vendor):** *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose: The testing and validating of the NICE DEMS solution will be conducted by the NICE resource using the **NICE Implementation Test Plan** to verify that the solution delivered to COSB functions in conformance to agreed specifications and is ready for training and COSB rollout.

Deliverable Scope / Content Expectations: NICE will provide full documentation of test details including all test results, test set up, and configuration of your solution. The deliverables will include: NETWORK TESTING PERFORMANCE & SCALABILITY INTEGRATION TESTING NICE DEMS SaaS & SECURITY SOFTWARE TESTING SECURITY TESTING USER ACCEPTANCE TESTING TEST SCENARIOS AND TEST CASES DEFECT TRACKING Sample Enclosed: NICE DEMS COSB SOLUTION VERIFICATION DOCUMENT

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** The document is in full compliance with the approved DED and required content areas documented above.
	Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.
	Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

NICE Test Plan Overview

NETWORK TESTING

Operation of NICE DEMS requires sufficient internet access bandwidth both for users to access the system and for the DSG to upload index and media data. NICE DEMS will be uploading all digital evidence related to a case; hence the key bandwidth drivers will be video, photos and audio. The specific upload bandwidth requirements must be calculated based on the typical/average case size and number of cases. The specific download bandwidth will be also dependent on the number of concurrent users.

COSB is responsible for deploying the network infrastructure to provide the necessary bandwidth between Agency data sources and NICE DEMS on-premise Data Source Gateway and between the DSG and DEMS Cloud infrastructure. NICE will work with the Agency during project design phases to determine the needed bandwidth required for each phase of the project.

All testing of the deployed solution will take place over Santa Barbara County's provided bandwidth from the DSG to the DEMS cloud instance. NICE will work with the County to document latency and overall network performance.

PERFORMANCE & SCALABILITY

NICE DEMS is a SaaS offering that has been architected and tested to support a large number of concurrent users. As a true web application, DEMS supports the ability for multiple Police Users to access and view the same digital evidence concurrently. Each user would be viewing the digital evidence item in their own way without impacting any other users, enabling each user to pause, rewind, and review at their own pace.

Also, any number of concurrent users can upload evidence to DEMS. It is important to note that the upload/virus check/transcode processes do not lock the user out of using other functions of the platform or from viewing other digital assets stored in DEMS. Uploading large amounts of digital assets will not impact the use of other parts of the platform.

The NICE DEMS Support team monitors the platform via NICE's maintenance portal which tracks platform performance, storage capacity, and platform activity. NICE uses this information to determine when and where additional platform resources are required to ensure agreed to levels of Service performance.

104

The inherent scalability of the Microsoft Azure cloud means that NICE DEMS can easily adjust to meet the changing investigative workloads and evidence storage requirements as COSB's needs evolve.

SYSTEMS INTEGRATION TESTING

NICE shall conduct integration testing where all components of the solution are installed and actual data exchanges from the interfacing systems are made from the database through the DEMS DSG, over the secured network, and into DEMS deployed in the Microsoft Azure Gov cloud. The integration testing shall include verification of all exchange of records as documented in the DEMS IDD (Integration design document) that is created for each integration interface. The exchange of records shall be performed in a test environment that mirrors the final production environment and demonstrates the accuracy of the records being exchanged and the proper capture of all data elements within the new DEMS system.

Test plan results will be provided to COSB with sufficient sample size to test different possible scenarios. Detailed reports will be provided.

COSB approval of test is required prior to cutover to production.

Deliverable Expectations Document: NICE Systems Integration Testing

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: NICE Integration Test Documentation
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
This document describes a list of tests – organized by individual integrations - that can be used to validate that the NICE DEMS system correctly collects data and media from integrated systems, in accordance with agreed upon specifications.

Deliverable Scope / Content Expectations:
NICE will provide full documentation of test details including all test results, test set up, and configuration of your solution. The deliverables will include integration tests for the following:

Stakeholder Agency/ Department	Product	System Type	Description
Sheriff	DVMS, Command, Nexus	Safe Fleet/COBAN	In-Car and Body Camera Video management and archive systems. DVMS and Command are on Prem and Nexus is cloud storage

Sheriff	Enterprise	Central Square	Criminal Records Management System (RMS) case management system for criminal, traffic and other law enforcement reports
Sheriff	ATIMS	ATIMS	Jail Record Management System (JMS) for inmate related data for all inmates from booking to release
Sheriff	Data Works Plus	Data Works Plus	Live Scan fingerprinting and mugshot systems, includes tattoo and facial recognition engines
Sheriff	Inform	Central Square	Computer Aided Dispatch/911 system. Tracks 911 call data, routing of emergency services to and from incidents that come through COSB Public Safety Dispatch Center.
Sheriff	911 call recorder	AT&T	Records all 911 calls that come into the Public Safety Dispatch Center
Sheriff	Archived Criminal Records	Laserfiche	Document Repository where completed case files are archived and stored
Sheriff	Inmate Phone System	GTL	Inmate phone system, records all inmate phone calls
Sheriff	Forensics Case Files	Windows Files	Digital evidence as related to photos, videos, documents, voice files etc.
Sheriff	Interview Recording System	iRecord	Interview recording system used by detectives when interviewing suspects and victims or other individuals related to a case.
Sheriff	Custody DVR Systems	Misc.	Recording systems in COSB custody facilities
Public Defender	eDefender	Journal Technologies Inc.	Content management system for case records

Public Defender	Box.com	Box.com	cloud-based fie storage and sharing solution that securely centralizes content.
District Attorney	Damion	Equivant	A case management system that facilitates processing LEA referrals from intake to case disposition.
District Attorney	eProsecutor	Journal Technologies Inc.	A case management system that facilitates processing LEA referrals from intake to case disposition.
District Attorney	CJDC MNI	SB County / Bruce Thomas	Internal name matching system across Law and Justice partner systems
Probation Department	Caseload Explorer (IMPACT)	AutoMon Inc	A web-based case management system that is used to manage all adult and juvenile clients being investigated, held, or supervised by Probation.
References / Standards		Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.

Deliverable Criteria	**Acceptable:** *The document is in full compliance with the approved DED and required content areas documented above.*
	Rework Required: *The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.*
	Unacceptable: *The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.*

NICE DEMS SaaS SOFTWARE & SECURITY TESTING

NICE follows the 'Disciplined Agile Delivery' software development model. All new software releases are thoroughly tested following ISO-9001 quality controls. Every software release also goes through a Security assessment to evaluate what security actions will need to be taken before the new software is released into COSB application staging.

Please see the System Security Plan and the DEMS Quality Control Plan for further details, security and quality controls provided as a part of the DEMS SaaS offering.

Azure provides NICE with key metrics about the resources that are used (CPU, RAM, Average Latency etc.). The NICE InContact operations center receives these metrics and have alarms configured appropriately which automatically create a support request which is forwarded to NICE's secure operations team.

DEMS also has behavioral metrics built into the application which allow us to monitor whether activities are occurring as expected e.g. is media processing and is it successful, has the DSG contacted DEMS and is COSB's DEMS receiving records (per COSB data source). COSB can see the status of the DSG connectivity via the admin portal which shows the health status of each DSG connector.

DEMS built-in protection mechanisms include:

• **Automatic & transparent security updates** – As your Software as a Service (SaaS) providers, NICE and its hosting partner, Microsoft, are responsible for managing all software and security updates. Integrated deployment systems manage the distribution and installation of security patches.

• **Intrusion detection & DDoS** – To protect the Microsoft Cloud, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the continuous monitoring and penetration-testing processes of Azure. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks.

• **Penetration testing** – NICE and its hosting partner Microsoft conduct regular penetration testing to improve NICE DEMS security controls and processes. By

constantly challenging the security capabilities of the service, NICE stay ahead of emerging threats.

Error Resolution - By default the DSG and NICE DEMS are configured to retry the processing of data or media items multiple times should transient errors occur e.g. network connectivity issues or source systems become unavailable. NICE monitors imports to ensure that NICE doesn't see significant numbers of failures and should this be the case NICE DEMS can manually re-trigger imports of particular time ranges. Should significantly numbers of retrievals of media items fail, there is functionality in the Admin portal that allows COSBs support team to manually re-trigger the retrieval. Also, should a media item fail to process due to a transient error, they can re- request the processing from the DEMS portal for that item. Should an error be identified with data fields in the source metadata which prevents matching or prevents the data being in the correct fields or format, changes can be applied by a NICE engineer to the ruleset and a re-index of the data can be triggered to update those items with the new processing rules.

Task 6 Knowledge Transfer and Training

Contractor shall develop a knowledge transfer plan and project/implementation team training plan to share and transfer system development and support knowledge to key County resources. Additionally, Contractors shall provide and deliver full onsite training and curriculum for each of the user roles identified in Sub-Task 6.1. Contractor shall coordinate with the County to adhere to each County Department Training Standards, guidelines and best practices.

The County must be able to access the online Learning Management System (LMS) on an ongoing basis with little to no additional cost.

In addition, Contractor shall provide the County a training course outline for review and acceptance at least thirty (30) calendar days prior to the scheduled training.

The Training Course Outline shall minimally include:

- Course Presentation Material
- Student training exercises
- Pre- and post-assessment materials

Contractor shall populate on-line help content consistent with documentation provided under this task. Contractor shall provide the capability for the County to update on-line help content. Also, Contractor shall work with the County to incorporate content describing the corresponding business process for each help menu item.

Contractor shall provide documentation specific to the County's DEMS implementation.

Contractor shall list and describe documentation that will be provided, including the formats in which the documentation will be made available.

Contractor shall provide the following Knowledge Management and Training sub-tasks and deliverables:

(Remainder of Page Intentionally Left Blank)

Task 6. Knowledge Transfer and Training Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
6.1	**Knowledge Transfer and Training Planning**	Contractor shall provide training for the following roles. Training shall be specific to each listed role: • Technical Administrator • DEMS COSB • Manager • Support Staff	Contractor shall develop (in cooperation with the County) a **Knowledge Transfer and Training Plan** to define the process of training personnel to levels appropriate for their roles. The Plan shall address the following topics: • Resources necessary to complete the training effort along with the tools and documentation that will be necessary to support proposed effort • Specific courses and course materials • Lists of materials, facilities, equipment, user profiles, access procedures, work samples, and other items needed for each training session, including items that County is to furnish • Training calendar indicating the specific attendees and locations for all user training sessions. The calendar shall also indicate any planned phases or iterations in the delivery of training • Knowledge Transfer to enable County personnel to operate, maintain, configure, and modify the new systems, including operation of the testing tools, supporting infrastructure, and security Contractor shall provide a report about the progress of training activities. The Deliverable shall include a DED

| 6.2 | Provide Training Curriculum | | For each course identified in the Training Plan, the **Training Curriculum** shall include (at a minimum):

・ Course presentation materials (Trainer Version)
・ Course presentation materials
・ Student training exercises pre-and post assessment materials
・ Training data specifications for training exercises (if applicable), including training data initialization procedures

The Deliverable shall include a DED |

| 6.3 | Provide User Manual Documentation | Contractor shall provide training curriculum of sufficient depth and clarity to provide breakdown of the course material. | The User Manual shall include (at a minimum):

・ ECM (Enterprise Content Management) end-user manual(s)
・ ECM mobility user manual
・ System administration and operations manual
・ On-Line Help administration manual
・ Ad hoc report writing manual
・ Run book that contains: network configurations, reboot procedures, monthly/daily maintenance along with trouble shooting guidelines

The Deliverable shall include a DED |

6.4	**Provide Technical Documentation**	Contractor shall provide technical documentation of sufficient depth and clarity to enable County technical personnel to understand the underlying structure and function of system components, to troubleshoot the application software and interfaces (including platform, network, and security interfaces), to support users (help desk), to perform all system administration and operation duties, and to plan for potential future integration with other applications.	The Technical Documentation shall include (at a minimum): • System architecture overview • Data dictionaries • Entity relationship diagrams • Interface configurations **The Deliverable shall include a DED**
6.5	**Conduct Training**	Contractor shall conduct and complete training sessions within a sixty to ninety (60-90) day period prior to system Go-Live. These sessions will be recorded and provided to the County within 5 business days of being conducted.	The Training Execution Results shall summarize the training efforts, its outcomes, remedial actions, and confirm its completion.
6.6	**Remedial Training**	Contractor shall conduct and complete remedial training sessions on a bi-weekly basis until County resources sufficiently complete the post assessment training	N/A

DELIVERABLE EXPECTATIONS DOCUMENT: NICE KNOWLEDGE TRANSFER AND TRAINING PLAN

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: Knowledge Transfer and Training Plan
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>
Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose:
NICE DEMS Training shall provide COSB personnel the expertise and product knowledge needed to acquire the skills required to undertake day-to-day activities using NICE DEMS. The specific training plan for SBCO users will be developed in collaboration with appointed SBCO personnel.

Deliverable Scope / Content Expectations:
NICE will provide full Knowledge Transfer and Training documentation to SBCO prior to the execution of the training plan. The deliverables will include: • TRAINING STRUCTURE, RESOURCES, TOOLS, AND DOCUMENTATION • TRAINING FORMATS • SPECIFIC COURSES AND COURSE MATERIALS • LISTS OF MATERIALS, FACILITIES, EQUIPMENT, USER PROFILES • AGREED-UPON TRAINING CALENDAR • REPORT ABOUT THE PROGRESS OF TRAINING ACTIVITIES Sample Enclosed: NICE INVESTIGATE SAMPLE training CURRICULUM, TECHNICAL DESCRIPTION DOCUMENT

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and SBCO, related to the subject DEMS project.
Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above. Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or

	errors that need to be addressed before the document can be fully reviewed.

NICE Knowledge Transfer and Training Plan

TRAINING OVERVIEW

Training is a critical path item and the key to the last step of a successful project. To help gain maximum return on your investment in NICE DEMS as quickly as possible, NICE's Customer Education Services team provides users with the knowledge and skills needed to take full advantage of its capabilities right from the start.

NICE crafts their training approaches as carefully as NICE develops their award-winning solutions, using the most effective state-of-the-art training platforms and techniques.

NICE DEMS Training shall provide SBCO personnel the expertise and product knowledge needed to acquire the skills required to undertake day-to-day activities using NICE DEMS. **The specific training plan for SBCO users will be developed in collaboration with appointed SBCO personnel.** The plan will include specific details on the following:

- Resources necessary to complete the training effort along with the tools and documentation that will be necessary to support proposed effort

- Specific courses and course materials

- Lists of materials, facilities, equipment, user profiles, access procedures, work samples, and other items needed for each training session, including items that County is to furnish

- Training calendar indicating the specific attendees and locations for all user training sessions. The calendar shall also indicate any planned phases or iterations in the delivery of training. During the Planning phase the dates for the Training will be established and confirmed as the ongoing deployment is underway and as part of the validation communication.

- Knowledge Transfer to enable County personnel to operate, maintain, configure, and modify the new systems, including operation of the testing tools, supporting infrastructure, and security

TRAINING FORMATS

Training shall be delivered in the following formats:

- **Train-the-Trainer sessions** led by NICE to successfully enable delivery of classroom-based training for the NICE DEMS Solution.

  o Training shall cover key knowledge points to be transferred in the classroom, trainer demonstrations, student exercises, end of module review quizzes, and best approaches for delivery.

  o Training will be delivered on-site for approximately twenty COSB Trainers

- Self-guided online training modules for use as new users are added to the platform as well as refresher training for existing users

- In application Help documentation to assist the user with specific functionality as needed

- Scheduled Webinar updates facilitated by NICE to provide training on functionality associated with new software releases

- Quarterly touchpoints between NICE and select SBCO Investigate users to obtain feedback and ensure maximum utilization of the system and its capabilities

Training Curriculum

NICE shall provide a training plan and curriculum for the roles outlined below. NICE shall coordinate with SBCO Training Manager to adhere to COSB training standards, guidelines, and best practices.

NICE shall provide training for the following roles:

- System Administrator

- Super User – "Train the Trainer"

- Investigate COSB

- Justice COSB

KEY USER APPLICATION COURSES

NICE hands-on training covers the full functionality and capability of NICE applications for Key Users and Administrators, conducted at COSB's sites.

NICE recommends that training take place on the live COSB DEMS system. It is most effective when students can go through training working with their own cases in Investigate.

Each student must have a laptop or computer equipped with internet access.

Training Scheduling Criteria

The entire curriculum requires one day of education. Depending on the number of sessions and students, the appropriate training plan, communication plan, and schedule shall be determined during the Planning phase.

As a baseline, NICE recommends a minimum of 3 days of on-site training at each stakeholder location. NICE understands it is difficult for staff to be away from their work for an entire day thus NICE provides a level of flexibility to deliver in half day segments. This also allows for some practice time as well away from the classroom.

Module Title	Outline
DEMS Portal Overview	By the end of this module, you shall be able to: - Describe the NICE DEMS Solution - Log in to the NICE DEMS Portal - Reset your password - Configure your notifications - Configure your user settings - Use Help

Case and Evidence Items	By the end of this module, you shall be able to: • Create a New Case and Upload Evidence Items • Navigate an Existing Case • Case Item Actions • Navigate Case Evidence Items • Case Evidence Item Actions
Case and Evidence Views	By the end of this module, you shall be able to: • Describe the views available for Case and Evidence Items • Work with Grid and List view • Work with the Timeline View and Playback Video & Audio • Work with the Map View and Playback Video & Audio
Filtering and Ordering Cases	By the end of this module, you shall be able to: • Describe Filtering and Ordering • Filter Cases and Evidence Items • Filter using the Refine by Option • Filter using Keywords • Filter using Configurable Fields • Create a Saved Filter • Use the Ordered by Option
Search Evidence	By the end of this module, you shall be able to: • Search for Cases and Case Evidence Items using Search Criteria • Add Searched Evidence to a Case • Perform a Document Search • Perform an Audio Search
Evidence Suggestions	By the end of this module, you shall be able to: • Navigate the Suggestions Page • View Suggestion Information • View Suggestion on the Map View • Add Suggestions to a Case
Evidence Requests	By the end of this module, you shall be able to: Submit a Request to a Business Submit a Request to a Citizen Submit a Request to a Business using Map View Track Requests Add Media Items to a Case

116

Audio and Video Evidence Items	By the end of this module, you shall be able to: • Use Playback Controls • Clip Audio and Video Files • Create a Snapshot • Redact Audio from Media • Redact Video from Media • Use Zoom Controls • Add a Bookmark
Sharing a Case	By the end of this module, you shall be able to: • Overview of Sharing Case and Evidence • Share a Case and Case Evidence Items with Users • Share a Case and Case Evidence Items via Download with Users • Manage Shares using the Sharing Page

TRAIN-THE-TRAINER COURSES

NICE provides a specialized program that enables in-house trainers to conduct internal courses for NICE users, all based on the techniques and content NICE's own trainers have found most effective. This shall help extend NICE solution skills throughout the organization and maintain high levels of proficiency over time. The learning experience NICE has found to be most effective is a three-pronged approach. First, NICE delivers the course material to COSB education specialist. Second, NICE shall co-deliver the class with your education specialist and lastly, NICE shall observe COSB education specialist deliver the class. The course Trainer Guide along with the education material shall be provided to COSB education specialist.

TRAINING COMPLETION

This Deliverable shall include:

- Summary of all training provided including course, date, and attendees

- Summarized training exercise results

- General observations of completed training and future training recommendations

POST IMPLEMENTATION ONGOING TRAINING OPPORTUNITIES

NICE shall provide the following training opportunities for new users, or for when new capabilities are added to the DEMS offering.

- **Self-paced eLearning modules** - available 24/7, covering basic and advanced usage of NICE products

- **Webinars** – Live eLearning events, hosted by NICE Education Specialists, held periodically to cover new features/capabilities and various topics around NICE products and best practices

- **Documents** – User guides available in the DEMS application

- **Notifications** – Receive information about latest NICE training promotions and news

- **Updates** – Learn about new updates and features from NICE

# DELIVERABLE EXPECTATIONS DOCUMENT: NICE USER MANUAL DOCUMENTATION

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: User Manuals
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>
Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose:
A complete set of user manuals are available to end users and administrators on-line in the NICE DEMS application. This documentation is kept current within the SaaS solution as new features and capabilities are added.

Deliverable Scope / Content Expectations:
While all user and administration manual are provided in the on-line format, embedded in the SaaS application, then can also be provided as stand-alone files upon request. The deliverables will include: USER MANUALS / GUIDES ADMINISTRATOR MANUALS / GUIDES 3RD PARTY USER GUIDES (e.g., outside counsel) Sample Enclosed: NICE DEMS screen images from the application, showing help menus and software functionality information available to users for access at any time.

| References / Standards	NICE Software Quality and Documentation Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and SBCO, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** The document is in full compliance with the approved DED and required content areas documented above. **Rework Required:** The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. **Unacceptable:** The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

User Manual Documentation
SAMPLES OF TRAINING MATERIALS

NICE Training materials consist of quick reference guides and instruction for hands-on interaction with the solution, in addition to the interactive on-line system user manuals.

The following examples are reference guides in a Power Point format, used in training sessions with a professional trainer.
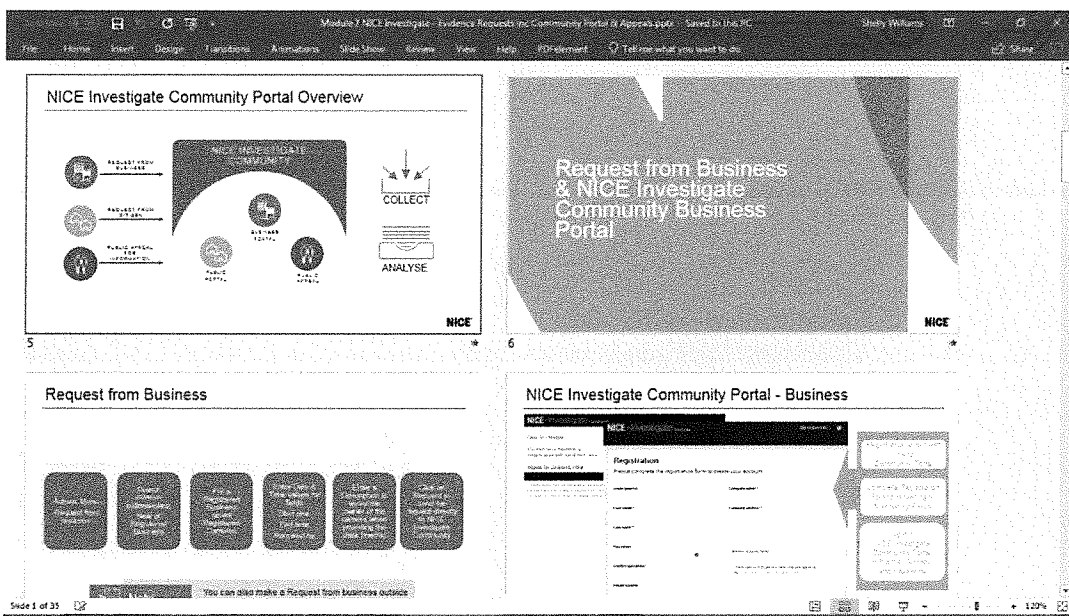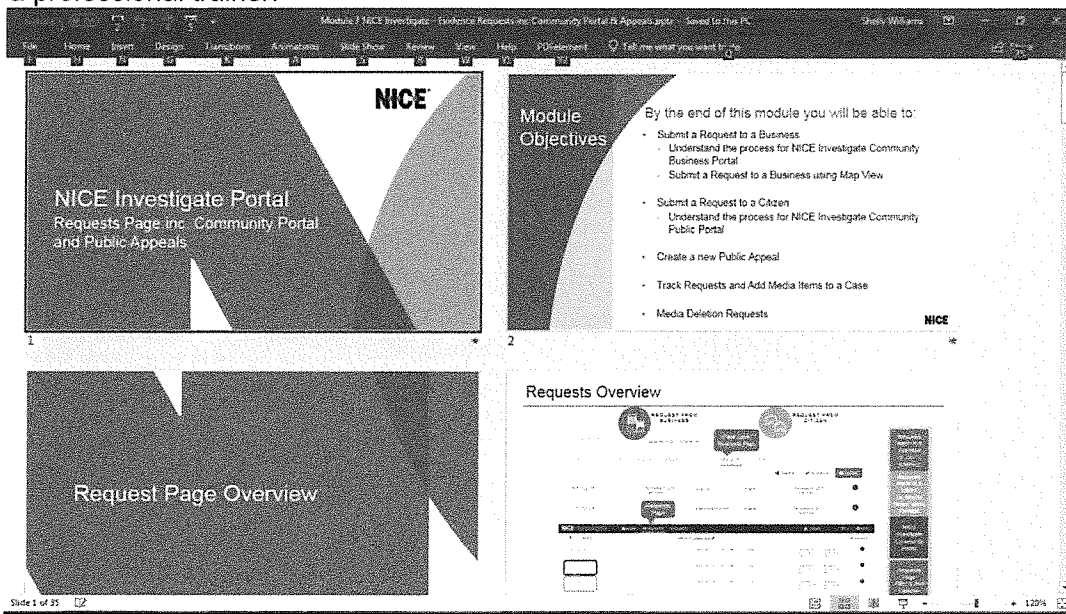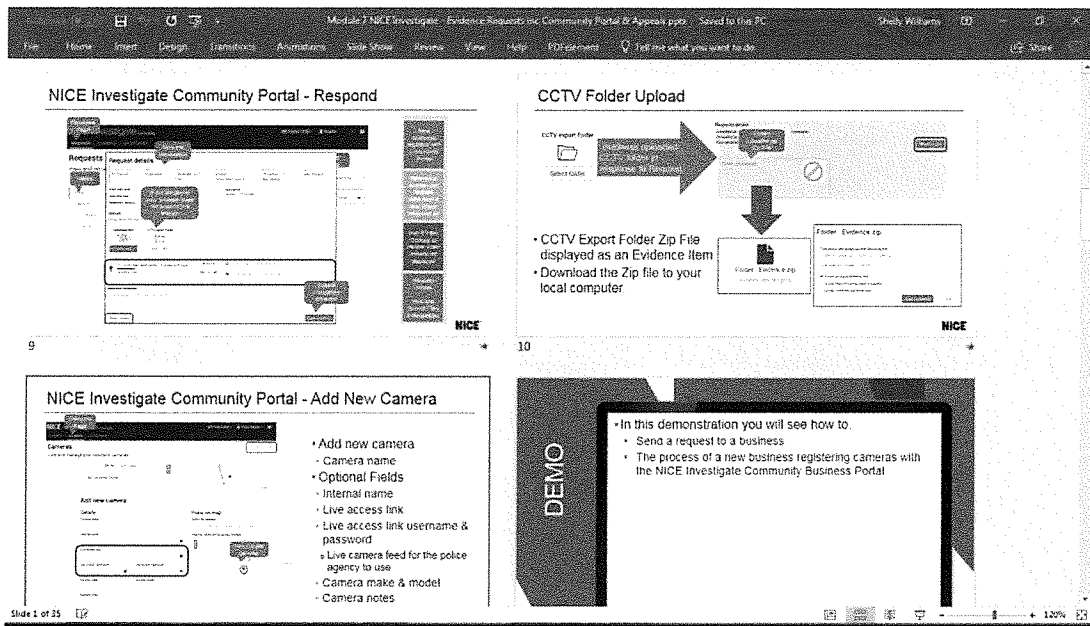
SAMPLE IN-APPLICATION HELP DOCUMENTATION

A complete set of user manuals are available to end users and administrators on-line in the NICE DEMS application. Simply by clicking on the help icon in the user interface, the user has access to any and all information concerning the use of the application, provided in a live, interactive format – easily searchable by topics, keywords, indexes, and more.

This documentation is kept current as new features and capabilities are added. Following are example screen shots of this documentation.
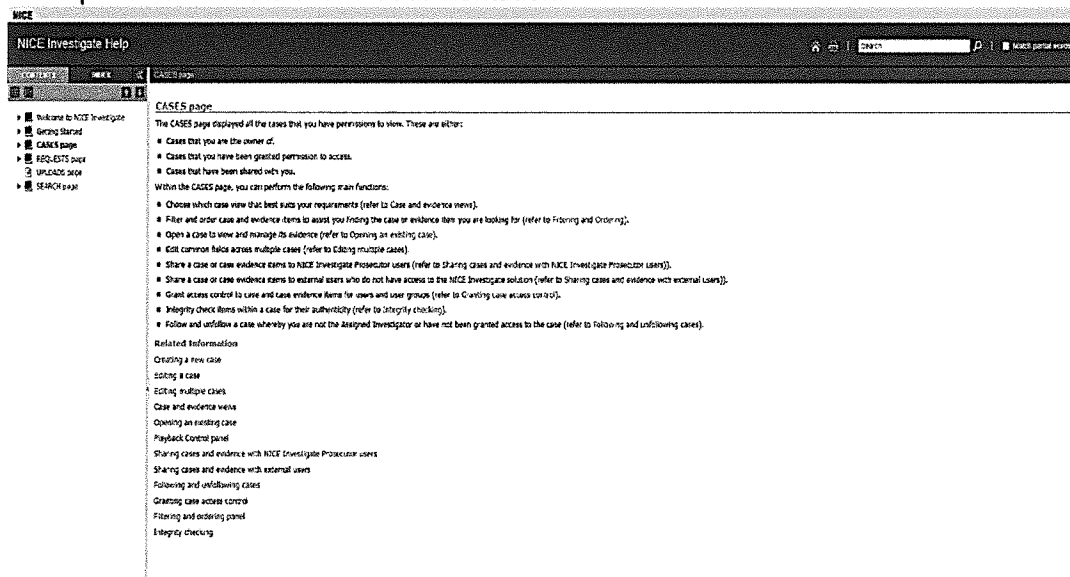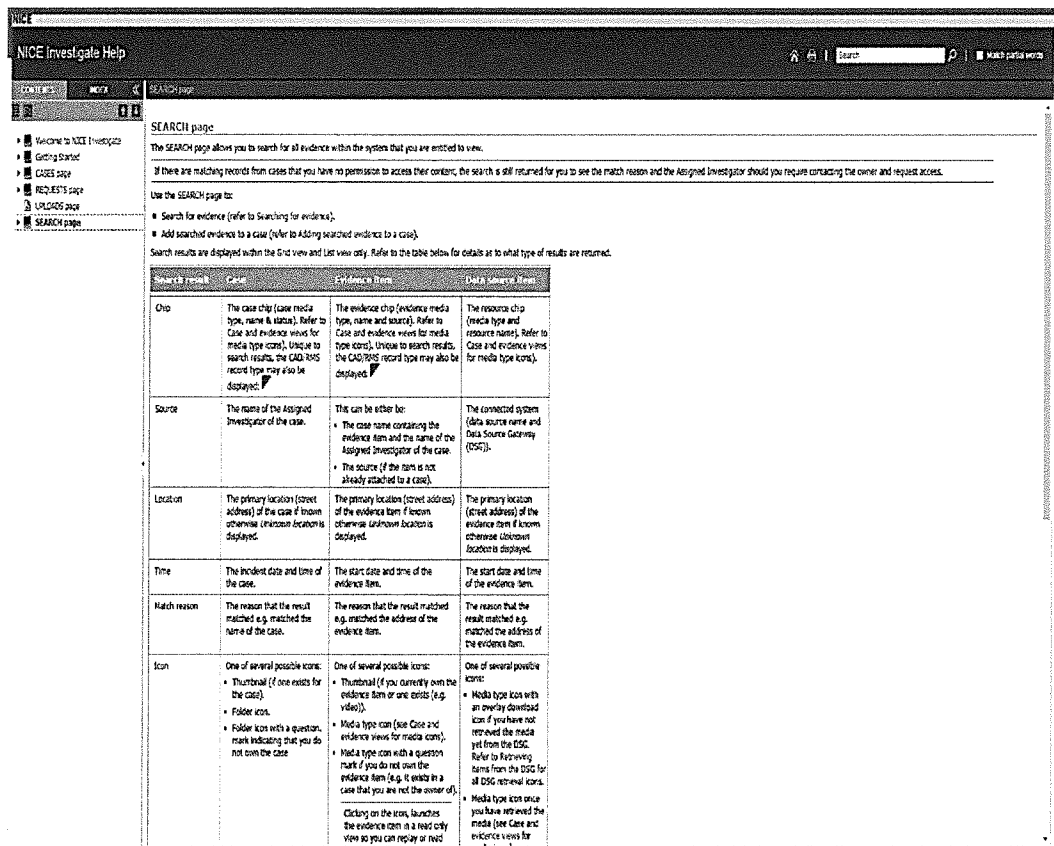
RUNBOOK DOCUMENTATION

COSB network configurations are provided in the System Design and Development Document that is delivered to COSB during Project Implementation.

All necessary solution reboots and other troubleshooting and maintenance procedures are the responsibility of the NICE DEMS Support team. Consequently, no COSB documentation is required for such activities.

DELIVERABLE EXPECTATIONS DOCUMENT:
NICE TECHNICAL DOCUMENTATION

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: Technical Documentation
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>

Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >

Deliverable Description and Purpose: All NICE DEMS customers receive a copy of the NICE DEMS Technical Description Document. The document provides sufficient detail for customers to understand the technical aspects and key architectural points of the DEMS SaaS suite of products.	

Deliverable Scope / Content Expectations: NICE will provide full documentation with the DEMS solution's Technical Description. The deliverables will include: ARCHITECTURE, DATA STORAGE, MEDIA FILES, COMMUNICATIONS, DATA BACKUP, BUSINESS CONTINUITY AND DISASTER RECOVERY NICE COMMUNITY PORTALS NICE DEMS DATA SOURCE GATEWAY Sample Enclosed: NICE DEMS TECHNICAL DESCRIPTION DOCUMENT	
References / Standards	NICE Software Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and SBCO, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** The document is in full compliance with the approved DED and required content areas documented above. **Rework Required:** The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. **Unacceptable:** The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

Technical Documentation

All NICE DEMS customers receive a copy of the NICE DEMS Technical Description Document. The document provides sufficient detail for customers to understand the technical aspects and key architectural points of the DEMS SaaS suite of products.

A copy of the entire NICE DEMS Technical Description Document is attached hereto as Attachment C.

Task 7. System Implementation

Contractor shall use a proven implementation methodology based on industry standards and best practices. The implementation methodology for this project will be a phased approach with the Sheriff Office and the District Attorney executing Go-Live first. Once that has been successfully completed and if the Box.com integration meets the identified criteria in Task 4. Systems

Integration Expectations, COSB and NICE will plan for the phased release of Public Defender's instance of DEMS. The methodology establishes an accountability framework which allows Contractor to deliver high-quality services throughout the project. The framework shall link project stages to defined quality gates and deliverables.

Contractor shall validate that each interface to an external system is working correctly. Contractor will repair all interface-related problems caused by Contractor-developed interfaces.

In addition, Contractor shall assist the County with testing and release preparation in the preproduction environment.

Contractor shall provide the following System Implementation sub-tasks and deliverables:

Task 7. System Implementation Sub-Tasks and Deliverables

Task #	Sub-Task	Descriptions	Deliverables
7.1	**Implementation on Planning**	In preparation for the pre- production release, the Contractor shall establish a pre-production plan.	The **System Implementation Plan** shall clearly identify the timing of each stage and key milestones, including the rationale for Contractor's timeline and any assumptions. The Plan shall align the stages, milestones, and deliverables in the project plan with this Statement of Work.
7.2	**PreProduction Release**	When functionality is ready to be delivered to the County for UAT, it shall be delivered in the form of a Pre- Production Release. Since the County will perform UAT and approve all releases into production, a pre- production release is equivalent to a production release and requires the rigor associated with a production release.	Each Pre-Production Release shall include the following: A. Release Description including Architecture or Design updates, Security Configuration, new functionality introduced, defects fixed, modifications to interfaces with other systems, other changes to existing code, and any software configuration changes B. Release Contents including a description of the release structure and contents and instructions for assembling and/or configuring the components of the release C. Detailed configuration information including any dependencies and instructions at a level of detail that will enable System Administration staff to re-configure the system D. Database documentation conforming to industry standards E. Detailed configuration information for any 3rd party software Contractor shall provide updated documentation when system upgrades to software or any Contractor supplied equipment occurs through the life of the Contract. **The Deliverable shall include a DED**

| 7.3 | **Production Release Planning** | Upon successful completion of the Pre- Production testing, Contractor shall, in coordination with the County, create a Production Release Plan that shall consist of an updated Pre- Production Release notification to assist the County in successfully releasing and maintaining DEMS in the Production environment. | The **Production Release Plan** shall include, but not be limited to, the following components:

A. Updated Configuration Information required to satisfy the County production configuration management requirements.

B. Updated System Architecture.

C. Updated Detailed Design, including detailed system, technical, security and user documentation. Deployment schedule.

In addition, the Plan shall include detailed step-by-step activities (both Contractor and County activities) and the timeline for the cutover process. The plan shall define the milestones where readiness to proceed is assessed, go/no-go criteria, and fallback positions to be taken if no-go conditions are encountered **The Deliverable shall include a DED** |
| 7.4 | **Production Release** | Upon successful completion of UAT, the County will schedule a release to be moved to the Production environment. | Each Production Release shall include the following:

A. Release-specific Software system components

B. Release Description including Architecture or Design updates, new functionality introduced, defects fixed, security configurations, modifications to interfaces with other systems, other changes to existing code, and any software and hardware configuration changes

C. Release Contents including a description of the release structure and contents and instructions for assembling and/or configuring the components of the release

Detailed hardware and software configuration information including any software and hardware dependencies and instructions at a level of detail that will enable System administration staff to rebuild and configure the hardware environment without outside assistance

Database documentation conforming to industry standards

Detailed configuration information for any 3rd party hardware and software

Contractor shall provide updated documentation when system upgrades to software or any Contractor supplied equipment occurs through the life of the Contract. **The Deliverable shall include a DED** |

| 7.5 | **Production Cutover Planning** | Contractor shall provide multiple cutover cycles, if specified in The Solution Implementation Plan, including at minimum one Table Top Rehearsal to confirm the process and to establish the cutover timeline. | The Production Cutover Plan shall include detailed step-by-step activities (both Contractor and County activities) and the timeline for the cutover process. The plan shall define the milestones where readiness to proceed is assessed, go/no-go criteria, and fallback positions to be taken if no-go conditions are encountered. The plan needs to include a clear communication plan as part of production cutover and a strategy for enough back filed items that make day- to-day operations with the stakeholder agencies/departments a success. **The Deliverable shall include a DED**. |

Deliverable Expectations Document:
NICE Pre-production Release and Release Plan

Project Deliverable Number:	Title of Deliverable:
<Insert - TBD>	Pre-production Release, Pre-production Release Plan
Draft Submission Due Date:	County Draft Review & Comment Period:
<Insert – TBD, as mutually agreed >	*<Insert - TBD>*
Final Submission Due Date:	County Final Review & Comment Period:
<Insert – TBD, as mutually agreed >	*<Insert - TBD>*
Reviewed By Required:	Deliverable Document Format:
<Yes/No – by whom –TBD as mutually agreed >	*< Word / PDF>*
Deliverable Owner (County):	Deliverable Author (Vendor):
<Name, Role – TBD, as mutually agreed >	*<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
During the Initiation discussion, the NICE project manager and COSB project manager shall review the overall project delivery scope, high level project plan, connector capability requirements and COSB site readiness.

Deliverable Scope / Content Expectations:

Solution Design Document

Updated System Architecture

Use cases, business process flows or a similar mechanism describing how the SOLUTION shall be used in the context of each COSB business process

SOLUTION reporting capabilities in the context of COSB business processes

SOLUTION security and privacy controls

Key business process and/or policy changes required to conform with SOLUTION capabilities

Summary level descriptions of SOLUTION changes needed to meet COSB requirements

Detailed discovery session

Security

Access Control needs

DSG vm and bandwidth requirements

Detailed DSG requirements documents

Planning sessions with sessions with database SMEs

Detailed project plan with timelines for execution

Project objectives

Project scope definition with detailed requirements

Including requirements traceability matrix

Project resources

(Remainder of Page Intentionally Left Blank)

   a. NICE's Project Team (e.g., organization, names, role definition and organization reporting lines)

   b. Project roles and responsibilities (e.g., RACI showing COSB and NICE roles and responsibilities for work breakdown structure)

  D. Project schedule / work breakdown structure

   o NICE shall conduct workshops with COSB to determine the solution production deployment approach for rolling out the SOLUTION, including possible phasing strategies, site specific considerations, and benefits and risks of strategy alternatives.

  E. Quality management plan

  F. Risk management plan and Risk Register

  G. Release management plan

  H. Communication plan (including the frequency of meetings)

- **Defined and documented DEMS Access Control policy**
- **Defined and documented Evidence Storage Retention policy**
- **Documented COSB Training Plan**

<u>Samples Enclosed:</u>

NICE DEMS Provisioning Strategy

NICE DEMS DSG Provisioning

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** *The document is in full compliance with the approved DED and required content areas documented above.* **Rework Required:** *The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.* **Unacceptable:** *The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.*

Implementation Methodology

INITIATION PHASE

Objective: Review the objectives, design, and scope of the solution as sold to ensure all parties are on the same page.

Preparation for Successful Deployment of NICE DEMS

The NICE project manager shall review with the internal NICE customer engagement team the overall objective and details of the solution design as prepared and purchased by COSB. The NICE project manager shall schedule a Kickoff call with COSB project manager and relevant stakeholders to review the objectives, design, and scope of the solution as sold to ensure all parties are on the same page.

During the Initiation discussion, the NICE project manager and COSB project manager shall review the overall project delivery scope, high level project plan, connector capability requirements and COSB site readiness. The respective project managers shall also establish the communication cadence for the project. They shall review all the project documentation that is associated with each phase of the project to ensure all stakeholders are receiving status updates and project control details throughout the project. At each step in the process COSB shall have a complete understanding of the current status, next steps, and a timing confirmation to reduce and eliminate risks.

First Critical Path Phase: Prerequisites for COSB Data Readiness

This shall include but not be limited to the technical infrastructure, remote access and all the associated APIs and Database access for the preparation of the DSG connection and set up. This is an area of significant risk to the success of the project and impact to the timeline. The NICE project manager and team shall work with COSB to establish a clear understanding for the secure remote connectivity required for the project and solution on going.

From the earliest discussions around the third-party systems NICE shall be capturing data from though the workshop conducted, the immediate access to the data structures, DB access and or APIs is a critical milestone. This area can have a two-fold impact on the project and solution. Short term it shall impact all the timelines and planned activities, and second if the access to the source data are not understood or available the solution and data within shall not be accurate, useful, or provide value. NICE shall discuss this further during planning.

Keeping the success and timely completion of the project in mind, it is always very useful for all stakeholders to have visibility into steps along the timeline in order to understand what to expect along the way. NICE takes pride in partnering with COSB during all phases of solution delivery, understanding that it may be COSB's first time with an engagement of this type.

Deliverables

- Identify key project stakeholders
- Formal Kickoff Meeting and Project Kickoff Presentation
- Review of high-level project plan
- Review of connector capability requirements including all the associated APIs and database access requirements
- Review of site readiness prerequisites such as technical infrastructure, remote access needs

PLANNING PHASE: PRE-PRODUCTION PLANNING

Objective – to gather detailed requirements for connector development and solution deployment After all parties have reviewed and agreed to the scope, the next step is Planning.

At this stage, the respective project managers shall refine the high-level project plan and lock down the detailed project plan with timelines for the Execution which includes development of the DSG to handle the third-party data, provisioning the instances in the cloud, data collection of the

historical case data, and migrating the historical data for reference, while testing these multiple areas along the way. The Execution phase wraps up with the training and then transitions to COSB for your planned Rollout of the solution to the users. The first major activity of the Planning phase is a detailed discovery session with COSB teams.

A key element to success is the connections to COSB third party systems that feed data to the NICE DSG. As per the Initiation phase where the requirements were shared for this milestone, the NICE and COSB teams shall complete a detailed design and respective review over the course of approximately two weeks. This shall contribute to the development of the detailed overall project deployment plan. As previously shared, this is a significant milestone and risk area to the project timeline and the solution itself. COSB needs to take special care around this activity that COSB needs to deliver to NICE. Historical data shall also be reviewed and taken into consideration as a deliverable and milestone COSB is responsible for. Once COSB has identified the data, NICE will plan for the acquisition, migration of the data and testing shall be in the plan and associated tasks.

With the detailed project plan and timeline agreed to, the respective project managers shall review specific tasks required to deliver the implementation or Execution phase flawlessly. The respective project managers shall identify the specific resources needed from both organizations to accomplish each task.

With the tasks identified, the respective project managers shall build out the detailed work breakdown structure for each task with the associated timelines and dependencies. The site preparation task shall have a "go - no go" milestone two weeks prior to the planned execution phase.

Deliverables: Pre-Production Release Documents

Solution Design Document

- Updated System Architecture
- Use cases, business process flows or a similar mechanism describing how the SOLUTION shall be used in the context of each COSB business process
- SOLUTION reporting capabilities in the context of COSB business processes
- SOLUTION security and privacy controls
- Key business process and/or policy changes required to conform with SOLUTION capabilities
- Summary level descriptions of SOLUTION changes needed to meet COSB requirements

Detailed discovery session

- Security
- Access Control needs
- DSG vm and bandwidth requirements

Detailed DSG requirements documents

- Planning sessions with sessions with database SMEs

Detailed project plan with timelines for execution

- Project objectives
- Project scope definition with detailed requirements

— Including requirements traceability matrix

* Project resources

* NICE's Project Team (e.g., organization, names, role definition and organization reporting lines)

* Project roles and responsibilities (e.g., RACI showing COSB and NICE roles and responsibilities for work breakdown structure)

* Project schedule / work breakdown structure

NICE shall conduct workshops with COSB to determine the solution production deployment approach for rolling out the solution, including possible phasing strategies, site specific considerations, and benefits and risks of strategy alternatives.

* Quality management plan

* Risk management plan and Risk Register

* Release management plan

* Communication plan (including the frequency of meetings)

    — Defined and documented DEMS Access Control policy

    — Defined and documented Evidence Storage Retention policy

    — Documented COSB Training Plan

CONVERSION AND DATA MIGRATION PLAN

During the Project Planning Phase, a detailed project plan will be created with timelines for the Project Execution Phase which includes development of the DEMS Data Source Gateway (an on premise software appliance that hosts integration connectors to existing data sources) to handle interfacing to third party data sources, provisioning the DEMS cloud instances, data collection of the historical case data, and migrating the historical data for reference, while testing these multiple areas along the way.

The first major activity of the Planning phase is a detailed discovery session with COSB teams. The Execution phase wraps up with training and then transitions to COSB for your planned Rollout of the solution to the users.

A key element to a successful DEMS deployment is the proper design of the DEMS DSG connections to COSB's third-party systems that feed data to the DEMS cloud instance deployed for COSB. The NICE and COSB teams will work together to gather requirements for each DSG connector and complete detailed designs and respective reviews over the course of approximately two weeks. Requirements for migration of historical data will also be reviewed and taken into consideration as a deliverable and milestone in the overall Project Plan.

With the detailed project plan and timeline agreed to, the respective project managers will review specific tasks required to deliver the implementation or Execution phase flawlessly. The respective project managers will identify the specific resources needed from both organizations to accomplish each task.

COSB AIR FOR DETAILED TRACKING OF ALL ACTION ITEMS

During the Project Initiation Phase a COSB AIR is created. The Action Item Registry (AIR) is used

throughout the duration of the project to log and track all action items associated with the project. It is updated and maintained by the NICE Project Manager and provides a single location for all identified action items, issues, and identified project risks.

The following example of an action log is from an actual customer air. As shown, every item is tracked with its own ID# along with a description of the action item, the date the issue was raised and an owner who is responsible for the resolution of the issue.

- The project team, which consists of key representatives from NICE, any subcontractor/s and COSB, agrees on a priority for each tracked action item. The owner is then responsible for providing a projected close date and completing the assigned action item. The owner provides updates as needed at the weekly project team meetings

- This same process is utilized as it relates to the Project Risk Register and the Project Issues log, with the identified owner(s) being responsible for identifying the issue resolutions plan/risk mitigation plan.

(Remainder of Page Intentionally Left Blank)

Data Conversion and Data Migration Planning and Tracking
A key part of the NICE DEMS Project Planning Phase are the technical discovery sessions that are held with COSB.

During these sessions, representative subject matter experts from COSB meet with NICE technical personnel to discuss and document data migration requirements from existing COSB databases to NICE DEMS. Requirements identified from these sessions are documented in an Integration Design Document. There will be a detailed list of requirements that will be documented and agreed to for each project integration.

The IDD is then used by the NICE DEMS R&D team when developing the DEMS DSG connectors.

The following shows an IDD detailing the data migration requirements of 911 call recordings from a customer's NICE Inform database to NICE DEMS. As, you can see, IDDs are very detailed and specific in nature. NICE documents every data field that will be migrated and show how it will be used and shown in NICE DEMS.

All IDDs must be reviewed and approved by COSB SMEs before any connector development work can begin.

132

Deliverable Expectations Document Production Execution Phase Deliverable Expectations: NICE

Production Release, Production Release Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Production Release, Production Release Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose: The objective is deploying NICE DEMS for Los Angeles County, testing, and training

Deliverable Scope / Content Expectations: **Solution Implementation Plan**   Installation and/or setup   Solution Analysis and Design   Solution Configuration   Solution Build (e.g., data conversion, interfaces, reports/forms/dashboards)   Testing (e.g., unit testing, system, UAT)   Training   Production Deployment (e.g., including possible phasing strategies, site specific considerations, and benefits and risks of strategy alternatives)   Production Go-Live Support   Post-Production Go-Live Support   **DSG Connector development, turn up, testing**   **NICE DEMS Configuration**   **NICE DEMS provisioning and turn up/testing**   **Indexing of historical data**   **Testing and validating of the NICE DEMS solution using the NICE Implementation Test Plan**   **Complete COSB Training**   **Weekly Project Status Updates**   Tasks completed for the period   Tasks planned but not completed for the period   Tasks planned for next period

	Upcoming COSB resource needs (90-day forecast)

Issues

Risks

Decision requests

Samples Enclosed:

NICE DEMS Provisioning Strategy NICE DEMS DSG Provisioning COSB Site Readiness

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** *The document is in full compliance with the approved DED and required content areas documented above.*
	Rework Required: *The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.*
	Unacceptable: *The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.*

EXECUTION - PRODUCTION RELEASE

Objective – deploying NICE DEMS for [CUSTOMER NAME] PD, testing, and training

Production Release Plan – An overview of the Production Release Plan is provided below. See the attached NICE DEMS Provisioning Strategy document, DSG Provisioning document and Customer Site Readiness document for further details.

System Implementation Planning (Production Cutover Planning) is detailed in the attached sample Project Management Plan.

DEPLOYING NICE DEMS, TESTING & TRAINING
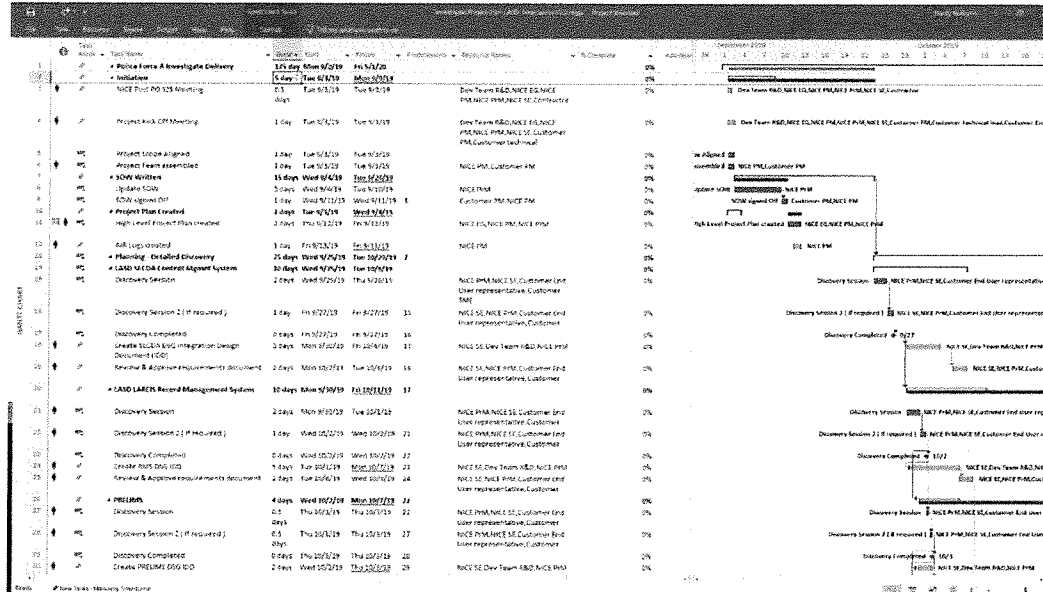
The deployment of your NICE DEMS solution is performed by specialist NICE installation technicians via secure remote access provided by COSB. Under the coordination of your NICE project manager, the NICE resource(s) are responsible for everything from the development of the connectors to your third-party systems (DSG), configuring and provisioning of the NICE DEMS application, testing and training, to final hand-off to your users and the NICE operations and support organization.

As agreed during the Planning phase, the NICE resources under the direction of the project manager shall remotely install the software for the DSG on COSB's premise environment. The NICE DEMS pre-production instances shall be set up in MS Azure as a unique instance for COSB.

The NICE resource shall establish connectivity between your third-party source system(s) as outlined in the detailed design and scope plan, then test the connection(s). Once the DSG environment is established and tested, NICE resources shall connect the DSG via secure link to COSB instance in MS Azure. The DSG connection to MS Azure along with the NICE DEMS pre-production instance shall be tested by the NICE resources to confirm the data in the NICE DEMS application.

As part of the use of NICE DEMS, historical data shall be very useful and helpful as a compliment to the current case data. Another key milestone is the identifying and acquisition of the historical data and then the migration of this data.

Validation and communication are critical path items to the success of the deployment. At each step in the deployment process, the NICE project manager shall be communicating with COSB project manager to provide status updates of the progress and completion of each task and validate. The validation is a two-step process where it first confirms delivery of an execution task in the delivery process and then ensures both parties are on track for the overall project delivery timelines as set forth during the Planning phase.

The testing and validating of the NICE DEMS solution shall be conducted by the NICE resource using the NICE Implementation Test Plan to verify that your solution is ready for training and COSB rollout.

135

They also provide full documentation of the details including all test results, the set up, and configuration of your solution are documented.

SYSTEM PRODUCTION - IMPLEMENTATION PLAN OVERVIEW

DEMS Software Development & Test (NICE responsibility)

DSG Connector Development & Test

- This initial testing will be done on the NICE DEMS deployment with access to test data provided by COSB.

DEMS SW development (as required)

- It is expected that DEMS SW development is minimal as the majority of required capabilities are already available in the released DEMS SaaS offering.

COSB Specific configurations (NICE responsibility)

Nice will implement COSB specific security, retention and matching rules that were established during the Project Planning Phase. Nice will perform unit testing to confirm adherence to user requirements.

- Security Rules
- Retention Rules
- Evidence Matching Rules

DEMS Deployment and Provisioning (NICE Responsibility)

- Azure Configuration
- Azure Deployment
- COSB Specific Provisioning

Site Readiness for Solution Deployment (COSB responsibility)

Installation of the Solution shall be performed via a remote access or on premise. Remote access is a key activity detailed on the NICE Site Preparation Checklist and is an implementation milestone.

Remote VPN access is required. Access to the Products is required when performing various installation and maintenance support activities for the Solution. Local administrative rights are also required for some installation activities and maintenance activities. On-site access may be necessary for certain activities.

This will need to be completed for each stakeholder agency location

- Environmental requirements defined
- Site readiness document delivered by COSB
- VM and remote access available to NICE

DSG Installation and Provisioning (NICE Responsibility)

Each stakeholder agency will have a DSG(s) deployed at their location to connect to their specified data sources. Scheduling of these deployments can be phased. NICE does not need to have all locations up and operational in order to begin COSB handover and rollout. It is

recommended that the COUNTY phase the agency cutovers based on COSB priority.

⚬ Install and Configure DSG connectors

DSG Testing (Joint NICE/COSB Responsibility)

This will be joint testing to ensure the DSG is collecting from data sources per COSB requirements. It is recommended that the COSB support this testing with access to the actual data source or a replica test database.

⚬ Test DSG Connectors

⚬ DSG Sign Off by COSB

COSB On-Boarding

There will be a separate onboarding for each stakeholder agency.

⚬ User Certificates Installed

⚬ User Provisioning/Test

COSB Solution Verification Testing – UAT (1-2 weeks per Stakeholder location) Project Handover

⚬ Close Air Logs

⚬ Close all site documentation revisions

⚬ Lessons Learned

Close Project

DELIVERABLES INCLUDE:

⚬ Solution Implementation Plan

— Installation and/or setup

— Solution Analysis and Design

— Solution Configuration

— Solution Build (e.g., data conversion, interfaces, reports/forms/dashboards)

— Testing (e.g., unit testing, system, UAT)

— Training

— Production Deployment (e.g., including possible phasing strategies, site specific considerations, and benefits and risks of strategy alternatives)

— Production Go-Live Support

— Post-Production Go-Live Support

⚬ DSG Connector development, turn up, testing

⚬ NICE DEMS Configuration

⚬ NICE DEMS provisioning and turn up/testing

⚬ Indexing of historical data

⚬ Testing and validating of the NICE DEMS solution using the NICE Implementation Test Plan

⚬ Complete COSB Training

- Weekly Project Status Updates
    - Tasks completed for the period
    - Tasks planned but not completed for the period
    - Tasks planned for next period
    - Upcoming COSB resource needs (90-day forecast)
    - Issues
    - Risks
    - Decision requests

Deliverable Expectations Document: Production Execution Phase - NICE Production Cutover Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Production Cutover Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *<Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
The objective of this plan is that the NICE DEMS solution shall go live and transition to service. At this stage, closure, the technical delivery of your DEMS solution is complete and the Training has been delivered. The NICE project manager shall conduct an introduction for COSB to NICE's Customer Support organization and processes. COSB shall be set up in NICE's Wiser Customer Case Management system and COSB shall be shown how to open a support case via the Wiser Portal in the event that COSB needs to raise a case for support.

Deliverable Scope / Content Expectations:
Requirements Traceability Matrix
The specific SOLUTION component (e.g., screen, report, workflow, data field, etc.) where the requirement is met
The test scenario(s) where the requirement is tested
The training module where instruction is provided for the requirement (if applicable)
<u>**Samples Enclosed:**</u> **Customer Site Readiness**

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** *The document is in full compliance with the approved DED and required content areas documented above.* **Rework Required:** *The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.* **Unacceptable:** *The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.*

CLOSURE AND COSB ROLLOUT

Objective - the NICE DEMS solution shall go live and transition to service.

At this stage, closure, the technical delivery of your DEMS solution is complete and the Training has been delivered. The NICE project manager shall conduct an introduction for COSB to NICE's Customer Support organization and processes. COSB shall be set up in NICE's Wiser Customer Case Management system and COSB shall be shown how to open a support case via the Wiser Portal in the event that COSB needs to raise a case for support.

During the review of the Wiser Portal, the NICE project manager with the assistance of the NICE Support Manager shall review COSB support process, severity definitions and associated SLAs to ensure COSB is aware of the process and support delivery obligations of the NICE Customer Support organization.

The following criteria shall be used to determine readiness for transition to COSB rollout.

*REQUIREMENTS TRACEABILITY MATRIX (**Exhibit A Attachment A – Requirement Traceability Matrix**)*

- The specific SOLUTION component (e.g., screen, report, workflow, data field, etc.) where the requirement is met

- The test scenario(s) where the requirement is tested

- The training module where instruction is provided for the requirement (if applicable)

Change Management Process

Any changes to the Solution design and scope following execution of this SOW may impact project dates resulting in additional product and Services fees, as well as elevated risk to the project.

Changes to the Solution design, project scope, project dates, and any associated project dates, and any associated additional charges and/or costs must be mutually agreed upon in writing prior to the performance of any Services related to such changes, and shall only be valid when agreed upon in writing by both parties using the Change Order Request Form in Appendix D of this SOW. All changes to Services scope are subject to resource availability.

NICE utilizes a collaborative approach to gain agreement on the appropriate processes, policies, and standards. In establishing the Change Management service, NICE will work with the key stakeholders within COSB to review with them:

- NICE's standard Change Management processes and procedures, compared with existing COSB policies, processes and procedures

- Specific COSB requirements

- Any current points of pain and opportunities for process improvement

- Any gaps between COSB required process elements and the NICE standard process.

The output from this will be a clear policy document that is agreed with NICE and COSB and will form the basis of process reviews.

NICE believes this inclusive approach to process design brings wider long-term benefits than simply imposing a process on COSB. This approach supports NICE's principles of collaboration and communication, working as a cohesive team with the support of COSB towards a common

goal.

NICE's end to end, ITIL aligned Change Management process is clear, easy to engage with and minimizes the bureaucracy that can traditionally be associated with Change Management. NICE mandates that all stakeholders interact with the process and will not hesitate to veto any change requests that do not follow required impact assessment and approval processes.

CATEGORIZING CHANGES

NICE will implement a standard ITIL-aligned approach to categorization of change, tailored for COSB 's business and designed to simplify and streamline the change management process without introducing risk.

The process will include specific procedures and work instructions for identifying and handling any change required to correct an existing or potential fault with the Solution or provided as a necessary improvement to the application. This includes:

- Emergency change

- Normal (operational change)

- Standard change

- Project change – minor, significant and major.

When projects are ready for release into the production environment, they must also follow the operational change process so that the impact of the release into the live environment can be assessed and any user impact minimized.

EMERGENCY CHANGE

When an Emergency Change is requested, NICE will adopt a pragmatic approach to the implementation to restore services to users as quickly as possible without compromising the integrity and security of the infrastructure. Work may be undertaken in advance of confirming commercial arrangements, subject to written authorization from a suitably empowered COSB representative who attends the Emergency Change Advisory Board (CAB) meeting.

OPERATIONAL CHANGE

Operational changes will be raised either for preventative maintenance or to resolve an open incident or problem record. In every case, if there is impact on service, such as any kind of outage, or a significant risk to service, NICE processes will dictate that such changes must be approved by COSB.

STANDARD CHANGE

The Supplier considers standard changes to be operational changes that are frequently occurring, carry little or no risk and have fully understood and documented implementation.

To achieve an efficient end-to end-change management process, NICE will work with COSB to identify such Standard Changes and agree on reduced authorization levels, or even remove the need for release approval so that these changes can be implemented quickly, with minimum bureaucracy. This will deliver an expedited delivery timescale, and reduce the cost associated with re-creating the same Change detail repeatedly.

During transition, NICE will collaborate with COSB to create the associated change models and work instructions. Thereafter, any potential additions to the standard change category will be approved prior to re- categorization.

PROJECT CHANGE

Any releases to the live environment must be approved by COSB including those handled by project managers. Project release requests must include comprehensive information on the new or changed service, proof of testing, success criteria and evidence that the Service Desk, as well as all involved support teams have accepted the new or changed service into support.

The Project release request will include a detailed plan explaining the suggested timetable of events, roles and responsibilities, software release notes, knowledge transfer requirements, and any additional pertinent information required for COSB to understand and approve the change process.

This rigorous acceptance into the service process protects the live environment and ensures that new or changed services are not only functional but also able to be supported. In NICE's experience, this approach is vital in a multi-supplier environment to ensure full end-to-end communication of any changes to process or service.

REPORTING AND MEASUREMENT

A number of Change Management Key Performance Indicators (KPIs) are tracked as standard. These allow NICE to measure not only compliance to contract, but also the efficiency and effectiveness of NICE's process and service, thus contributing greatly to the Continual Service Improvement (CSI) approach. This will help NICE maintain visibility of any risks involved in changes to ensure business continuity is managed through change.

Examples of KPIs tracked using the Change Module of Remedy (used by NICE) include but are not limited to those listed below.

Description	How and Why
Completion of Change Impact Assessments	Drives behaviors necessary to push through change related technical and assessment work in a timely manner
Number and percentage of Changes rejected	Good indicator of how the process is working
No. of Incidents traced back to Changes	This KPI directly supports the goal of Change Management, minimizing the impact of Change-related incidents.
Number and percentage of Emergency Changes	A high occurrence of Emergency Change might be an indicator for other issues.
Number and percentage of Changes successful	Total number of successful Changes, and relative to the total amount of requested Changes
Number and percentage of Changes rolled-back (incl. reasons)	Total number of Changes that were rolled-back during implementation (failed changes)
Time taken to approve	Useful indicator of the timespan of a CHG if NICE and the COUNTY can agree upon average timings for different types of CHG

SUMMARY

Change is not only inevitable but required and should be celebrated where it brings about

142

improvements to the overall service to COSB. NICE will collaborate with all technical teams to facilitate change quickly and easily and with minimal risk. NICE will ensure that the management of change is effective, efficient and has minimal disruption to COSB.

Task 8 Risk Management

Contractor shall provide the following Risk Management sub-tasks and deliverables:

Task 8. Risk Management Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
8.1	**Risk Management Planning**	Contractor shall develop a Risk Management Plan to describe the approach to ensure that risks /issues are reported, tracked and resolved.	The **Risk Management Plan** shall describe the approach to ensure that risks/issues are reported, tracked and resolved. **The Deliverable shall include a DED.**

DELIVERABLE EXPECTATIONS DOCUMENT (DED):
NICE Risk Management Plan

Project Deliverable Number: <Insert - TBD>	Title of Deliverable: Risk Management Plan
Draft Submission Due Date: <Insert – TBD, as mutually agreed >	County Draft Review & Comment Period: <Insert - TBD>
Final Submission Due Date: <Insert – TBD, as mutually agreed >	County Final Review & Comment Period: <Insert - TBD>
Reviewed By Required: <Yes/No – by whom –TBD as mutually agreed >	Deliverable Document Format: < Word / PDF>
Deliverable Owner (County): <Name, Role – TBD, as mutually agreed >	Deliverable Author (Vendor): <Name, Role - – TBD, as mutually agreed >
Deliverable Description and Purpose: Risk Management is carried out on all NICE projects to identify, address, and eliminate sources of risk before they become threats to successful project completion. The Program Manager leads the Risk Management Process by taking input from the project team and is responsible for progressing the plans to manage the risk. A Risk Register is created during the project's planning phase and is used throughout the project to support the capture, analysis, monitoring and control of project risks.	

Deliverable Scope / Content Expectations: NICE will provide full documentation of risk tracking and monitoring details as relevant to your solution. The deliverables will include: • NICE RISK MANAGEMENT PLANNING • TRACKING RISKS AND LESSONS LEARNED • DEFECT TRACKING • NICE DISASTER RECOVERY PLANNING • NICE DEMS'S RESILIENT CLOUD ARCHITECTURE – MITIGATING THE RISK OF SYSTEM DOWNTIME Sample Enclosed: See Sample Risk Register Screen Image on the following page.	
References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.
Deliverable Criteria	**Acceptable:** The document is in full compliance with the approved DED and required content areas documented above. **Rework Required:** The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved. **Unacceptable:** The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

NICE Risk Management Planning

Risk Management is carried out on all NICE projects to identify, address, and eliminate sources of risk before they become threats to successful project completion. The Program Manager leads the Risk Management Process by taking input from the project team and is responsible for progressing the plans to manage the risk. A Risk Register is created during the project's planning phase and is used throughout the project to support the capture, analysis, monitoring and control of project risks.

A baseline Risk Assessment along with this Risk Management Plan and Risk Register are all a part of the detailed Project Plan that will be created for this solution deployment. NICE will work with SBCO stakeholder agencies to establish an initial Risk Register identifying potential risks along with the recommended risk mitigation approach for each.

In addition, NICE's approach to managing, identifying, mitigating and tracking risk when implementing new solutions includes ongoing and updated documentation of all aspects of the project:

- A project plan detailing all phases and planned activities is developed by the NICE project manager and distributed to all stakeholders, and is updated as changes to the project occur

- A checklist with open activities is updated every 2-4 days to ensure schedule adherence

- An issues log is maintained by the NICE project manager to ensure that any outstanding issues are tracked and addressed timely

- Change orders are required throughout the implementation plan to clearly track and log all change requests

Throughout the project there are regular project reviews between the project managers and other team members as relevant to project stages. The risk register will be reviewed at these meetings to ensure timely mitigation of risk items.

Example of NICE Risk Register:

TRACKING RISKS AND LESSONS LEARNED

Since NICE's first DEMS deployment, NICE has gathered many insights on how to improve NICE's execution of each stage of NICE's deployment process, which then also translates to improved risk management. Following are just a few of the risk areas that NICE has encountered along with mitigation steps that were taken and ongoing changes implemented so as to lessen the opportunity for these same risks to occur again.

These items will be included as a part of the Baseline Risk Assessment for the SBCO DEMS Risk Management Plan.

EXAMPLES OF PREVIOUS PROJECT RISKS, RESOLUTIONS AND LESSONS LEARNED

Site Readiness

The most common risk associated with project management is the site not being fully prepared for system implementation. To mitigate this risk, NICE develops a formal statement of work that documents all technical configuration details and environmental dependencies, which is required to be approved by both NICE and COSB.

Further, since implementation cannot take place at an unprepared site, COSB will verify with a signed **site survey and preparation** document that the site is fit for implementation. The NICE project manager also ensures that your organization has the critical people represented on the implementation project team.

Accessing database structure or needed API for DSG connectors

- The risk is that some vendors do not support open access to data stored in their platforms or the database structure is not known by COSB. In such cases, vendor involvement is required to support the NICE Investigation integration.

- **Risk Mitigation plan** – early in the project NICE will request copies of the database structure or copy of the APIs for each database to which NICE DEMS will connect.

Feature gap between COSB expectations and what is delivered

- The risk is that the deployed solution does not deliver to the COUNTY's expectation

- **Risk Mitigation plan** – COSB involvement is critical in the Project Initiation and Project Planning phases. During these early phases in the project, the County and NICE work closely together to finalize the project statement of work, and to actively participate in discovery sessions. It is important that COSB provide the appropriate personnel to ensure requirements are properly stated, understood, and documented by NICE.

Users not utilizing the system as expected to obtain desired solution benefit for the organization

- The risk facing users that do not fully adopt the system may never realize the benefit of the platform, or only realize a limited fraction of the solution's potential for improved productivity and accuracy of investigations.

- **Risk Mitigation plan** - Training and awareness are key activities to mitigate this risk. With NICE DEMS, awareness begins day one. NICE will hold awareness meetings with all key stakeholder groups, with the objective to educate them on the value they will realize by learning to use the new platform.

- **A robust training plan.** NICE will ensure that users are properly prepared to access the value of NICE DEMS. Training incorporates specific scenarios relevant to COSB, and entails working with actual COSB data, so that investigators may progress their cases while they are in training, with personalized guidance from the trainer and consultant.

146

NICE Disaster Recovery Planning

NICE DEMS'S RESILIENT CLOUD ARCHITECTURE – MITIGATING THE RISK OF SYSTEM DOWNTIME

Success in today's public safety climate requires high availability, efficiency and compliance of people, technologies, and processes. The COUNTY's focus on protecting communities and resolving crime are County priorities. NICE shall support the COUNTY by improving the COUNTY's operational efficiency through a combination of technical innovation and assured reliable performance of the NICE DEMS solution.

To accomplish this, **NICE offers very extensive experience in creating and managing projects and service portfolios, supporting the full lifecycle of its DEMS Solution and services** – in cooperation with end users for the best possible match between NICE's technologies and services and agreed to performance targets.

Since the combination of each COSB's project objectives, operational conditions, and associated resources is different, NICE's deployment teams are empowered to work with the relevant agencies to craft tailored deployment service plans while leveraging the expertise reflected in approved methodology, tools, and processes for quality project implementation.

Your organization is empowered to optimize the NICE platform management, minimize system downtime, and meet regulatory compliance standards while keeping your IT costs down throughout the ownership lifecycle – with NICE's mature, proven mix-and-match service portfolio and in cooperation with a team of experts that is fully focused on the mission-critical needs of public safety and government organizations.

NICE DEMS is the industry's most comprehensive cloud-based solution for managing investigations and digital evidence, leveraging the ultra-secure Microsoft Azure Government cloud. NICE DEMS meets the FBI's rigorous CJIS (Criminal Justice Information Services) requirements. It has earned the CJIS ACE Compliance Seal from Diverse Computing for NICE DEMS following a rigorous 553-point review of the solution.

NICE DEMS adds little burden to your IT team. Since the solution is hosted in the secure Microsoft Azure Government cloud, it requires much fewer resources to maintain when compared to traditional on-premise applications. NICE's secure, cloud-based deployment model also gives you:

- **Improved accessibility of information** - NICE DEMS promotes collaboration among satellite agencies, communities, investigators and prosecutors by centralizing access to information, enhancing the effectiveness of law enforcement.

- **Confidence in Data Security with Criminal Justice Information Services (CJIS) compliance** – NICE has earned the CJIS ACE Compliance Seal from Diverse Computing for NICE DEMS, following a rigorous 553-point review of the solution. Microsoft Azure Government is the first hyper-scale commercial infrastructure cloud platform contractually committed to meeting FBI's CJIS security requirements for federal, state, and local governments. NICE's collaboration with Microsoft allows law enforcement agencies to use this secure cloud platform to help safeguard digital evidence and ensure the integrity of investigations.

- **Operational agility** – the solution is ideal for agencies with growing or fluctuating case load and demands. If your case load increases or storage needs increase, you can instantly

147

scale up your cloud capacity, drawing on the service's remote servers. Likewise, if you need to scale down again, the solution is inherently flexible to support that need.

- **Automatic software updates and virus checking** – NICE DEMS servers are off-premises, out of sight and out of your police department's hair. As your software-as-a-service provider, NICE takes care of all of the regular software and security updates, saving your agency time and resources and freeing you up to focus on what really matters.

NICE shall provide implementation, maintenance, and support of the DEMS solution for the period as stipulated per master terms and conditions.

NICE's services shall include (at a minimum):

- Provision of upgrades, including enhancements and new features
- Service desk support (refer to the Table 2: Service Levels below)
- Defect correction
- Impact analysis of upcoming patches and upgrades
- Modifications to NICE provided components and configurations to support upcoming patches and upgrades
- Testing and deployment of patches and upgrades in all environments
- Continuous health checks of the production system
- Continuous tuning and other required system level administration
- Recommendations for system performance tuning
- Application modifications required to support scheduled infrastructure upgrades

As part of the default offering, NICE DEMS is based upon Microsoft Azure Technologies, and leverages Azure's resilience features, minimizing the risk of downtime due to availability of cloud resources.

Microsoft Azure provides transparent resilience for storage and queues which form the core of the NICE DEMS infrastructure. All data is synchronously replicated across three different storage nodes within the same Azure datacenter.

The NICE DEMS specific code runs as multiple load balanced instances of each of the front and back-end services. It is designed to handle short term connection outages with automated retry policies.

There are also redundant copies of all media and metadata within a data center.

In addition, the DR solution includes Geo-redundancy, providing the ability for failover to another datacenter if required. The recovery process results in a short period of downtime of less than 4 hours for a catastrophic data center outage.

NICE DEMS's disaster recovery solution (DRS) includes everything required for failover, including the necessary operation of system software, deduplication storage, and recovery hardware.

NICE DEMS within a Single Data Center:

Default Resilience
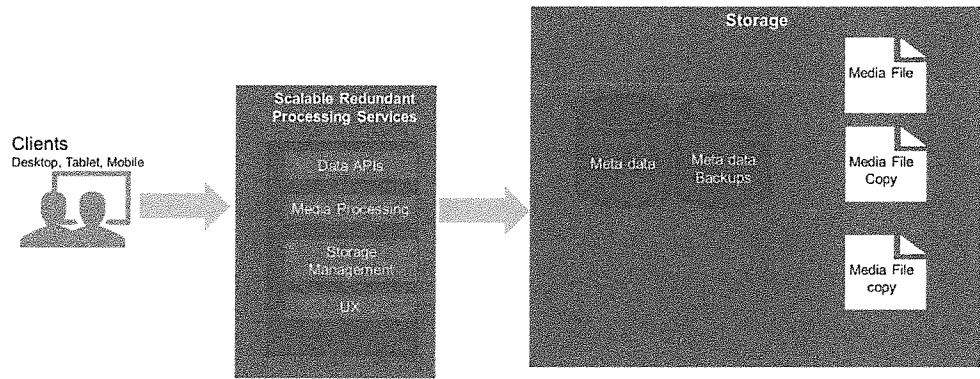
NICE DEMS with Geographic Redundancy:
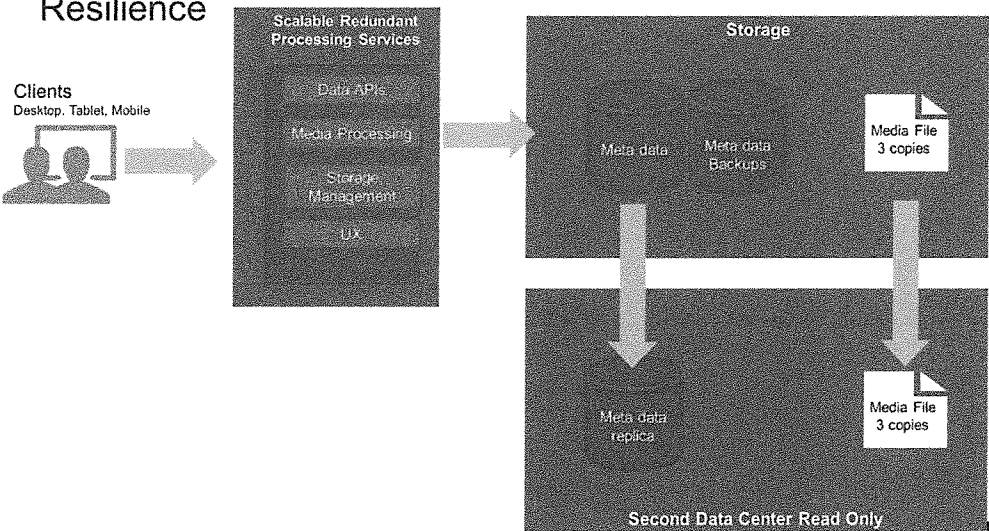
Resilience

The NICE Operations organization is in constant monitoring and tuning state of the NICE DEMS solution in the Azure Cloud to ensure the reliable daily use for COSB. This organization is also making routine and scheduled updates to ensure COSB has both the solution availability of 99.9% and the key feature set for COSB users as per the agreement. The two organizations have a seamless process to handle all solution incidents in Azure through to COSB-raised support cases.
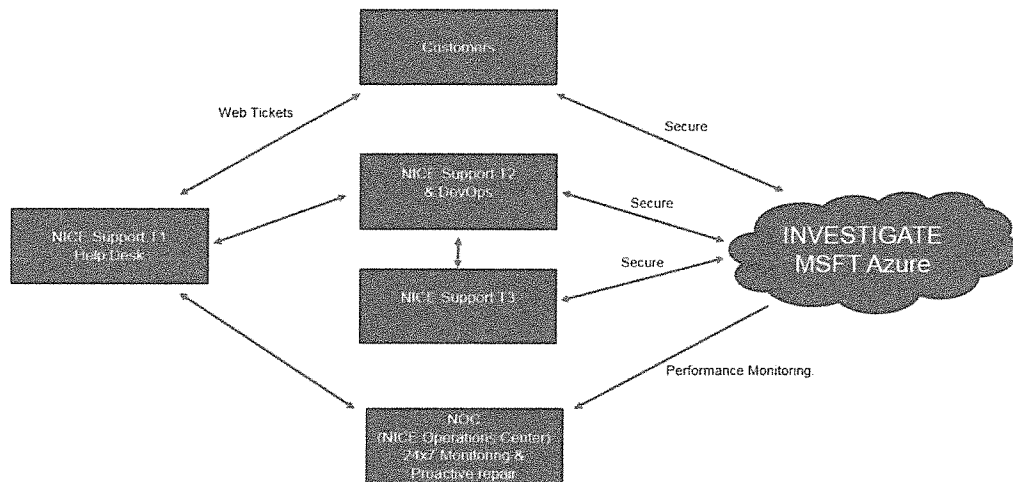
NICE shall be subject to the following response requirements for production issues reported by COSB:

Level	Level Definition	Response Requirement
Level1	An error, malfunction or other deficiency that meets both of the following criteria: The deficiency significantly impairs COSB's normal business operations; diminishes employee safety or well-being; exposes COSB to significant liability or risk; significantly increases the cost, decreases the value, or impedes the efficiency of COSB resources or operations; or significantly inconveniences COSB customers. No workaround is currently developed, implemented, and accepted to alleviate the deficiency's impact.	• NICE shall acknowledge emergent issue within one (1) hour. • NICE will attempt to resolve emergent issue within four (4) hours. • NICE will provide continuous best efforts and updates until the issue is resolved.
Level 2	An error, malfunction or other deficiency that meets both of the following criteria: The deficiency causes substantial inconsistencies, irregularities, inefficiencies, or potential for mistakes, but does not meet the criteria for a Level I Priority. No workaround is currently developed, implemented and accepted to alleviate the deficiency's impact.	• NICE shall begin taking action towards a resolution within a time period of 5- 24 hours. • NICE will attempt to resolve emergent issue within 5-24 hours. • NICE will provide ongoing and diligent best efforts and updates until the issue is resolved.

Level 3	An error, malfunction or other deficiency that does not meet the criteria for Level I or Level II Priority, but causes system response time to fall below fifty percent (50%) of system response time requirements for more than four (4) hours per month	● NICE shall successfully implement a resolution within a period of thirty (30) days.
Level 4	An error, malfunction or other deficiency that has little or no immediate impact on COSB's business operations, costs, risks, employees, or customers, but is desirable for the long-term viability and utility of the system	● NICE shall successfully implement a resolution within a period of ninety (90) days.

NICE DEMS is a SaaS offering and is fully managed by NICE Services team in conjunction with Microsoft Azure Cloud Services. All recovery procedures are the responsibility of NICE and Microsoft. COSB is notified of any service disruptions along with information of service recovery. No actions are required on the part of COSB for addressing NICE DEMS Service interruptions.

Task 9. Quality Control

Contractor shall provide the following Quality Control sub-tasks and deliverables:

Task 9. Quality Control Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
9.1	**Quality Control Planning**	Contractor shall establish and utilize a comprehensive Quality Control Plan to assure the County a consistently high level of service throughout the term of the Contract	The Quality Control Plan shall include, but may not be limited to the following: • The County's management of the requirements. This includes the identification of inconsistencies between the requirements, and the project's plans and work products • A record of all inspections conducted by the Contractor, any corrective action taken, the time a problem was first identified, a clear description of the problem, and the time elapsed between identification and completed corrective action, shall be provided to the County upon request • The County's requirements traceability matrix that will be used for requirements management, and will map where in the software a given requirement is realized or implemented • include: baseline control and monitoring the software library. Approved changes to baseline software and/or documentation shall be made properly and consistently in all products, and no unauthorized changes are to be made • **The Deliverable shall include a DED.**

Deliverable Expectations Document (DED): NICE Quality Control Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Quality Control Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Draft Review & Comment Period:** *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Final Review & Comment Period:** *<Insert - TBD>*

Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	**Deliverable Author (Vendor):** *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
The purpose of this document is to specify the plan for quality activities related to NICE Public Safety Software products, in this case, specifically the NICE DEMS SaaS Solution.

Deliverable Scope / Content Expectations:
NICE will provide documentation describing NICE's Quality Control / Software Quality Assurance. The deliverables will include:

- NICE QUALITY CONTROL PLAN:
  - SOFTWARE RELEASE LIFECYCLE
  - TESTING STRATEGY AND PLAN
  - SOFTWARE CONFIGURATION MANAGEMENT
  - CHANGE MANAGEMENT
  - SOFTWARE SECURITY
  - TOOLS
  - RESPONSIBILITIES
  - KPI, MEASUREMENT

Sample Enclosed:

The entire NICE Quality Control Plan is a 'sample' – NICE uses the same process for all software development, for all customers.

References / Standards	NICE Software Testing and Quality Standards based on ISO 9001 guidelines, ISO 90003 (guidelines for the application of ISO 9001:2000 to SW engineering), mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.

Quality Control Plan – Purpose and Scope

The purpose of this document is to specify the plan for quality activities related to NICE Public Safety Software products.

NORMATIVE REFERENCE

This plan covers the requirements of ISO 90003 (guidelines for the application of ISO 9001:2000 to SW engineering), section 7.1.2 – Quality Planning.

Reference to relevant sections of standards (ISO, etc.) and regulations.

RELATED DOCUMENTS

- NICE solution Life cycle definition

- NICE solution Release Testing Strategy
- Change control process

TERMS AND ABBREVIATIONS
- CR Change Request
- EA Early Availability
- GA General Availability
- KPI Key Performance Indicator
- NPL NICE solution Life Cycle

QUALITY REQUIREMENTS
NICE PUBLIC SAFETY SOFTWARE Products need to meet the following basic requirements:

- Meet market needs – cover the marketing requirements for each release
- Release quality products – no open showstopper defects when releasing a product
- Release on time – according to the agreement with Product Manager

Software Release Life Cycle

The NICE DEMS SaaS Software release cadence is to release 2 to 3 New Feature releases each year. Additional maintenance and bug fix release are planned as needed throughout the year.

The Life Cycle for NICE PUBLIC SAFETY SOFTWARE product releases is called NPL – NICE Solution Life Cycle. The objective of the NPL is to standardize the practices and processes used during the Product Lifecycle and to serve as a planning and execution framework to ensure meeting the quality requirement stated above.

Software development work required for COSB specific DSG integrations will also follow this process.

The following diagram illustrates the NPL:
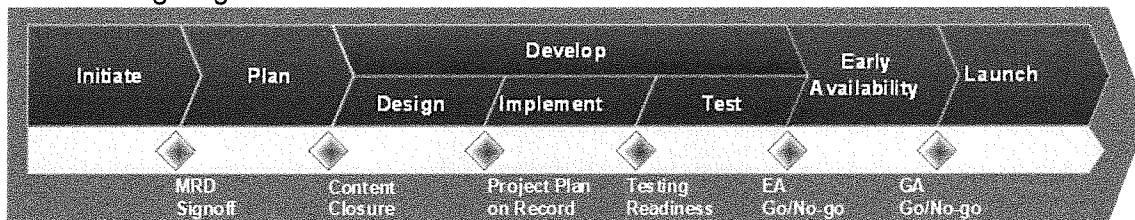
The NPL is built upon a set of major phases; each one ends with a major gate (review). Following is a short description of each phase and the relevant gate at the end of it:

Phase	Description	Relevant Gate which ends the phase
Initiate	Provide validated marketing requirements and business justifications for the new product	MRD sign-off

	version which meets the overall product strategy over time.	
Plan	Define an agreed scope and timeline for the new product version.	Content closure
Design	Provide a written detailed specification and design for the selected release content and agree on Project Plan on Record	Project Plan On Record (PPOR)
Implement	Implement and release content by incrementally developing high quality source code.	Testing Readiness
Test	Run end-to-end system test to ensure that the content of release specification is fully matched with the product implementation.	EA Go/No-Go
Early Availability	Assess the new product version in a well-controlled environment.	GA Go/No-Go
Launch	Launch the new product version for wide distribution. Maintain continuous support for NICE customers to ensure high satisfaction over time.	N/A

Following is the release timeline:
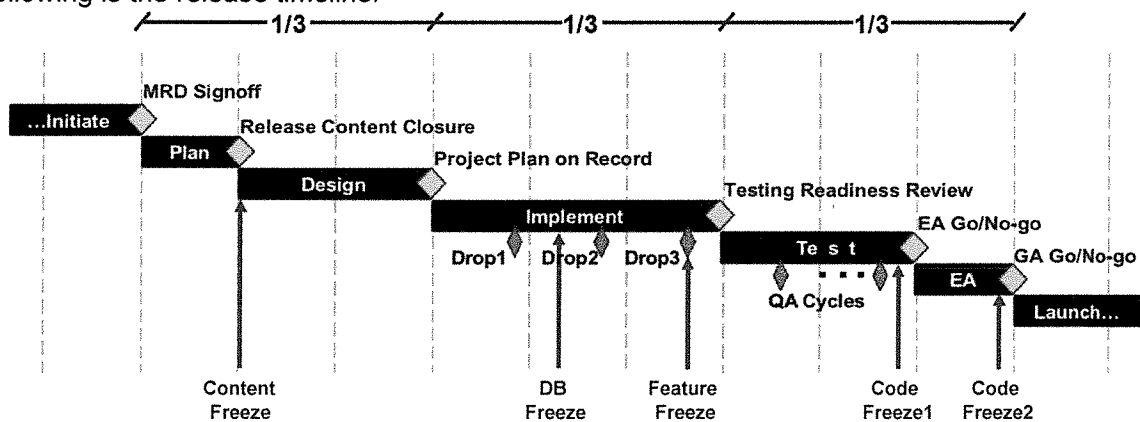
Refer to the NICE solution Life Cycle (NPL) for more details on the activities and reviews in each phase – link on the next page.

Team Structure
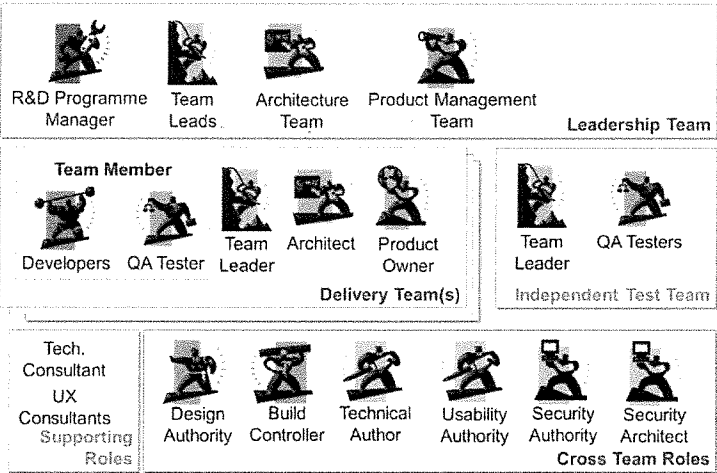
Product Lifecycle Process - Deliverables
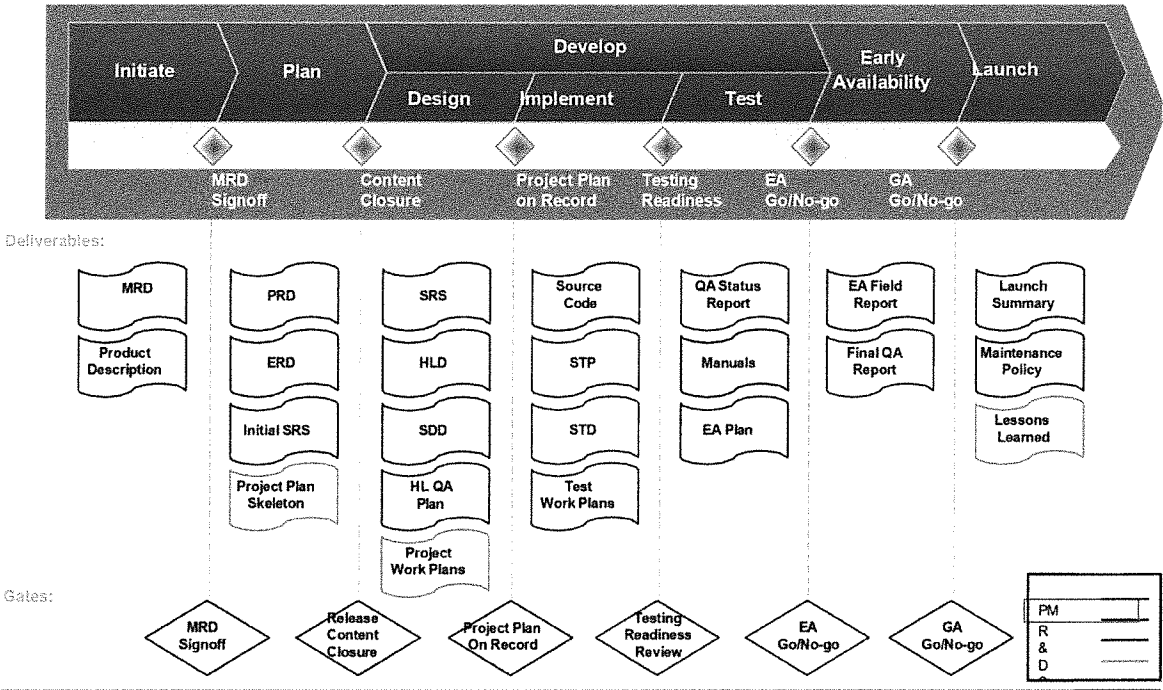
Cross-functional delivery teams exist, in alignment with agile development processes. Each team ensures all new DEMS functionality is well tested, and the Independent Test Team looks across the teams, identifies risks and determines what additional testing might be needed.

The DEMS development team has chosen to follow a disciplined agile approach which has a risk driven lifecycle and a governance framework to address the specific needs for technically complex Public Safety solutions.

Development Process: Gate Reviews and Quality Plans

* Gate Review: 4 gates: readiness for evaluation, development, transition and release
* Process defined in terms of activities, roles, deliverables and principles.
* Project quality plans capture the specific implementation of each project
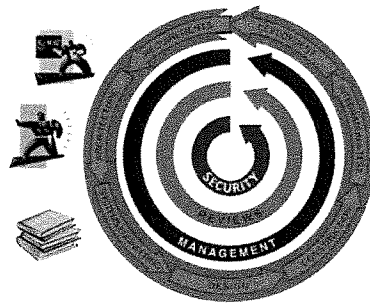

"Consider quality & security early"

"Take time to communicate"

"Change the process"

Certified to:

ISO 9001 Quality Management
ISO 27001 Information Security

13

Software development gate reviews provide decision-making checkpoints at each critical step along the software project lifecycle. These gate reviews provide a consistent and systematic mechanism for effective reviews by pre-defining required deliverables and activities that must be met at each gate (documented entry and exit criteria). They also provide a methodical mechanism for early identification of problematic issues and risks. Decision-making is fact based with verification of readiness and status at each critical milestone.

This process has proven to enhance the overall quality of NICE R&D deliverable software.

Quality Assurance: Product Test

* Test documentation tailored to meet the IEEE829 Standard for Software and System Test Documentation
* Test is intrinsic to the project from evaluation to release, with a commitment to 'test' throughout all lifecycle stages
    * Requirements review by all key stakeholders, including QA engineers
    * Test strategy agreed prior to exiting evaluation
    * Peer code reviews – conducted throughout development
    * Design reviews
    * Unit testing
    * Integration testing and System testing
* Test metrics fed back into the project quality metrics and analyzed as part of the release criteria

NICE

Testing Strategy

1.1 UNIT TESTS

Unit tests are done by developers in separate/standalone environments, or by using simulators/test tools. Every new code is unit tested before submission to integration tests. In addition, every major change to an existing component undergoes a set of unit tests.

1.2 INTEGRATION TESTS

Integration tests are done by developers from different teams. Every new feature undergoes integration tests before system tests are started.

1.3 SYSTEM TEST

1.3.1 Scope

The scope of the system tests is shown in the following diagram:

Applications							
S&R						**IBA**	
Localization	PBO and Compliance Suite enhancements	Reports	SOD	Actimize SDK	BSF	KPI Management-My Universe	Business Analyzer-raphical call chain
	Request on behalf	Errors Accuracy Summary Repor	Total, Interaction base recording Voice and screen	Single Sign on		Packages	Reporter
	Customizable email notification	Errors Accuracy Trend Report	ROD	Link from ACT to NP		Desktop assistant - SS	Notifications
	Customizable email addresses	Errors Distribution Pareto Report	Monitor and playback			Quality Plan	
		Business Issue Error Accuracy Trend Report	Screen content analysis				

1.3.2 Test Objectives

The objectives of the testing activities are as follows:

- Verify products against their requirements.
- Validate that the product performs as expected.
- Ensure system components and business processes work end-to-end.
- Build a test model that can be used on an ongoing basis.
- Identify and resolve issues and risks. 1.3.3 Testing Approach

The objectives of the testing activities are as follows:

The testing period is divided into 2 cycles to ensure quality prior to the EA phase.

- The first cycle supports finding the maximum issues in short time, in order to allow R&D sufficient time to solve and stabilize the product.

• The second cycle focuses on regression and stability of the EA candidate product.

1.3.4 Test Preparation

The purpose of Test Preparation is to verify that requirements are understood and to prepare for Test Execution. This sub-phase is conducted during the design phase.

The types of tests covered:

• Operational Readiness tests

• Sanity Tests

• Functionality Tests

• Compliance tests (compliance to standards)

• System Tests (end to end, with a copy of semi-real database)

• Performance tests

• Automated tests 1.3.5 Test Execution

The purpose of Test Execution is to execute the test cycles and test cases created during the Test Preparation activity, compare actual results to expected results, and resolve any discrepancies.

This sub-phase includes the following activities:

• Set up environments

• Verify entry criteria

• Conduct tests

• Compare actual results to expected results

• DEMS and resolve discrepancies

• Conduct regression test, performance and long term

• Verify exit criteria – EA Gate criteria (Early Availability)

1.3.6 Test KPIs

The following KPIs measure the effectiveness & efficiency of the system testing activity (for more details refer to NICE solution testing strategy document):

• Test Case preparation productivity (designed steps per hour)

• Test Execution summary (% pass/fail/not run)

• Defect Acceptance (% of valid defects submitted by testing engineers)

• Defect Rejection (% of rejected defects)

• Test Efficiency (% of defects identified during testing out of total number of defects in the product, including post-release defects)

- Defect Severity index. This is a weighted severity index calculated for open defects at the time of release. The weights are: Showstopper = 10, Severe = 7, Medium = 2, Minor = 1

- Automation Test Execution productivity

- Automation Coverage

1.3.7 Acceptance Tests

The first installations of a specific release are installed during a phase called Early Availability (EA). During EA, COSB conducts acceptance tests, and the results of those tests are reviewed by R&D in order to verify that the product has been validated successfully.

Software Configuration Management

NICE PUBLIC SAFETY SOFTWARE configuration management (SCM) is managing NICE PUBLIC SAFETY SOFTWARE product in development projects. The SCM system is maintaining codebase, changes (AKA tasks), version lines, stages and baselines.

The SCM solution in NICE PUBLIC SAFETY SOFTWARE is IBM® Rational® Synergy. This environment is a task-based software development and delivery solution that brings together global, distributed development teams on a unified change, configuration, and release management platform.

The development process includes "tasks check-in" operation. This is an entrance operation of code change to the product's codebase. There is a recommendation to link tasks to Synergy CR, representing defect, feature, or sub-feature.

1.4 BUILD FACTORY

The build factory is a centralized unit performing product end-to-end build. Builds are executing in a well-defined periods depending on the product lifecycle. For example, while debugging, there is a daily centralized build.

The build process includes code checkout, compilation, linkage, deployment, and package and sanity test level0 performance. Each step can break the build.

Change Management

Change management during the product life cycle is conducted according to the change control process. The requested changes are submitted to a centralized DB where submitters, reviewers & approvers have the ability to review and approve each CR.

High-level flowchart of the process:
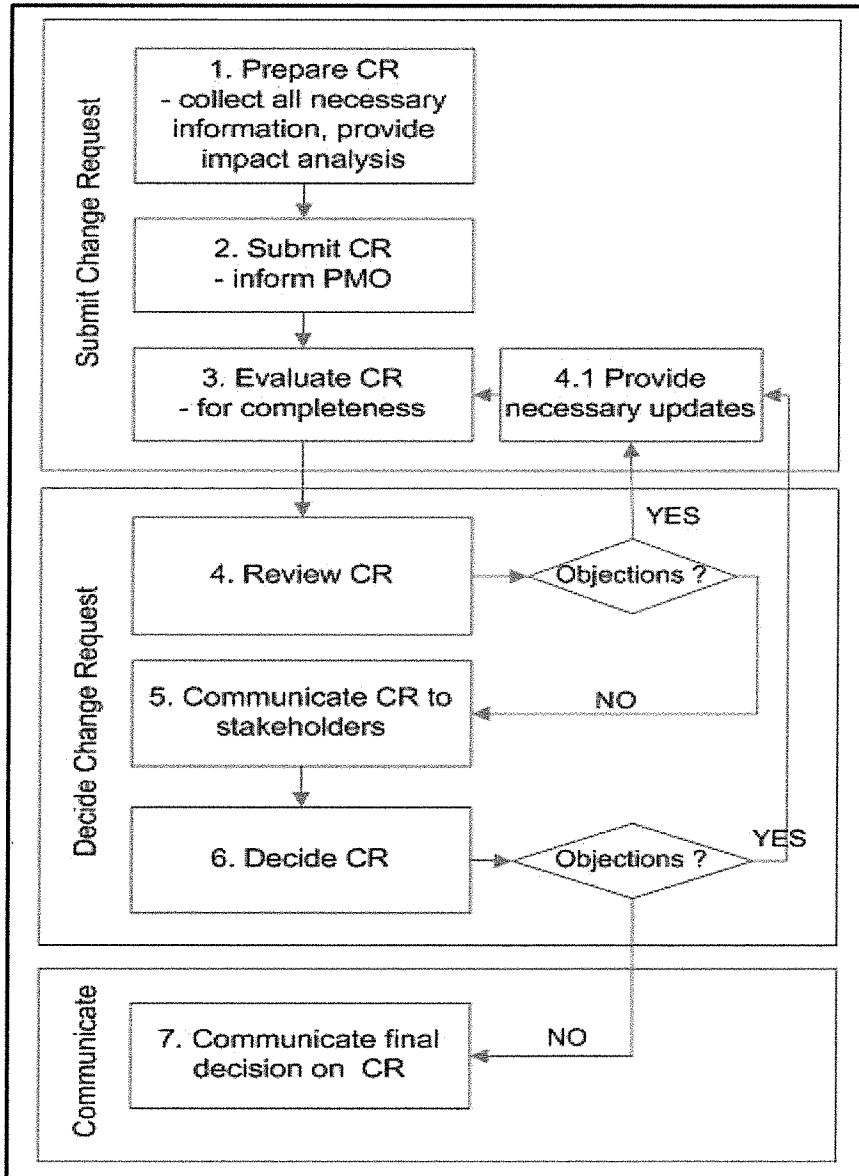
For additional information, please refer to the change control process.

Tools

In order to assist with achieving the desired SW product quality, the NICE PUBLIC SAFETY SOFTWARE division uses the following tools:

Development Process: Tools and Technologies

* Closely aligned to the Microsoft technology stack

Programming Language	C#
Software Framework	.NET
Application Lifecyle Management Work-flow, requirements, defects, test	Team Foundation Server (TFS)
Version Control	TFS/Git
Build Control	Team City
Open Source Software Vetting	Black Duck
Security Scanning	Nessus

Continuous Integration

* Developer checks in the code
* Build is triggered
* Compilation completes
* Build Verification Tests are executed

14

NICE

Responsibilities

The responsibility of each employee is to provide a quality product/sub-product that satisfies the requirements and quality level agreed upon with his internal customer.

The corporate quality & compliance group conducts control activities over the NICE PUBLIC SAFETY SOFTWARE activities. This includes: ISO audits (internal/external), KPIs, and case studies/root cause analysis. The group also maintains the ISO 9001 certification of the company (NICE is certified to ISO 9001 since 1998).

SW security

NICE is certified for ISO 27001 (Information Security management system) and is being audited on a yearly basis by the "Standards Institute of Israel" (SII).

KPIs/Measurements

The following KPIs are measured for all NICE PUBLIC SAFETY SOFTWARE products:

* Released defects
* Release On Time Delivery
* % readiness of NPL gates

Task 10. Production Control and Transition Plan

Contractor shall provide implementation, maintenance, and support of the production DEMS during the Term. Additionally, Contractor will provide system support until all the stipulations below are met and the System has been accepted by the County.

Contractor shall provide the following sub-tasks and deliverables:

Task 10. System Warranty Sub-Tasks and Deliverables

Task #	Sub-Task	Descriptions	Deliverables
10.1	**Software Transition Planning**	Contractor shall provide a comprehensive Production Support and Transition Plan (Software Transition Plan) complying with IEEE 12207.2, section 5.3.3 - system architectural design.	The **Software Transition Plan** will describe how the Contractor intends to support DEMS and transition that support over to the responsible County entities. This should include a description on how to ensure the County resources are capable to support the system.
10.3	**System Acceptance**	• The resolution of all documented Contractor- responsible deficiencies as stipulated through the approved defect and issue tracking process. • DEMS successfully performs in the production environment for a period of one hundred and eighty • (180) consecutive business days without any level 1 or level 2 deficiencies. • All integrations have been run successfully three (3) times without any level 1 or level 2 deficiencies. • Knowledge transfer and training for end users and technical support staff has been provided. • The successful completion of all other work breakdown structure elements, tasks, and deliverables as specified in the Contractor project schedule as approved by the County.	Once all System Acceptance conditions have been met, Contractor shall provide to the County for approval, a System Acceptance document that shall include a final Requirements Traceability Matrix identifying all System requirements allocated to current, in-production System components. Sign-off of this document by the County will constitute System Acceptance and trigger the beginning of Maintenance and Operations.

Deliverable Expectations: NICE Production Control and Transition Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: Production Control and Transition Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Draft Review & Comment Period: *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	County Final Review & Comment Period: *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	Deliverable Document Format: *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	Deliverable Author (Vendor): *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:
Under the coordination of your NICE project manager, the NICE resource(s) are responsible for everything from the development of the connectors to your third-party systems (DSG), provisioning of the NICE DEMS application, testing and training, to final hand-off to your users and the NICE operations and support organization. The Production Control and Transition Plan, once finalized based on agreed-upon solution, will describe the production control related to all production phases, as well as incremental transition plan required by COSB.

Deliverable Scope / Content Expectations:

NICE will provide full documentation of production control and transition planning as relevant to your solution. The deliverables will include:
  · PRODUCTION CONTROL AND TRANSITION PLANNING o   PROJECT EXECUTION
   o TRANSITION INTO PRODUCTION
    ▪   System Acceptance
    ▪   Knowledge Transfer
    ▪   Closure and Hand-over
  · SOLUTION MAINTENANCE AND OPERATIONS o ACTIVITY REPORTING o VOICE OF COSB
  · NICE DEMS CUSTOMER SUPPORT o SYSTEM HEALTHCHECK PACKAGE OPTION
 Sample:
 System Acceptance Testing (Customer Solution Verification) – provided under Sample Test Plan

References / Standards	Vendor Project Management Methodologies based on PMI standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and COSB, related to the subject DEMS project.

Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above.
	Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.
	Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

NICE Production Control and Transition Planning

NICE DEMS PROJECT EXECUTION

Deploying NICE DEMS

The deployment of COSB's NICE DEMS solution is performed by specialist NICE installation technicians via secure remote access provided by COSB. The solution can be deployed incrementally, in stages and phases as required by the COSB.

Under the coordination of your NICE project manager, the NICE resource(s) are responsible for everything from the development of the connectors to your third party systems (DSG), provisioning of the NICE DEMS application, testing and training, to final hand-off to your users and the NICE operations and support organization.

As agreed during the Planning phase, the NICE resources under the direction of the project manager will remotely install the software for the DSG on COSB's premise environment. The NICE DEMS pre-production instances will be set up in MS Azure as a unique instance for COSB.

The NICE resource will establish connectivity between your third-party source system(s) as outlined in the detailed design and scope plan, then test the connection(s). Once the DSG environment is established and tested, NICE resources will connect the DSG via secure link to COSB instance in MS Azure. The DSG connection to MS Azure along with the NICE DEMS pre-production instance will be tested by the NICE resources to confirm the data in the NICE DEMS application.

As part of the use of NICE DEMS, historical data will be very useful and helpful as a compliment to the current case data. Another key milestone is the identifying and acquisition of the historical data and then the migration of this data.

Validation and communication are critical path items to the success of the deployment. At each step in the deployment process, the NICE project manager will be communicating with the COSB project manager to provide status updates of the progress and completion of each task and validate. The validation is a two-step process where it first confirms delivery of an execution task in the delivery process and then ensures both parties are on track for the overall project delivery timelines as set forth during the Planning phase.

TRANSITION OF NICE DEMS INTO PRODUCTION
System Acceptance

The testing and validating of the NICE DEMS solution will be conducted by the NICE resource using the NICE Implementation Test Plan to verify that your solution is ready for training and COSB rollout.

They also provide full documentation of the details including all test results, the set up, and configuration of your solution are documented. NICE and the COUNTY are now ready for training.

Please refer to NICE Test Plan for additional information on System Acceptance testing.

- The **System Acceptance Testing (COSB Solution Verification)** document describes a list of tests that can be used to validate that the NICE DEMS system has been correctly installed and provisioned.

- The NICE Data Source Gateway will be fully provisioned by NICE Professional Services and as such is not directly covered in the scope of this document (although it does cover the data sent by the DSG).

Knowledge Transfer and Training

Training is a critical path item and the key to the last step of a successful project. To help gain maximum return on your investment in NICE DEMS as quickly as possible, NICE's Customer Education Services team provides users with the knowledge and skills needed to take full advantage of its capabilities right from the start.

NICE crafts NICE's training approaches as carefully as NICE develops their award winning solutions, using the most effective state-of-the-art training platforms and techniques.

During the Planning phase the dates for the Training were established and confirmed as the ongoing deployment was underway and as part of the validation communication.

Closure and Hand-over

At this stage, closure, the technical delivery of your DEMS solution is complete and the Training has been delivered.

Voice of COSB

Upon closure the NICE project manager will remind the COSB project manager that a member of the NICE Voice of the Customer organization will reach out to them to schedule a live phone interview to capture valuable feedback on the project and the NICE resources who participated in the project. NICE thanks COSB in advance for taking the time with this last step in the critical path to a successful customer experience.

SOLUTION MAINTENANCE AND OPERATIONS
Activity Reporting

The NICE project manager will conduct an introduction for COSB to NICE's Customer Support organization and processes.

COSB will be set up in NICE's Wiser Customer Case Management system and COSB will be shown how to open up a Support Case via the Wiser Portal in the event that COSB needs to raise a case for support.

During the review of the Wiser Portal, the NICE project manager with the assistance of the NICE Support Manager will review the COSB support process, severity definitions and associated SLAs to ensure COSB is aware of the process and support delivery obligations of the NICE Customer Support organization.

COSB can use the Wiser Portal at any time to directly review and run reports on any ticket activities.
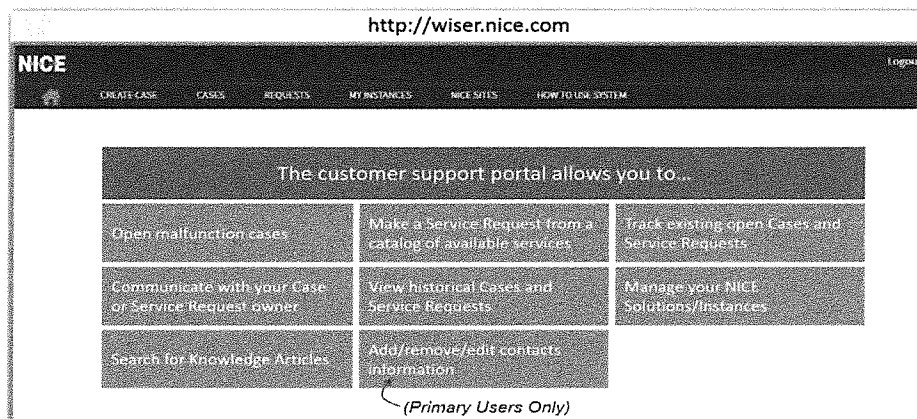
NICE DEMS CUSTOMER SUPPORT

To provide NICE's customers with an outstanding customer experience, NICE has a 24/7/365 Customer Support and Operations team that ensure the lifecycle management of the NICE DEMS solution. NICE's Customer Support organization was a 2017 recipient of the Stevie International Business Award for best customer support department.

The NICE Operations organization is in **constant monitoring and performance tuning state** of the NICE DEMS solution in the Azure Cloud to ensure the reliable daily use for COSB. This organization is also making routine and scheduled updates to ensure COSB has both the solution availability of 99.9% and the key feature set for COSB users as per the agreement. The two organizations have a seamless process to handle all solution incidents in Azure through to COSB-raised Support Cases.
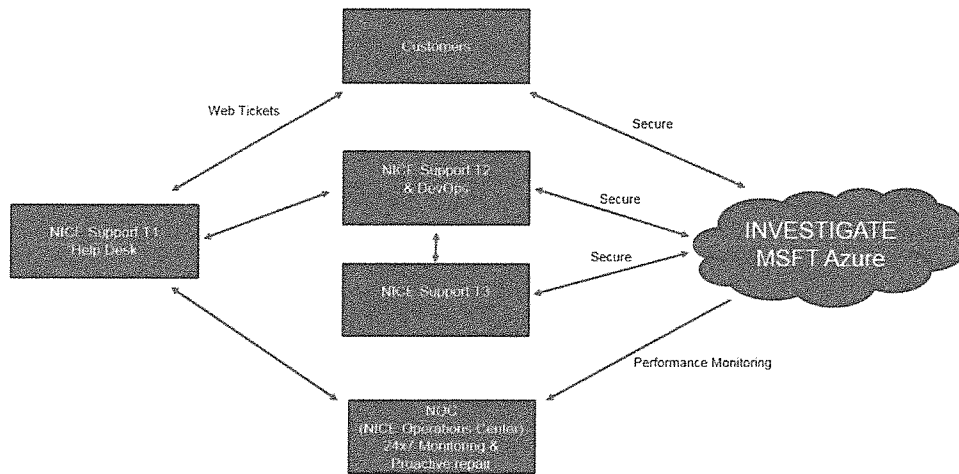
NICE is simple to contact and raise Support Cases and questions about your NICE DEMS solution.

- For all of your NICE Support needs log into the NICE Customer Portal (or enter to: wiser.nice.com)

From this portal you can:

- Manage your NICE Solutions (now called "Instances")
- Open malfunction Support Cases
- Make a Service Request from a catalog of available services
- Track existing open Support Cases and Service Requests
- Communicate with your Support Case or Service Request owner
- Search for Knowledge Articles

A secondary option to reach NICE for Customer support is to call **1-800-NICE611**

The objective of COSB Support and Operations team is to deliver world class support to COSB based on the support severity levels and associated SLAs. If you experience an issue as defined below you can expect a prompt response.

Level	Level Definition	Response Requirement
Level 1	An error, malfunction or other deficiency that meets both of the following criteria: (i) The deficiency significantly impairs COSB's normal business operations; diminishes employee safety or well-being; exposes COSB to significant liability or risk; significantly increases the cost, decreases the value, or impedes the efficiency of COSB resources or operations; or significantly inconveniences COSB customers. (ii) No workaround is currently developed, implemented, and accepted to alleviate the deficiency's impact.	NICE shall acknowledge emergent issue within one (1) hour. NICE shall attempt to resolve emergent issue within four (4) hours. NICE shall provide continuous best efforts and updates until the issue is resolved.
Level 2	An error, malfunction or other deficiency that meets both of the following criteria: (i) The deficiency causes substantial inconsistencies, irregularities, inefficiencies, or potential for mistakes, but does not meet the criteria for a Level I Priority. (ii) No workaround is currently developed, implemented and Accepted to alleviate the deficiency's impact.	NICE shall begin taking action towards a resolution within a time period of 5-24 hours. NICE shall attempt to resolve emergent issue within 5-24 hours. NICE shall provide ongoing and diligent best efforts and updates until the issue is resolved.
Level 3	An error, malfunction or other deficiency that does not meet the criteria for Level I or Level II Priority, but causes system response time to fall below fifty percent (50%) of system response time requirements for more than four (4) hours per month	NICE shall begin taking action towards a resolution by the next business day. NICE shall successfully implement a resolution within a period of thirty (30) days.
Level 4	An error, malfunction or other deficiency that has little or no immediate impact on COSB's business operations, costs, risks, employees, or customers, but is desirable for the long-term viability and utility of the system	NICE shall begin taking action towards a resolution by the next business day. NICE shall successfully implement a resolution within a period of ninety (90) days.

4

In the event that COSB feels it is necessary to raise the awareness of a Support Case and would like to escalate the communication around COSB concern, NICE has an escalation path and methodology to ensure COSB knows who to contact.

NICE's services shall include (at a minimum):

- Release and provision of core DEMS SaaS upgrades, including enhancements and new features
- Service desk support (refer to the Table above)
- Defect correction
- Impact analysis of upcoming DEMS patches and upgrades
- Modifications to NICE provided components and configurations to support upcoming patches and upgrades
- Testing and deployment of patches and upgrades in all environments
- Continuous health checks of the production system
- Continuous tuning and other required system level administration
- Recommendations for system performance tuning
- Application modifications required to support scheduled infrastructure upgrades

SYSTEM HEALTH CHECK PACKAGE

NICE's Routine System Health Checks will help you prevent operational disruptions and assure reliable performance of NICE solutions.

The routine review of your NICE solution's application and technical health will utilize remote diagnostics tools and scripts. It will include:
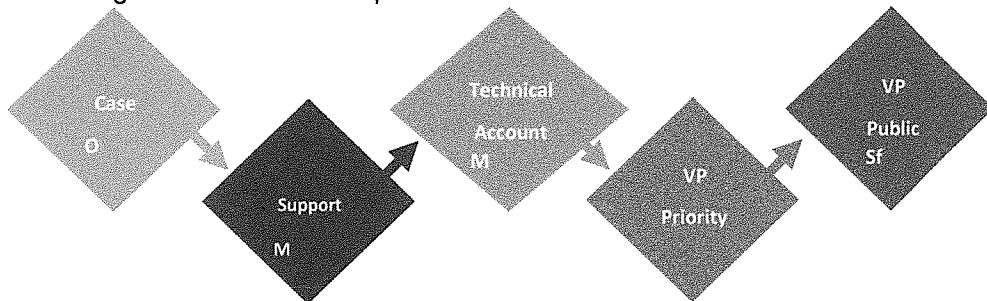
- Review of performance, scale, sizing, and associated items
- Monthly checks and reporting on current status with data and insights for improved planning

NICE shall conduct monthly review meetings with COSB post deployment. Meeting objectives include:

- Communicate and manage contracts performance
- Enhance relationship management through open performance dialogs
- Create actionable strategies and remediation plans as needed

NICE Support Program

Congratulations on the acquisition of your NICE DEMS solution, the finest in the industry. Your organization has demonstrated that it values quality, service constancy, and the delivery of the best-in- class service to the citizens in your community.

It is for just these reasons that NICE includes a comprehensive Support Program to assist with keeping your NICE solution performing optimally

and to ensure your prompt access to the applications, features, and innovation that NICE dedicated Engineers are working on every single day!

There are many benefits to having a NICE Support Program. Here are a few of them:

Predictable Ownership Costs and Convenience

- The total cost of ownership of the solution over its lifetime is predictable – no budgeting surprises.

- An included Support Program is convenient. When you need assistance with your NICE solution, you'll be covered and promptly served.

Protect your Mission-critical Systems with Fast and Transparent Service

- NICE Support is available 24 hours per day and 7 days a week.

- Customers under NICE Support Program have anytime access to NICE's on-line service portal. No more waiting in phone queues. You can also self-monitor the resolution progress and run service ticket reports.

- Service packs and hot fixes are included. If your NICE solution contains hardware purchased from NICE, the Support Program includes the provision of replacement parts for failed or faulty hardware. If needed, such parts are shipped overnight to arrive the next business day.

- Documented, structured and clear escalation processes are established. NICE's management and technical experts are ready to step in when needed, to assure your satisfaction.

Access to the Most Experienced Service and Support Professionals

- NICE's support team is the most experienced in the industry and has gain deep domain expertise through its focus strictly on law enforcement agencies for 30+ years. It is ready to help you keep your agency operating at peak efficiency.

- Supporting more than 5,000 deployments worldwide, NICE engineers leverage the highest number of experience hours, coupled with the most certifications and training in the industry. They work closely with the NICE R&D team, which is fully dedicated to Public Safety solutions – no diversions.

- NICE's global support organization supports agencies in every time zone, ready to remotely dial into the solution and resolve any service condition. Simply put, when you need support, NICE is ready.

- **For critical requests, call NICE's Toll-free number 1-800-NICE-611 (800-642-3611) to ensure timely handling. NICE can provide assistance 24 hours per day, 7 days a week (subject to your purchased Support Program Option).**

6

*Submitting Requests via Wiser On-line Portal

- **Self-register for access to Wiser On-line Portal** - **Enter additional contacts for your organization**

- **Explore NICE's robust knowledge base for self-help opportunities**

- **Create a Support Case: assemble and enter all required information that describes your request per the list below**
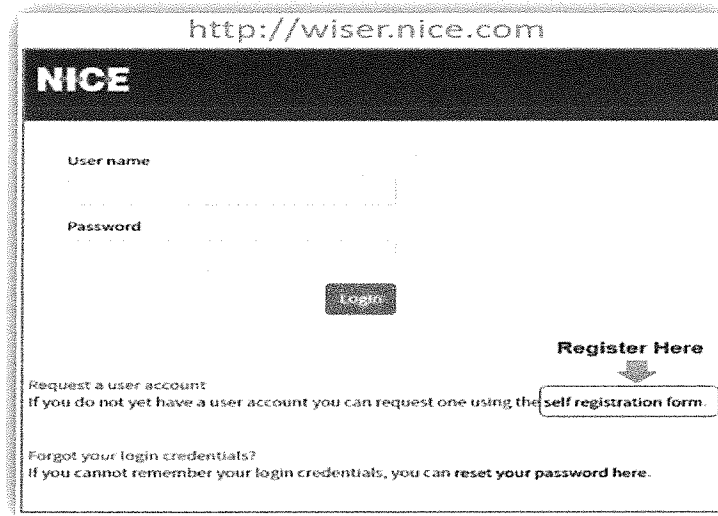
- **Monitor Support Case Resolution: you, and any contacts listed in the "External list" will receive an email notifying you when the Support Engineer responds to your note.**

Provide the following information when submitting a Support Case

- **Company name**
- **Confirm the address of equipment that needs attention**
- **Company contact name, telephone number, and email**

- **Dial-in information for remote connection**
- **Software version and any Service Packs installed if available**
- **The last 60 days of change management information**
- **Clear and concise description of problem**
- **Alarm in its entirety including IP address**
- **Provide the steps/scenario when the problem occurs** • **Is the problem affecting all users or only a certain group?**
- **What is the impact to your operations?**
- **Provide print screens whenever necessary** Priority (Severity) Definitions

Severity Level	Definition	Examples
1. Critical (System Unavailable) *	I. Critical issue that severely impacts of the SaaS Solution. II. No workaround.	A. The SaaS Solution is completely unavailable. B. The majority of users cannot login. C. Data integrity issues.
2. High (System Impaired) *	I. Major functionality is significantly impacted. II. No workaround.	A. Service interruptions to some but not all functionalities. B. Alerts not being generated
3. Medium (Minor Impact)	I. Multiple users impacted by a moderate loss of the SaaS Solution. II. Critical or High impact on a nonProduction SaaS Solution. III. A workaround exists.	A. Functional limitations which are not critical to COSB's daily operations (e.g., reports not being generated). B. Moderate degradation in function, or feature performance.
4. Low (Informational)	I. Minor loss of the SaaS Solution features. II. Inquiries III. Medium or Low impact on non-Production SaaS Solution.	A. There is no significant COSB impact. B. Non-Critical or minor loss of functionality or features.

*Reserved for the Production SaaS Solution only.

8

Support Case Escalation

NICE endeavors to provide a high level of support for all of its customers. However, there are times when COSB may want to escalate a Support Case to a higher level within NICE. The Support Case Escalation process ensures that these times are correctly and effectively managed and receive the appropriate attention. The five escalation steps:
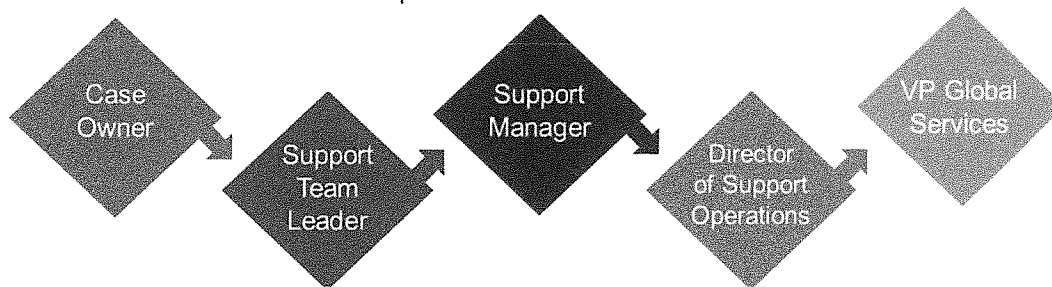
Remote Support

Rapid response by NICE and delivery of the Support Program services requires COSB provide immediate remote access to the NICE solution via a Virtual Private Network supplied by COSB.

(Rest of Page Intentionally Left Blank)

Attachment A Requirement Traceability Matrix (RTM)

Instructions

Attachment A - Requirement Traceability Matrix

INSTRUCTIONS:

This document lists all FUNCTIONAL and TECHNICAL requirements in the form of short statements. Proposer shall place an "x" in the appropriate column. A response shall be selected for each requirement. Proposer shall provide comments, clarification, or references to other areas of the proposal which provide additional details related to the requirement. Proposer shall ONLY rely on references to documents that are included in the proposal in their response. Do not include URL links to information on the Internet.

The requirements are prioritized by a designation of either **Mandatory (M)**, **Priority (P)**, **Highly Desirable (H)**, or **Desirable (D)**. Mandatory functional and technical requirements will be evaluated as PASS or FAIL. If Proposer cannot meet a mandatory requirement, the County will find this Proposer non-responsive and will give Proposer no further consideration. Therefore, the County will not evaluate and score Proposer's proposal. Priority (P), Highly Desirable (H), and Desirable (D) requirements will be evaluated in the overall scoring of the response. Responses in the Response Code column are to be limited to the codes listed below.

RESPONSE CODES:

Response Code	Description
Y	**Yes** – The requirement shall be met by the core proposed platform. This capability exists or is being used in-production elsewhere and can be demonstrated.
N	**No** – The requirement cannot be met.
C	**Customization or Modification** – The requirement shall be met by making programmatic (software development) changes to existing software, developing new software and/or building an interface to the applications listed in this RFP. (Note: This response code includes any software currently in development to meet this requirement by Proposer but which is not yet installed in any client production system).
T	**Third Party Software** – The requirement can be met with a third-party software product, other than the core DEMS provided by Proposer. This includes any work required to incorporate the third party software to operate seamlessly with DEMS. Proposer shall provide a list of all third party software products and include associated costs in the Cost Proposal section of this RFP.

- Proposer shall provide a concise narrative in column 'I' to describe how the solution addresses each functional area. Where appropriate, Proposer shall provide examples of how and where similar requirements are being met on other projects. Proposer shall use illustrations, diagrams, screenshots and/or other sample material to provide additional clarity. Where applicable, Proposer shall identify the third party solutions fulfilling the specific requirements and describe whether these solutions will be standalone or will integrate with the proposed DEMS solution.

- Proposer shall provide additional narrative explanation in column 'I' for any requirement that has been given a Response Code of 'T' or 'C' to provide further clarification and/or additional details to any specific requirement listed above. For easy reference, Proposer shall refer to each requirement by its Requirement ID.

Functional Requirements

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
		Receive & Classify Evidence						
RC-2.3.1	Capture Evidence	The solution shall provide the ability to capture and directly upload digital evidence via a mobile device in the field.	P	X				NICE DEMS solutions provide a mobile user interface optimized for uploading digital evidence via a mobile device. Additional capabilities of this mobile application include initiating requests for digital evidence to witnesses and others, and viewing digital evidence items organized by cases on the mobile device.
RC-2.3.2	Capture Evidence	The solution shall provide the ability to support multiple types or format of digital evidence, including but not						NICE DEMS solution allows for any file format to be uploaded, stored, managed, shared, and downloaded. Also, NICE DEMS is designed to recognize a comprehensive set of media formats automatically. Recognized formats are also viewable within the NICE EDEMS user Interface.
RC-2.3.2.1	Capture Evidence	• Documents (e.g., Word, Excel, PPT, PDF)	M	X				Audio formats that can be reviewed directly in Investigate include but are not limited to the following: .mp3; .wav; .aif (standard Apple audio); .aiff; .wm (Windows Media); .pcm (analog to digital, computers, CDs, digital audio); .gsm for telephony (.wav); .3gp (mobile phone speech/video); .aac; .ac3; .wma (Windows media audio); .ra (for streaming audio over internet); .dvf /.dss (for dictation) — Document file formats that can be viewed directly in NICE DEMS include but are not limited to the following: .pdf; .doc*; .txt; .LST; .mbox; HTML; .rtf; .xls; .ppt; .docx; .eml — Image formats that can be viewed directly in NICE DEMS include but are not limited to the following: .jpg; .tiff; .gif; .png; .bmp — Video formats that can be played directly in NICE DEMS include but are not limited to the following: MP4 Video files (.mp4, .m4v, .mp4v, .3g2, .3gp2, .3gp, .3gpp); .mpeg; .mp2; .m2ts (MPEG-2 TS Video file); .avi; .wmv; .mkv; .asf; .webm; .mov; H.264; .flv; G64x; .dav
RC-2.3.2.2	Capture Evidence	• Images	M	X				Image formats that can be viewed directly in NICE DEMS include but are not limited to the following: .jpg; .tiff; .gif; .png; .bmp
RC-2.3.2.3	Capture Evidence	• Audio recordings	M	X				Audio formats that can be reviewed directly in Investigate include but are not limited to the following: .mp3; .wav; .aif (standard Apple audio); .aiff; .wm (Windows Media); .pcm (analog to digital, computers, CDs, digital audio); .gsm for telephony (.wav); .3gp (mobile phone speech/video); .aac; .ac3; .wma (Windows media audio); .ra (for streaming audio over internet); .dvf /.dss (for dictation)
RC-2.3.2.4	Capture Evidence	• Video recordings	M	X				Video formats that can be played directly in NICE DEMS include but are not limited to the following: MP4 Video files (.mp4, .m4v, .mp4v, .3g2, .3gp2, .3gp, .3gpp); .mpeg; .mp2; .m2ts (MPEG-2 TS Video file); .avi; .wmv; .mkv; .asf; .webm; .mov; H.264; .flv; G64x; .dav
RC-2.3.2.5	Capture Evidence	– Body-worn video	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.6	Capture Evidence	– In-car video	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.7	Capture Evidence	– Interview room video	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.8	Capture Evidence	– Surveillance video	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.9	Capture Evidence	• Emails and Text Messages	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.10	Capture Evidence	• IM/Chat logs	M	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.11	Capture Evidence	• Browser logs	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.12	Capture Evidence	• Closed Circuit Television Video (CCTV)	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.13	Capture Evidence	• Electronic system logs (e.g., door locks, entry systems)	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.14	Capture Evidence	• Transaction logs (e.g., ATM, Banking)	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.15	Capture Evidence	• Indexing of cellphone data	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.2.16	Capture Evidence	• DNA and other forensic result reports	P	X				Supported for capture via direct integrations as well as manual uploads and uploads via request workflows as needed for each scenario
RC-2.3.4	Capture Evidence	Proposer shall provide a list of supported file formats. The solution shall provide the ability to support compressed archive files. (e.g. ZIP, 7z)	P	X				Compressed archive files such as .7z can be directly uploaded to NICE DEMS solutions. They will then unzip and manage the individual file items. The unzipped files are visually linked together in the NICE DEMS solutions as a single evidence item with multiple files attached. This will assist users in better understanding the relationship between files as well as assisting with sharing and downloading of appropriate files as needed.
RC-2.3.5	Capture Evidence	This solution shall allow imports of specific proprietary codecs that may be associated with digital evidence collected at a crime scene, imported by witnesses and pubic (via a secure web portal), provided from surveillance equipment and other sources	M	X				NICE DEMS solutions provide a mobile application (as well as web interface) that supports communications with Witnesses. A NICE DEMS user can send a request to a witness (or multiple witnesses) via either interface. The witness will receive a text message (or an email) with a link to a secure web portal to upload their evidence. Many Proprietary codecs are supported for import. Additionally, NICE DEMS can also directly import data and files from surveillance equipment and other sources.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RC-2.3.6	Ingest Evidence	The solution shall allow for witnesses and members of the public to securely upload various types and formats of digital evidence to be added to a case file for investigative purposes. Industry Standard/Common formats including but not limited to: MP3, MP4, MOV, AVI, FLV, MKV, WMV, H.264, MPEG-4, MULTIPLE PROPRIETARY CODECS, JPG, JPEG, PNG, GIF, TIFF, PSD, PDF, ESP, AI, RAW . Proposer shall provide a list of all accepted digital evidence formats for secure upload by the public	P	X				NICE DEMS solutions provide a secure upload portal for Witnesses, Citizens, Investigators and Business. Any type of evidence can be collected in this manner (images, video, documents, comments, etc.). All formats listed in the requirement are fully supported for upload by the public. NICE DEMS then automatically converts the files to standard, universally viewable and playable formats. Please reference our Supported Media Types document for further illustration.
RC-2.3.7	Ingest Evidence	The solution shall provide the ability to ingest and allow access to forensic files, including but not limited to: • Mobile device files (e.g. AXIOM, Cellebrite and EnCase) • Computer forensic files (e.g. EnCase) Proposer shall indicate any file size limitations.	H	X				NICE is partnered with Magnet solutions. If an agency is a Magnet/NICE user, a document is created in NICE DEMS (index report) that has a hyperlink in it. The hyper link will open the Magnet Review (Magnet's remote investigation tool) website with a Magnet login to view the Magnet Review functionality of the Magnet Cell Phone/Forensic PC Image extractions in NICE interface (without Magnet). The plan will also allow users to actually view the reports and the attached evidence contained in the report (the tests /images etc.) and have all those hyperlinks active pointing to the original case in Magnet. All the files are uploaded for secure storage in NICE DEMS.

If the customer is not a Magnet user, the raw file gathered from the extraction software or .bin (android) or .tar (apple) file can be uploaded into NICE DEMS for secure storage that also saves room on locals servers. This includes CSAM material.
The raw file cannot be viewed or previewed in NICE- it's simply storage. We have a Cell Phone/Forensic PC Image dump file type that allows for easy sorting and filtering of stored Cell Phone/Forensic PC Image extractions.
That file would have to be downloaded by the user, then opened and parsed out in their forensic parsing tool of choice (AXIOM, Cellebrite and EnCase for mobile devices) & (EnCase ,FTK, XRY) Forensic PC Image extractions). This method still allows for sharing and storage of large Cell Phone/Forensic PC Images. There is no requirement for USBs, hard drives, fips, etc. with these methods.

A Cellebrite UDFR file can also be uploaded and shared/downloaded the same way. There is no preview of a UDFR file. UDFR file is a Cellebrite summary report file that has the data from the Cell Phone/Forensic PC Image in it, it's often shared with a UDFR reader. Exe file)

If the user has created an artifact summary report in pdf or html format, it can be uploaded and shared- the report should be viewable/previewable in NICE. |
| RC-2.3.8 | Ingest Evidence | The solution shall provide the ability to schedule upload or transfer of files (including schedule for off hours and weekends) | P | X | | | | NICE DEMS integrations are uniquely customizable to offer scheduled uploads or transfer of files in order to not interrupt core business hours. Evidence ingest can be scheduled for the County's off hours or weekends as required by the County. |
| RC-2.3.9 | Ingest Evidence | The solution shall provide the ability to convert files to a standard file format | P | X | | | | NICE DEMS solutions automatically transcodes the original evidence file into a working copy with a standard format (see below) that is then viewable via its media player(s) (and can be edited, annotated, shared, etc) using a standard web browser access:
oVideo - .mp4
oAudio - .aac
oPictures - .jpg
oDocuments - .pdf |
| RC-2.3.10 | Ingest Evidence | The solution shall provide the ability to ingest digital evidence via a batch upload process. | P | X | | | | Our recommended ingestion method for digital evidence is automated collection. NICE Data Source Gateway (DSG) software appliance interfaces between NICE DEMS and your data sources to automatically upload digital evidence items that are tagged with valid case related identifiers into a NICE DEMS case folder. Digital evidence items along with all of their associated metadata are securely uploaded without any need for user intervention, while users who need to know can receive notifications of the new evidence items added. This approach saves time and improves the accuracy of the data collected, while also improving the efficiency and effectiveness of every investigator.
Officers continue to use their existing evidence capture devices and applications, while NICE DEMS connects to these existing platforms and storage locations and automates the collection process to bring all evidence into a centralized storage repository. Evidence is then organized into electronic case folders and made accessible to authorized users.
NICE DEMS can upload an individual digital evidence item or multiple evidence items in bulk for secure storage, for viewing by authorized users, or sharing with others. |
| RC-2.3.11 | Ingest Evidence | The solution shall provide the ability to maintain and preserve the original nested folder structure of the digital evidence upon ingestion. | P | X | | | | NICE DEMS solution will preserve the linking of folder/sub-folder/file relationships for uploaded evidence items. |
| RC-2.3.12 | Ingest Evidence | The solution shall provide the ability to capture metadata from the case management system, via API/Web Service interfaces, during ingestion. | P | X | | | | NICE DEMS solutions case folders are automatically created and assigned via integration with your agency's Case Management (or Records Management, depending on agency type) system. When a case is created and assigned in RMS/CMS, the RMS/CMS to NICE DEMS integration will trigger a case creation in NICE's interface. Folders are automatically created for each case, and evidence items are placed into their appropriate case folders. Case related metadata from the RMS/CMS is extracted and associated with each case folder in NICE DEMS. Each evidence item has its own individual set of metadata as well. All case related information in RMS/CMS is shared via the integration so that all pertinent case details are accessible in NICE DEMS. The integration keeps both platforms in sync with the most up to date information. NICE can also provide a two-way integration, where your CMS/RMS system provides direct links to cases/evidence in NICE DEMS. |

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RC-2.3.13	Ingest Evidence	The solution shall provide the ability to enter free-form metadata text associated with digital evidence.	P	X				With NICE DEMS Automated Ingestion, evidence items are uploaded along with all associated metadata. For manual uploads to NICE DEMS, embedded metadata, such as EXIF data, is also uploaded with the evidence item. The end user also has the ability upon upload to add additional relevant metadata. At any time, an end user with the proper privileges can access an evidence item in NICE DEMS and add further metadata as needed.
RC-2.3.14	Ingest Evidence	The solution shall provide the ability to set specific metadata fields as mandatory.	P	X				NICE DEMS solutions system administrator with the proper privileges has the ability to set specific metadata fields as mandatory.
RC-2.3.15	Ingest Evidence	The solution shall provide the ability to convert files via OCR	M	X				NICE DEMS supports automated OCR for all media files. Optical Character Recognition converts images of typed, handwritten or printed text into machine-encoded text in order to be made searchable within the NICE platform. Therefore, all images, PDFs/scanned documents, are run through our OCR engine upon upload to NICE DEMS. This OCR content is then fully searchable in NICE DEMS.
RC-2.3.16	Ingest Evidence	The solution shall provide the ability to manually upload one or more pieces of digital evidence and associate them to a specific case.	P	X				A NICE DEMS user can upload one or multiple evidence items directly to a specific case folder in NICE DEMS interface. A user who may not have access to a case folder can also upload evidence items to NICE DEMS and then tag the items with a case ID at the time of upload or at a later time. Once the tag is added to the uploaded items, NICE DEMS will add the items to the appropriate case folder.
RC-2.3.17	Ingest Evidence	The solution shall provide the ability for agencies that do not have a DEMS, or have a DEMS that is not compatible with the solution, to manual upload files via a portal.	P	X				Agencies that do not have DEMS can be provided a free upload portal to manually upload digital evidence via NICE DEMS interface (for example, this is used by prosecutors to provide access to multiple law enforcement agencies, some of which do not have DEMS). NICE DEMS is technologically agnostic, which allows API connectors to be created for all Digital Evidence source systems, and retain continuity with uniform experience for users even as these source systems change over time.
RC-2.3.18	Ingest Evidence	The solution shall provide the ability to generate notifications/warnings upon file ingestion (e.g., for recognized sensitive content such as child exploitation or malware).	M	X				All media uploaded to NICE DEMS is scanned for viruses/malware. If malware is detected, uploading of the infected media is terminated. The user is notified and appropriate audit logs are created. NICE DEMS can also be configured to identify sensitive file types upon ingestion and appropriately categorize these sensitive files so that access is restricted per Santa Barbara County guidelines for such material. End users also have the ability to mark files as sensitive upon manual upload. The system can also be configured to blur thumbnails of unsafe evidence items, warning users of the sensitive nature of the evidence item. A user with the proper privileges can then select to view and the images will be rendered without the blurring.
RC-2.3.19	Retain Evidence	The solution shall provide the ability to store digital evidence in its native format.	P	X				All digital evidence items uploaded to NICE DEMS are stored in their native formats, available for disclosure alongside 'transcoded' copies. Once media is successfully uploaded to NICE DEMS, it is virus checked and, depending on file format, a working copy is created. The working copy is a version of the original, transcoded to a common media format that is viewable and can be played back via the NICE DEMS web-based user interface and is made available for universal sharing with others.
RC-2.3.20	Retain Evidence	The solution shall provide the ability to track and maintain the metadata associated with digital evidence.	P	X				All collected metadata is stored alongside the digital evidence items to which it belongs in NICE DEMS. When an end user accesses a digital evidence item, all associated metadata is also available to view, use for filtering, and other functions.
RC-2.3.21	Retain Evidence	The solution shall provide the ability to associate and synchronize separate video and audio files of the same digital evidence.	P	X				The NICE DEMS solution Timeline view provides users the ability to select video and audio files within a specified time period (which could be within the same case) and play all these files back synchronously as they occurred according to their time stamps, to help investigators and other users better understand the timing of events, documenting the case from multiple angles and perspectives.
RC-2.3.22	Classify & Tag Evidence	The solution shall provide the user the ability to indicate that content is sensitive, and apply permissions rules and workflows based on this indication. This may be based on metadata, categories, tags/flags or other methods that persist with a file as access is granted to, or it is transferred to other divisions	M	X				NICE DEMS solutions provides a user with the ability to tag any Digital Evidence with appropriate classification and permission rules. Sensitive content (e.g. in child exploitation cases) can be defined based on metadata that can also include tags, so that it falls into a category with very restricted access rights, permitting access only to select users. When a user opens a NICE DEMS case folder, the user is presented with a view of all of the evidence associated with a case, to the extent of each user's permissions. Each evidence item is visualized as an evidence card (sensitive material being blurred to limit viewing to only authorized parties) with summary information such as: ▫Evidence Type (audio, video, document, image) ▫Evidence name/Title ▫ Evidence Category ▫ Data Source (where the evidence originated) ▫Thumbnail preview of the evidence item
RC-2.3.23	Classify & Tag Evidence	The solution shall provide the ability to assign a unique DEMS identification by predetermined standards in an automated fashion to the digital evidence, upon ingestion.	P	X				NICE DEMS solutions can be configured to assign a unique DEMS identification number to all digital evidence items upon ingestion. When creating the integration to the Santa Barbara evidence source systems, NICE DEMS will bring across all metadata and property fields related to evidence, maintaining the organization, status, and structure provided. With RMS/CMS integration, all evidence items will be also properly associated to specific relevant case ID numbers.

Req ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RC-2.3.24	Classify & Tag Evidence	The solution shall provide the ability to share the assigned unique DEMS identification number with other County systems.	P	X				NICE DEMS solutions integrations can be 2-way in which relevant data can be provided to other County systems as needed.
RC-2.3.25	Classify & Tag Evidence	The solution shall provide the ability to index any associated metadata attached to the digital evidence upon ingestion.	P	X				All metadata collected and stored in NICE DEMS is indexed. The NICE DSG also continuously searches all connected data sources in real time and delivers the resulting search index to NICE DEMS. Additionally, a one-time backward search is performed during the initial connection to a data source to collect 'historical' or 'legacy data' results based on a configurable time period. NICE DEMS indexes both structured (documents, data, etc.) and unstructured (video or audio) evidence to enable subsequent keyword and content based searching.
		The solution shall provide the ability to add metadata or a related file that provides direction on how the digital evidence content can be used.						NICE DEMS solutions provides a rich set of default metadata fields for digital evidence items. It also inherits the key metadata fields from connected data sources. Our customers are also able to add and configure additional metadata fields as required for alignment with existing business processes. The NICE DEMS System Administrator may configure a metadata field that provides direction on how the digital evidence content can be used.
RC-2.3.26	Classify & Tag Evidence		P	X				Users can associate related files with evidence items by selecting the "Add a Variant" option from the Evidence details view in NICE DEMS. This option allows a user to attach an external file, or to save and attach a variant of the existing evidence item such as a clip or snapshot that was created.
								The variants/attached files are managed alongside the original evidence and can be viewed and shared as needed by NICE DEMS users.
RC-2.3.27	Classify & Tag Evidence	The solution shall provide the ability to add additional metadata to digital evidence to facilitate categorization and assignment.	P	X				NICE DEMS solution provides a rich set of default metadata fields for digital evidence items. Media types/sub types are included in the default set of metadata fields. Types are configured per the customer's requirements. Case and evidence assignment are also default metadata fields in NICE DEMS. Our customers are also able to add and configure additional metadata fields as required for alignment with existing business processes. The NICE DEMS System Administrator may configure a metadata field that provides direction on how the digital evidence content can be used.
RC-2.3.28	Classify & Tag Evidence	The solution shall provide the ability for users to classify evidence based on classification standard which can be set individually per agency or instance of the software	P	X				A NICE DEMS System Administrator(s) can configure case and evidence level metadata fields as well as tags and labels to align evidence categorization with standards already in use by the agency. This is very easy to do from the administration portal. For example, Administrators are able to set standard classifications of evidence and even set those fields as "required" by the users. Should there be a set of metadata available from a Datasource (i.e. BWC system) NICE DEMS can automatically inherit that classification as well. Lastly, users can apply their own classifications and labels ad-hoc to their individual cases.
RC-2.3.29	Classify & Tag Evidence	The solution shall provide the ability to generate unique numbered and / or lettered Bates stamps to individual pages or documents of evidence.	M	X				NICE DEMS supports the ability to sequentially number individual pages or documents of evidence as a Bates-stamp. Users will have the option to bates stamp their documents using individually unique numbers per page.
RC-2.3.30	Classify & Tag Evidence	The solution shall provide the ability to save the last bates stamp letter and or number(s) used and resume Bates stamp number / letter sequence to additional pages or documents of evidence.	M	X				NICE DEMS Bates stamping will resume the number in sequential order from the last stamped document in the case to ensure continuity. Each case will start the bates stamping numbers from xxx1 and continue numbering until each document in the case receives a unique, sequential number.
RC-2.3.31	Classify & Tag Evidence	The solution shall provide the ability to generate Bates stamp numbers to a specified region of the individual pages or documents of evidence.	P	X				NICE DEMS Bates stamping is flexible and provides the user the ability to determine where on the page to apply the Bates Stamp.
RC-2.3.32	Classify & Tag Evidence	The solution shall provide the ability to generate Bates stamp numbers based on a customized schema or prefix or suffix.	P	X				Bates Stamping schemas can be customized for your agency's use in the following ways: o Optional prefix/suffix o Support for a combination of letters and numbers o Define position of the Bates number on the page
RC-2.3.33	Classify & Tag Evidence	The solution shall provide the ability to add new data fields to facilitate categorization and assignment.	P	X				NICE DEMS solutions provides the ability for new data fields to be added as mandatory or optional for the initial intake of evidence and associated data collection. Additionally, as users of NICE DEMS are reviewing, annotating, vetting and redacting digital evidence, they also have the ability to mark the digital evidence items for categorization, assignment, and particular disclosure package. An evidence disclosure package field can be configured so that the user can mark purposed for this activity along with keyword tagging. We recommend using NICE DEMS keywords for this activity as multiple keywords can be assigned to a given evidence item. Once ready for disclosure, the user filters the evidence view based on the appropriate disclosure package keyword, select the items shown and create the disclosure package.
RC-2.3.34	Classify & Tag Evidence	The solution shall provide the ability to rename files in batches to add the Bates stamp or Bates stamp range to the filename for each file.	P	X				NICE DEMS provides the ability to add a Bates Stamp to a single page or range of pages for a given file or batch of files.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RC-2.3.35	Cross-Reference Evidence	The solution shall provide the ability to cross-index evidence by the case, defendant, Court case number, or associated metadata.	P	X				NICE DEMS solutions can automatically cross-index evidence by the case ID and other metadata. When our integration with CMS/RMS is implemented, indexing with Case ID metadata can be automated. Other types of metadata (e.g. Court Case Number) can be collected and cross-referenced either via manual entries or via integrations as well, as applicable to each data type. Using the extensive collection of metadata, NICE DEMS also provides extensive search capabilities to assist users in finding relevant information in digital media stored in NICE DEMS or any of its connected data sources. All types of evidence can be searched by virtually any combination of collected metadata, to include date, time, user, geolocation, free text wild cards or partial information, and any other data that is either automatically collected or manually entered during evidence uploads. Filtering tools are available to assist the user in narrowing down search results to easily find items of interest. The user can save a filtered view for quick recall at a later time. Each search result will provide summary details of the item with a way to drill down for more details. The user can also click into the evidence item or case folder for further review.
	Exchange Evidence							
EE-3.3.1	Request Evidence	The solution shall provide the ability to submit a request of digital evidence to other users/groups/roles.	P	X				Evidence collection workflows are available in NICE DEMS - they support the collection of digital evidence from other groups, businesses and citizens. A NICE DEMS user has the ability to send an evidence collection request to intended recipients, using online forms and workflows that associate those requests to specific cases. When the recipient receives the request via email, the request will include a link that allows the recipient to securely upload requested evidence. The uploaded material is then made available to the requestor (with notification to the requestor) for review and to accept if desired. All requests are tracked in NICE DEMS, providing the user with a summary of outstanding and completed activity. A user which made the request can also elect to get notifications indicating when a request has been opened and when it has been fulfilled.
EE-3.3.2	Request Evidence	The solution shall provide the ability to submit a request of digital evidence to other agencies	M	X				NICE DEMS solution supports evidence collection workflows - It supports the collection of digital evidence from other agencies, businesses and citizens. A NICE DEMS user has the ability to send an evidence collection request to intended recipients, using online forms and workflows that associate those requests to specific cases. When the recipient receives the request via email, the request will include a link that allows the recipient to securely upload requested evidence. The uploaded material is then made available to the requestor (with notification to the requestor) for review and to accept if desired. All requests are tracked in NICE DEMS, providing the user with a summary of outstanding and completed activity. A user which made the request can also elect to get notifications indicating when a request has been opened and when it has been fulfilled.
EE-3.3.3	Request Evidence	The solution shall provide the ability to route requests to users/groups/roles.	P	X				NICE provides a way for users/groups/roles to register in NICE DEMS as request recipients. The NICE DEMS system administrator also has the ability to set up users/groups/role as request recipients. This provides the information needed to properly route requests. In addition to approved recipients, users of NICE DEMS can also send requests to new recipients.
EE-3.3.4	Request Evidence	The solution shall provide the ability to generate a notification when a digital evidence request is received.	M	X				NICE DEMS solution tracks all requests, providing the user with a summary of outstanding and completed activity. The user who made the request can also elect to get notifications indicating when a request has been opened and when it has been fulfilled. The recipient of the request will receive an email notification of the request. If the recipient is a registered NICE DEMS user, then the recipient will also receive an in-application notification. For registered users, the email notification is an optional setting that can be disabled if desired.
EE-3.3.5	Request Evidence	The solution shall provide the ability to generate a notification once a request is fulfilled.	M	X				All requests and their stages are tracked in NICE DEMS, providing the user with a summary of outstanding and completed activity. A NICE DEMS user who made the request can also elect to get notifications indicating when a request has been opened and when it has been fulfilled.
EE-3.3.6	Distribute Evidence	The solution shall provide the ability to share digital evidence in its native format, based on customizable rules and workflows. These workflows should be automated where possible while requiring manual triggers.	M	X				NICE DEMS provides the ability to share digital evidence in its original format. We also automatically make a universally playable copy that can be shared along with the original. Customized rules can be set up for auto sharing of items based on specified case or evidence attributes. Items can also be blocked from sharing based on specified case or evidence attributes.
EE-3.3.7	Distribute Evidence	The solution shall provide the ability to manually throttle uploads and/or transfers	D	X				NICE DEMS distributes evidence from the cloud and does not require any use of local county bandwidth or throttling. Evidence is shared from the NICE DEMS cloud instance to a linked, cloud-based Sharing Portal that is a part of the NICE DEMS solution. Share recipients receive an email notification with a link to the shared data. Recipients can log into the Share Portal and view all shared evidence and/or download as desired.
EE-3.3.8	Distribute Evidence	The solution shall provide the ability to generate a notification to users when upload of a large file is being attempted, including providing estimated time for upload	H	X				All files are uploaded in the background of NICE DEMS. A separate browser window is displayed which allows users to track the upload progress as well as the estimated time remaining for an upload. Users can monitor this upload without impacting the functionality of their DEMS application or local device.
EE-3.3.9	Distribute Evidence	The solution shall provide the ability to generate a notification to confirm a successful/unsuccessful upload.	P	X				NICE DEMS solutions has an Upload Progress page that provides the user progress on each individual file upload. The user is also able to receive an in-app/email/text notifications when uploads are completed and when uploaded files are ready to be viewed.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
EE-3.3.10	Distribute Evidence	The solution shall provide the ability to manage what evidence and when it is released to ensure proper procedure of releasing evidence.	D	X				Users are able to mark evidence with a variety of Discovery status settings (ex. No Not Disclose, Ready For Discovery, Needs Review, etc.), DEMS System Administrators can set up disclosure rules to ensure only appropriately tagged evidence items are able to be shared. If an evidence item is not marked appropriately and the end user tries to share that item, a notification will be shown to the user stating that the evidence item is not properly tagged and can't be shared in its current state. These tools will assist users in ensuring proper procedures are followed when releasing evidence.
EE-3.3.11	Distribute Evidence	The solution shall provide the ability to export digital evidence.	P	X				NICE DEMS solutions provides the ability for a user with the proper privileges to export digital evidence items, associated metadata, notes, comments, bookmarks and other annotations.
EE-3.3.12	Distribute Evidence	The solution shall provide the ability to attach associated metadata to all exported digital evidence.	P	X				Please reference EE-3.3.10 response above
EE-3.3.13	Distribute Evidence	The solution shall provide the ability to distribute notes and/or annotations associated with digital evidence.	P	X				Please reference EE-3.3.10 response above
EE-3.3.14	Distribute Evidence	The solution shall provide the ability to create workflows for specific categories of content (e.g. content that is manually indicated to contain child exploitation). This may be based on metadata, categories, tags/flags or other methods that persist with a file as access is granted to, or it is transferred to other divisions	M	X				NICE DEMS is able to read flags as set forth in RMS/CMS and treat a case differently based on those tags/flags present. Should a case be marked as confidential, evidence thumbnails will be turned off. Users are also able to establish this within NICE. Moreover, NICE DEMS has a robust access control policy where cases will only be shown to those users who have rights to see them. An access control policy rule can be established based on evidence metadata, categories, tags, or any other relevant media attribute. NICE can establish a strict access control policy for specific categories of cases where the content may be sensitive or not be available to the everyday user. Last but not least, access can be denied or granted on an individual case or evidence item basis for unique instances where there is an exception to the access control policy.
EE-3.3.15	Distribute Evidence	The solution shall provide the ability to create administrative notes associated with individual items of evidence or a case folder, that are transmitted along with the evidence from agency to agency	H	X				Comments are able to be made and saved on a case and individual evidence item level. When that case and/or evidence item is then shared to a connected agency's system, those comments can be selected to be shared alongside. If sharing to a non-NICE user via the share portal, users also have the ability to include comments and bookmarks in their share activity.
EE-3.3.16	Distribute Evidence	The solution shall provide the ability to manage which notes and/or annotations associated with digital evidence are visible to other users/groups/roles.	P	X				NICE DEMS solutions provides users/groups/roles the ability to manage which notes and/or annotations associated with digital evidence.
EE-3.3.17	Reference Offline Evidence	The solution shall provide the ability to reference evidence residing outside of DEMS.	P	X				Html links are supported in NICE DEMS, if there is the need to select a link that points to an evidence item residing outside of DEMS. The user can also create a digital evidence item record that provides details and relevant metadata associated with evidence that is not residing in the DEMS.
EE-3.3.18	Render Evidence Media	The solution shall provide the ability to package digital evidence and save onto physical media (e.g. flash drive, CDs, external drive).	P	X				With NICE's "Share via Download" the recipient of the Share receives a zip file of all shared content. This package of files can then be saved onto physical media. The user who receives the shares has the ability to save/download digital evidence onto physical media.
EE-3.3.19	Manage Routing Rules	The solution shall provide the ability to develop and configure routing rules.	P	X				Review and approval routing rules can be created in NICE DEMS. Evidence request routing rules also exist and can be configured to meet the specific needs of your agency.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
EE-3.3.20	Package/Nest Evidence	The solution shall provide the ability to create and manage metadata to ensure that the repository is well organized (e.g., all files relevant to a case can be viewed as a collection), that views of content can be filtered, and that access control can be maintained (e.g., Adult vs. Juvenile cases).	H	X				NICE DEMS solutions organizes all evidence by metadata associated to every evidence item, such as by cases, by evidence types (video, audio, etc.), and other parameters, making the evidence easy to group and filter. Once logged into NICE DEMS, a user is presented with all the cases that this user has permissions to view. He can search through them, filter and group evidence, look for matches of evidence parameters across cases, and more. Inside each case folder, user can view all collected evidence and incident details associated with the case. Each evidence item is visualized as an evidence card with summary information such as: ☐ Evidence Media Type (audio, video, document, image); Evidence Name; Data Source (where the evidence originated); Thumbnail view of the evidence item Filter and sorting tools are available to assist the user in quickly locating and viewing desired evidence items. Your view can be ordered by: evidence name, time, media type You can further filter your view by any combination of parameters such as evidence type, data source; specified time range; free text field to filter on whatever text you desire; etc. Once an evidence item is located, NICE DEMS user is able to open the item and view the media and associated metadata within the NICE DEMS user interface Filtered views can be saved for quick recreation at a later time. NICE DEMS implements an attribute based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know". The control of access rights are established in NICE DEMS via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.
	Maintain Evidence Integrity							
MI-4.3.1	Control Evidence Authenticity	The solution shall provide the ability to detect digital evidence alterations from the original point of upload into DEMS via Secure Hash Algorithm validation.	M	X				All media uploaded to NICE DEMS is hashed and saved in its cloud storage. A working copy of the original is created for access and use by users. The original is protected, and never used in NICE DEMS for any alterations. The original can be downloaded or shared as required, in its full integrity. NICE Audit tracks when the evidence hash is created/signed. Audit Logs provide information on platform-generated activity such as automated upload of evidence to a NICE DEMS case folder, virus checking, security hash activity, and creation of transcoded copies of evidence items. Logged user activity includes accessing a digital evidence folder, viewing digital evidence items, creating or modifying evidence metadata, uploading, sharing, downloading digital evidence items, etc. Each audit entry includes information on who completed the action and when the action occurred, along with any additional details associated with the action. The authenticity of audit records is ensured by the use of a hash chaining mechanism (the audit records/blocks are linked and secured using cryptography). The chaining of blocks uses HMAC-256 and employs a 256-bit salt. Chain of custody reports are created from the evidence collected in the NICE DEMS audit logs. These chain of custody reports provide proof of authenticity of the collected evidence and can be sent alongside all other digital evidence when shared with the prosecution and others, such as for court purposes.
MI-4.3.2	Control Evidence Authenticity	The solution shall provide the ability to flag digital content which has been modified since it was originally uploaded into DEMS.	M	X				NICE DEMS solutions does not provide the end user access to modify the original digital evidence item, to protect the integrity of those originals. All end user activity in NICE DEMS is done with the working copy of the digital evidence item that is created upon upload. Audit Logs provide information on platform-generated activity such as automated upload of evidence to a NICE DEMS case folder, virus checking, security hash activity, and creation of working copies of evidence items. Logged user activity includes accessing a digital evidence folder, viewing digital evidence items, creating or modifying evidence metadata, uploading, sharing, downloading digital evidence items, etc. Each audit entry includes information on who completed the action and when the action occurred, along with any additional details associated with the action. The authenticity of audit records is ensured by the use of a hash chaining mechanism (the audit records/blocks are linked and secured using cryptography). The chaining of blocks uses HMAC-256 and employs a 256-bit salt. If there are concerns around a possible database anomaly, an integrity check can be performed on an evidence item at any time if required. This will check the integrity of the original evidence item stored in NICE DEMS.
MI-4.3.3	Control Evidence Authenticity	The solution shall provide the ability to preserve the original copy of digital evidence.	P	X				All media uploaded to NICE DEMS is hashed and preserved in its original state. A working copy of the original is created for access by users for annotating, bookmarking, clipping, etc. The original is never used in NICE DEMS. The original can be shared as required, as important evidence in court. NICE DEMS Audit tracks when the evidence hash is created/signed.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
MI-4.3.4	Control Evidence Authenticity	The solution shall provide the ability to create and restore backup copies of all digital evidence	D	X				NICE DEMS solutions provide high availability Geo-zone-redundant storage, with 99.9999999999999% durability of objects over a given year. This type of storage assures that three additional copies are stored in multiple regions and zones. Any of the three working functional copies of the storage can be restored to replace a failed copy.
MI-4.3.5	Control Evidence Authenticity	The solution shall provide the ability to prevent any changes to be applied to original copies of digital evidence.	P	X				All media uploaded to NICE DEMS is hashed and saved in its cloud storage. A working copy of the original is created for access by users. The original is never used / modified in any way in NICE DEMS, it is not accessible for making any changes.
MI-4.3.6	Control Evidence Authenticity	The solution shall provide the ability to track and label working copies of digital evidence.	P	X				Chain of custody reports are created from the evidence collected in NICE DEMS audit logs. These chain of custody reports provide proof of the authenticity of the collected evidence and can be sent alongside digital evidence when shared with the prosecution and others for court purposes. Each evidence item is maintained as the original and labeled as such. Any modifications to original evidence file will be saved as a variant (working copy) to maintain authenticity. NICE DEMS automaticly labels variants and links them to the original file. Both original copies and variants have their own activity and chain of custody logs.
MI-4.3.7	Control Evidence Authenticity	The solution shall provide the ability to identify and differentiate between the original copy, duplicates and other variations.	P	X				NICE DEMS solutions clearly differentiates between the original digital evidence item, the created working copy, and any variants created from the working copy. All of these items are linked together in NICE DEMS and can be downloaded/shared separately or together.
MI-4.3.8	Manage Digital Rights	The solution shall provide the ability to prevent and control the distribution, access and copying of digital evidence, based on user security roles.	P	X				NICE DEMS solutions implements an attribute based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know", for any activity including distribution, access, copying, and more.

The control of access rights are established in NICE DEMS via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.

It is also possible to create a connection to synchronize and inherit access control rules with a customer's existing records management system as a custom integration.

The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in NICE DEMS. |
MI-4.3.9	Manage Digital Rights	Utilizing Digital Rights Management, the solution shall provide the ability to assign expiration dates and times to access specific digital evidence when it is exported from DEMS.	H	X				NICE DEMS solutions provides the ability to share evidence with others via a secure download package that is created and sent via email to the desired recipient. When the NICE DEMS user creates the export package, the user sets a time duration for how long the link to the export package will be active. A secure access code is required to open the shared package. The access code is generated in NICE DEMS. It is responsibility of the sender to securely provide this access code to the recipient. The recipient is then able to enter the secure code to open the sent zip file and access the sent files.
MI-4.3.10	Manage & Track Chain of Custody	The solution shall provide the ability to remove access rights to digital evidence, based on user defined criteria.	P	X				The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in NICE DEMS.
MI-4.3.11	Manage & Track Chain of Custody	The solution shall provide the ability for users (with the appropriate permissions) to generate a full chain of custody across all agencies or instances of the solution	H	X				NICE DEMS solutions provide users with the option of generating full chain of custody across any agency participating in DEMS and Share via Discovery feature. Chain of Custody reports can be generated and shared if needed with any agency.
MI-4.3.12	Manage & Track Chain of Custody	The solution shall provide the ability to indicate if some or all pieces of evidence associated with a case shall be made available to specific users/groups/roles.	P	X				A NICE DEMS solutions user has the ability to Share a subset (or all) of case evidence items with others.
MI-4.3.13	Manage & Track Chain of Custody	The solution shall provide the ability to reassign digital evidence to different users/groups/roles.	P	X				Assignment of digital evidence in NICE DEMS is at a Case level. If a user is assigned an NICE DEMS Case folder, then the user is the assigned owner of all evidence items in that case folder. Reassignments can be made in NICE DEMS by system administrator/s.
MI-4.3.14	Manage & Track Chain of Custody	The solution shall provide the ability to update user access to digital evidence once a case is reassigned.	P	X				Assignment of digital evidence in NICE DEMS is at a Case level. If a user is assigned an NICE DEMS Case folder, then the user is the assigned owner of all evidence items in that case folder. Reassignments can be made in NICE DEMS by system administrator/s.
MI-4.3.15	Manage & Track Chain of Custody	The solution shall provide the ability to control, track and report the sequence of custody.	P	X				All assignments and reassignments are tracked in the NICE DEMS activity log, and become part of the overall chain of custody tracking. All of these details are shown on chain of custody reports.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
		Review Evidence						
RE-5.3.1	Search Evidence	The solution shall provide the ability to search for digital evidence by metadata associated with the content.	P	X				NICE DEMS solutions provides extensive analytics capabilities to assist users in finding relevant information in digital evidence originating from virtually anywhere. All types of evidence can be searched by virtually any combination of collected metadata, to include date, time, user, geolocation, free text wild cards or partial information, and any other data that is either automatically collected or manually entered during evidence uploads. The solution provides a simple free-text, Google-like search to the user to flexibly search for any type of content with powerful filter tools to further refine a search.
RE-5.3.2	Search Evidence	The solution shall provide the ability to search for digital evidence by simply entering one or more keywords from the files contained within the content (e.g., within a case or evidence files).	P	X				Document indexing and audio/video analytics are available to support searching of document content as well as audio content associated with video and audio recordings. The solution provides a simple free-text, Google-like search to the user to flexibly search for any type of content (including keywords) with powerful filter tools to further refine a search.
RE-5.3.3	Search Evidence	The solution shall provide the ability to search audio and video for a word, phrase, or name (full- text and phonetically).	D	X				NICE DEMS solutions provides the ability to search audio and video for words, phrases, names, sayings, and more. NICE DEMS uses transcripts automatically generated to become searchable. Therefore, fuzzy search for any combination of letters, numbers, and punction is available. NICE users are alwso able to apply phonetic transcription to any meta data field or description which will become searchable at that point.
RE-5.3.4	Search Evidence	The solution shall provide the ability to search video for major events / scene changes (e.g., passing car or person on a security camera clip).	D				X	NICE DEMS does not natively provide this capability. However, we are happy to work on a solution with a 3rd party Video Analytics partner to provide needed functionally for the County. This capability is currently not included in our quoted response. Additional effort and cost would be required to provide this functionality.
RE-5.3.5	Search Evidence	The solution shall provide the ability to search video through facial recognition.	D			X		Due to legal ambiguity regarding facial recognition vs. facial tracking, NICE DEMS has opted for facial tracking to be included as a standard feature. Each track (i.e. Face) identified through our facial tracking engine is able to be re-named and labeled appropriately by a NICE DEMS user during the redaction process. These labels (or suspected names) can also be added to the evidence item as a keyword, comment, or description which are then made searchable. However, we are happy to work on a solution with a 3rd party Video Analytics partner to provide needed functionally for the County. This capability is currently not included in our quoted response. Additional effort and cost would be required to provide this functionality.
RE-5.3.6	Search Evidence	The solution shall provide the ability to search for digital evidence across cases, based on user security roles.	P	X				Users of NICE DEMS are able to search for digital evidence across all cases. When providing search results, if a user does not have the proper privileges to access a search result, this will be visually identified in the NICE DEMS UI. The user will be provided details on the case # and case owner so that the user can then follow up with the appropriate person and request access to view the evidence item.
RE-5.3.7	Search Evidence	The solution shall provide the ability to narrow their search by one or more metadata values.	P	X				NICE DEMS solutions provides extensive search capabilities to assist users in finding relevant information in digital media stored in NICE DEMS or any of its connected data sources. All types of evidence can be searched by virtually any combination of collected metadata, to include date, time, user, geolocation, free text wild cards or partial information, and any other data that is either automatically collected or manually entered during evidence uploads. The solution provides a simple free-text search to the user to flexibly search for any type of content with powerful filter tools to further refine a search. The user can enter any string of words such as a name, a license plate number, an address, etc., and the system will look for matches and near matches across all indexed data. Filtering tools are available to assist the user in narrowing down search results to easily find items of interest.
RE-5.3.8	Search Evidence	The solution shall provide the ability to search for digital evidence, based on user-defined criteria.	P	X				NICE DEMS solutions provides extensive search capabilities to assist users in finding relevant information in digital media stored in NICE DEMS or any of its connected data sources. All types of evidence can be searched by virtually any combination of collected metadata, to include date, time, user, geolocation, free text wild cards or partial information, and any other data that is either automatically collected or manually entered during evidence uploads. The solution provides a simple free-text search to the user to flexibly search for any type of content with powerful filter tools to further refine a search. The user can enter any string of words such as a name, a license plate number, an address, etc., and the system will look for matches and near matches across all indexed data. Filtering tools are available to assist the user in narrowing down search results to easily find items of interest.
RE-5.3.9	View Evidence	The solution shall provide the ability to view a list of all digital evidence associated with a case.	P	X				Within the Case View, the user can open a case folder to view all collected evidence and incident details associated with the case. Digital evidence case folders are automatically created via an integration with RMS or CMS. No manual case creation is required. ·The assigned detective/investigator/prosecutor in RMS/CMS becomes the owner of the case folder in NICE DEMS ·All relevant incident details are collected and made visible in NICE DEMS to provide context to the digital evidence that is being reviewed. ·Case folders can also be created manually if needed. When a user opens a NICE DEMS case folder, the user is presented with a view of all of the evidence associated with a case. Each evidence item is visualized as an evidence card with summary information such as: ▢Evidence Type (audio, video, document, image) ▢Evidence Name ▢Data Source (where the evidence originated) ▢Thumbnail preview of the evidence item

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RE-5.3.10	View Evidence	The solution shall provide the ability to synchronize the viewing of multiple content sources by timestamp.	D	X				Evidence Timeline view is provided with NICE DEMS. The user has the ability to select evidence items in a given case and synchronously play them in the NICE DEMS Timeline View. With this powerful tool, a user can listen and playback the media synchronized together in the order in which these events occurred during the incident. An example would be the ability to listen to the initial 911 call while simultaneously viewing collected CCTV video captured at the scene. Other incident triggers such as those from gunshot detection systems can also be included on the timeline for further insight into the unfolding of an incident.
RE-5.3.11	View Evidence	The solution shall provide the ability to view notes and/or annotations associated with the digital evidence, based on user roles.	P	X				In addition to viewing an evidence item, the user can perform the following actions associated with the evidence item: - View and update associated metadata fields - Add/view a keyword tag to an evidence item for creating special groupings with the case folder - Add/view a comment/bookmark/annotation
RE-5.3.12	View Evidence	The solution shall provide the ability to view text and image evidence without requiring the file to be exported/downloaded	H	X				NICE DEMS solutions provide users the capability to view/playback and stream text, video and images right from the NICE DEMS interface operating on the Azure Cloud. There is no need to export or download evidence items to PC devices.
RE-5.3.13	View Evidence	The solution shall provide the ability to view or stream video evidence without requiring the file to be exported/downloaded	P	X				NICE DEMS solutions provides users the capability to view/playback and stream text, video and images right from the NICE DEMS interface operating on the Azure Cloud. There is no need to export or download evidence items to PC devices.
RE-5.3.14	View Evidence	The solution shall provide the ability to annotate and generate derivative content without downloading, including but not limited to: • bookmarking • translating (Spanish and other languages), • watermarking	P	X				NICE DEMS is the one single location for all evidence tools. Users are able to generate annotations, comments, bookmarks, a transcription and translated transcription, and much more all within one platform. This content is produced within the system and is linked to the original evidence file as to maintain the appropriate association. There is no need to download evidence or derivative content.
RE-5.3.15	View Evidence	The solution shall support map tile integration common for integrating with ESRI GIS systems	D	X				NICE has the ability to integrate with ESRI GIS by calling the server tiles to display within NICE DEMS.
RE-5.3.16	View Evidence	The solution shall provide the ability to view digital evidence through a provided viewer or player with standard play, rewind, fast forward and stop features.	M	X				To review a recording in NICE DEMS, the user simply clicks on the evidence name on the card in the Evidence view. The user is then presented with a play icon along with all the metadata details associated with the recording. By clicking the play button, the recording will begin playing in the player that's built directly in the NICE DEMS interface, and the user will be presented with additional player tools to assist in reviewing the recording: ▫Play/fast forward/rewind ▫.25x – 4x speed controls ▫Frame by frame advance ▫Zoom controls ▫Audio volume control ▫bookmark/comment on points of interest in the video recording
RE-5.3.17	View Evidence	The solution shall provide the ability to view digital evidence that does not require finding, installing, configuring, or maintaining CODECs, viewers and players.	M	X				When media is uploaded to NICE DEMS, the platform saves the original copy and automatically transcodes the original into a working copy with a standard format that is then viewable directly via the NICE DEMS user interface using a standard web browser. The working copy can also be readily shared with other users for universal viewing or playback. Benefit- County DEMS users are able to play video collected from local Law Enforcement and private businesses and citizens without wasting time otherwise needed for locating codecs and installing players.
RE-5.3.18	View Evidence	The solution shall provide the ability to restrict access to specific digital evidence to view-only, based on user roles.	P	X				NICE DEMS solutions implements an attribute based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know". The control of access rights are established in NICE DEMS via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role. It is also possible to create a connection to synchronize and inherit access control rules with a customer's existing records management system as a custom integration.
RE-5.3.19	View Evidence	The solution shall provide the ability to convert video digital evidence into common video formats (e.g., WMV, MP4, AVI, MOV, FLV), while maintaining the original copy.	M	X				NICE DEMS solutions automatically transcodes the original into a working copy with a standard format (see below) that is then viewable and playable via the NICE DEMS media player(s) using a standard web browser. oVideo - .mp4 oAudio - .aac oPictures - .jpg oDocuments - .pdf

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
RE-5.3.20	View Evidence	The solution shall provide the ability to synchronize the viewing of multiple content sources by timestamp.	D	X				With NICE DEMS Evidence Timeline view, the user has the ability to select evidence items in a given case and play them in the synchronized manner. With this powerful tool, a user can listen and playback the media synchronized together in the order in which these events occurred during the incident. An example would be the ability to listen to the initial 911 call while simultaneously viewing collected CCTV video captured at the scene. Other incident triggers such as those from gunshot detection systems can also be included on the timeline for further insight into the unfolding of an incident.
RE-5.3.21	View Evidence	The solution shall provide the ability to view multiple videos simultaneously	H	X				NICE DEMS solution allows multiple videos to be played from the NICE DEMS interface (along with audio files if desired) simultaneously - side by side in a tiled view, or on a timeline, or in a geographic map.
RE-5.3.22	View Evidence	The solution shall provide the ability to view video files in variable motion (e.g., frame by frame or slow motion).	D	X				To review a recording in NICE DEMS, the user simply clicks on the evidence name on the card in the Evidence view. The user is then presented with a play icon along with all the metadata details associated with the recording. By clicking the play button, the recording will begin playing and the user will be presented with additional player tools to assist in reviewing the recording: □ Play/fast forward/rewind □ .25x – 4x speed controls □ Frame by frame advance □ Zoom controls □ Audio volume control □ Bookmark/comment on points of interest in the video recording
RE-5.3.23	View Evidence	The solution shall provide the ability to view the metadata associated with digital evidence upon playback.	P	X				Once an evidence item is located in NICE DEMS, a user can open the item and view the media and associated metadata within the NICE DEMS user interface.
RE-5.3.24	View Evidence	The solution shall provide the ability to view digital evidence content as thumbnails or full size images/videos.	D	X				Digital evidence items can be viewed as thumbnails for the user to easily scan a selection of digital evidence items. The user can also select a given evidence item to expand the view via the media player, for full screen visibility along with having access to additional media player tools.
RE-5.3.25	Bookmark Evidence	The solution shall provide the ability to link reference points across digital evidence files.	H	X				NICE DEMS allows for users to tag evidence items within cases with Keywords. This is NICE's way of adding annotations to files in order to link/reference points across Digital Evidence files. Keywords are a quick and easy way to group a subset of information within a case together to quickly cross reference. NICE DEMS also allows for evidence item annotations, comments, and case comments; all of which are searchable globally.
RE-5.3.26	Bookmark Evidence	The solution shall provide the ability to enter reference points (e.g., time stamping in audio/video files and page stamping in documents) throughout the digital evidence file.	P	X				Bookmarks and comments can be added as reference points in a digital evidence items in NICE DEMS interface. These bookmarks and comments can also be shared alongside the digital evidence items when forwarding a case file to another justice partner (e.g. from law enforcement to the prosecutor.)
RE-5.3.27	Watermark Evidence	The solution shall provide the ability to add a unique identifier or watermark to selected digital evidence.	P	X				A unique identifier is automatically added to each evidence item that is ingested in NICE DEMS. In addition, a user has the ability to add a unique identifier to selected digital evidence.
RE-5.3.28	Watermark Evidence	The solution shall provide the ability to configure a watermark.	P	X				NICE DEMS does not support adding watermarks to printed evidence items (photos, documents, etc.). NICE DEMS does support adding unique identifiers on document and photos. The unique reference ID can be configured by the DEMS System administrator for end users.

Generate Derivative Content

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
GC-6.3.1	Redact Evidence	The solution shall provide the ability to create a redacted version of content (e.g., a piece of audio, video, document or digital photo) by using the solution tools available so that certain content remains confidential.	P	X				NICE DEMS solutions offers tools for the user to create variants of the working copy that can be used to highlight or obscure segments of the digital media. The variant copies that are created remain linked to the parent working copy in NICE DEMS and are visible whenever the parent evidence item is selected by the user. User can: - Create snapshots of key frames of video within the working copy. - Create video clips of key segments of video within the working copy - Create audio clips of key segment of audio within the working copy. - Redact objects is the video to ensure privacy of citizens and locations prior to sharing with others outside of the judicial process. - Redact portions of the audio file so that names, addresses, and other sensitive information is removed prior to sharing with others outside of the judicial process. -Enhance video and images directly with Adobe-like tools. -Extract specific selected portions of digital evidence. -Annotate and add notes to digital evidence.
GC-6.3.2	Redact Evidence	The solution shall provide the ability create a relationship between the source and redacted version (e.g., hierarchy tree structure) so that tracking and audit trail of that content can occur.	P	X				NICE DEMS solutions offers tools for the user to create variants of the working copy that can be used to highlight or obscure segments of the digital media. The variant copies that are created remain linked to the parent working copy in NICE DEMS and are visible - in a clear hierarchy - whenever the parent evidence item is selected by the user.
GC-6.3.3	Redact Evidence	The solution shall provide built-in enhancement capabilities to improve video and images directly	D	X				NICE DEMS provides interfaces for users to enhance video and images directly with Adobe-like tools.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
GC-6.3.4	Redact Evidence	The solution shall provide the ability to automatically blur selected recognizable features (e.g., face, distinguishable marks, license plates, signs) in a video.	D	X				NICE DEMS provides the ability for the user to identify face/s or other recognizable objects such as license plates and then select to blur the selected item throughout a video segment.
GC-6.3.5	Redact Evidence	The solution shall provide the ability to automatically redact text in documents based off of keyword(s).	H	X				NICE DEMS solutions provide tools to redact and search text in documents based off of any keywords.
GC-6.3.5	Redact Evidence	The solution shall provide the ability to disguise voices in video and audio digital evidence files.	D		X			NICE DEMS does not provide the ability to disguise voices in video or audio files. Currently, audio can only be redacted.
GC-6.3.6	Excerpt Evidence	The solution shall provide the ability to extract specific selected portions of digital evidence content.	P	X				User of NICE DEMS solutions can: - Create snapshots of key frames of video within the working copy. - Create video clips of key segments of video within the working copy - Create audio clips of key segment of audio within the working copy. - Extract specific selected portions of digital evidence.
GC-6.3.7	Excerpt Evidence	The solution shall provide the ability to link and associate video/audio excerpts.	D	X				Digital evidence items and created excerpts can be linked together in NICE DEMS via our Keyword linking capability. Items can be joined together via a keyword(s) created by the user. The keyword becomes a common metadata tag that can be used to filter to the identified group of items and view/share as desired.
GC-6.3.8	Annotate Evidence	The solution shall automatically show the source or originating agency for any piece of evidence or derivative content.	H	X				NICE DEMS will automatically categorize individual evidence items by data source as well as originating agency. For the Sheriff's Department, this is especially true as NICE will connect into each individual data source. As evidence is shared on to connecting agencies, that meta data will be linked to that evidence. Evidence uploaded from external-to-NICE agencies, can be flagged and filtered by the originating agency and/or source (i.e. Requests, community appeal, direct upload, etc.).
GC-6.3.9	Annotate Evidence	The solution shall provide the ability to add notes and/or annotations without altering the original digital evidence file. Access/permission to view these notes shall be restricted to the generating agency and shall not pass with the evidence	P	X				NICE DEMS allows authorized users to annotate and add notes to digital evidence, using working copies of evidence items (while preserving the integrity of the original evidence file). Generating agency may elect to share (or not share) these notes as it shares evidence items with another party.
GC-6.3.10	Annotate Evidence	The solution shall provide the ability to associate and link annotations across digital evidence files.	D	X				NICE DEMS allows for users to tag evidence items within cases with Keywords. This is NICE's way of adding annotations to files in order to link/reference points across Digital Evidence files. Keywords are a quick and easy way to group a subset of information within a case together to quickly cross reference. NICE DEMS also allows for evidence item annotations, comments, and case comments; all of which are searchable globally.
GC-6.3.11	Annotate Evidence	The solution shall provide the ability to apply multiple time markings in video and audio digital evidence files, indicating important evidence occurrences.	P	X				Multiple bookmarks/comments can be added to video and audio digital files.
GC-6.3.12	Transcribe Evidence	The solution shall provide the ability to generate automated transcription of audio and video digital evidence.	P	X				NICE DEMS solutions offers automated transcription of both audio and video evidence. Media files can be automatically transcribed upon ingestion. The resulting transcript remains synchronized to the media playback - as video progresses, so does the transcripted text, using time stamps associated to each transcripted phrase. This also makes it easy for users to review and update the transcribed text in the same interface as the audio/video playback, as part of the official transcript. The transcript document is generated and saved in the cloud, just like all other evidence. The transcript is also searchable, using a word, partial word, or a phrase, to find all recordings matching the search criteria.
GC-6.3.13	Transcribe Evidence	The solution shall provide the ability to transcribe dialogue in audio/video content to selected languages and/or dialects (e.g. Spanish) and associate with specific speakers. Proposer shall provide a list of supported languages.	P	X				NICE DEMS provides the ability to transcribe dialogue in audio/video content from over one hundred languages/and or dialects (including Spanish). Individual speakers can be distinguished and tagged with distinguishing labels. The following link provides the languages NICE DEMS supports. https://learn.microsoft.com/en-us/azure/cognitive-services/speech-service/language-support?tabs=stt#supported-languages
GC-6.3.14	Transcribe Evidence	The solution shall provide the ability to translate content to selected languages and/or dialects (e.g. Spanish) and associate with specific speakers. Proposer shall provide a list of supported languages.	P	X				NICE DEMS solutions provides the ability to translate dialogue in audio/video content from hundreds of languages/and or dialects (including Spanish) to a desired language. Individual speakers can be distinguished and tagged with distinguishing labels.
	Archive and Dispose Evidence							
AD-7.3.1	Archive / Preserve Evidence	The solution shall provide the ability to archive digital evidence to a lower tier file storage level, based on associated retention period.	P	X				NICE DEMS solutions provides robust long-term retention solutions for agencies that can be customized based on each agency's retention policies. While a case is open in NICE DEMS, it remains in 'Hot' storage within the Microsoft Azure Gov Cloud. Once that case is closed, and per the agency's triggers, cases will then be moved into an archive state which is a lower tier storage level aimed to manage long-term retention in a cost effective, automated, and timely way.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
AD-7.3.2	Archive / Preserve Evidence	The solution shall provide the ability to restore archived digital evidence.	P	X				NICE DEMS solutions provides the ability to rehydrate archived digital evidence There are currently two rehydrate priorities - High and Standard. Standard priority retrieves the media in approximately 15 hours and High priority can recover the media in approximately 1 hour for media under 10GB.
AD-7.3.3	Establish Retention Rules	The solution shall provide the ability to create independent retention polices for each agency or instance of the system, to ensure that digital evidence is available to users/groups/roles for the required amount of time, as configured by each agency.	M	X				NICE DEMS can automatically manage evidence retention based on predefined rules for every agency. Retention rules can be set based on any metadata characteristic or a combination of characteristics of an evidence item. Two of the most common parameters used to create retention rules include: ☐The type of case – Digital evidence can inherit the retention category that is assigned to a given case as obtained from metadata collected from the connected CAD or RMS. For example, retention rules can be based on case type and case status. For example, a retention policy can set retention for burglary cases to be 5 years, homicide cases to be retained forever, etc. All digital evidence items within a burglary case will inherit the 5 year retention rule unless overridden manually (by an authorized user). ☐The type of evidence –An evidence item type such as crime scene photos, body camera recordings, etc. can have a pre-defined deletion date such as 'x' months, once defined as a rule. A retention policy could be established that enforces cases to be present in the DEMS for 5 years and then sent to another secure retention repository for another 7 years. Once the retention rules are defined and updated in NICE DEMS, all evidence, upon upload to NICE DEMS, is assigned a retention category. Storage of an evidence item is then managed based on the assigned retention category and an appropriate deletion or move date is set. Reviews and approvals for deletion/move actions can be included as part of any retention policy set in NICE DEMS. Prior to the deletion/move of an evidence item, a retention policy can be configured to send an approval notice to a designated user(s) who then has the ability to review and approve the deletion/move or extend the retention period of the evidence item as needed. The evidence item will only be deleted/moved when the approval is provided.
AD-7.3.4	Establish Retention Rules	The solution shall provide the ability to override a retention or archiving policy to ensure that the digital evidence is treated accordingly.	P	X				NICE DEMS solutions users with the proper privileges can override an archiving or deletion date that has been set based on an established retention policy. The user is able to provide an updated archiving or deletion date that will then be managed by NICE DEMS accordingly.
AD-7.3.5	Establish Retention Rules	The solution shall provide the ability for the retention and archiving functions to be additive in the circumstance of differing rules applied to the content.	P	X				NICE DEMS solution's retention policy can be set so that retention and archiving functions can be additive in the circumstance of differing rules applying to the same content.
AD-7.3.6	Establish Retention Rules	The solution shall provide the ability for users (with the appropriate permissions) to update retention policies that apply to their agency or instance of the solution	P	X				NICE DEMS solution's users with the proper privileges can override a archiving or deletion date set based on an established retention policy. The user is able to provide an updated archiving or deletion date that will then be managed by NICE DEMS accordingly.
AD-7.3.7	Dispose Evidence	The solution shall provide the ability to identify the digital evidence nearing the end of the defined retention policy and generate a notification to the appropriate users/groups/roles.	P	X				Once a digital evidence item is assigned a retention category, it is managed in NICE DEMS according to the rules associated to that category. An archival date or a deletion date is set along with dates for review. The item is flagged for archival or deletion based upon the date set by the retention policy. Designated users are notified for reviews and approvals or these users are provided the opportunity to update the retention date as needed. Prior to archiving or deleting, the system will prompt the user to confirm the user's desire to complete the archive/deletion. If a user confirms and then realizes that a mistake has been made, the user has the ability to contact the System Administrator to restore the digital asset back to active storage. There is a "regret bucket" for deletions that has a timeframe of 'xx' days as configured by the customer. Once 'xx' days have passed, a digital asset is permanently deleted from the system and cannot be retrieved.
AD-7.3.8	Dispose Evidence	The solution shall provide the ability to export digital evidence for the purpose of archiving.	P	X				When archiving an evidence item, the item is moved from active storage and stored in the NICE DEMS Archive storage location. This is a lower cost storage location where access to the stored data is possible but not immediate. Associated metadata remains in NICE DEMS active storage and is available for searching. Users with the appropriate privileges can request access to archived digital assets at any time via NICE DEMS.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response				Comments or Page and Section number in the proposal where additional information can be found.
				Y	N	C	T	
AD-7.3.9	Dispose Evidence	The solution shall provide the ability to permanently delete digital evidence individually or in batches, based on built-in retention rules and periods.	P	X				When deleting an evidence item, the item is permanently removed from NICE DEMS cloud storage. As a default, all metadata associated with the deleted evidence items remains in NICE DEMS. However, metadata can also be deleted (purged) if desired by the County. In general, retention rules can be set based on any metadata characteristic or combination of characteristics of a digital asset (and the deletion can then occur for individual evidence items or batches of evidence, as applicable). Reviews and approvals for deletion can be included as a part of any retention policy set in NICE DEMS. Typically digital assets are configured to inherit the retention category that is assigned to a given case as obtained from metadata collected from the connected CAD or RMS. NICE DEMS automatically updates the retention classification of a Digital Asset when an update is made in CAD/RMS. This ensures that NICE DEMS contains accurate information consistently.

Support Evidence Management

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
SE-8.3.1	Manage Workflows	The solution shall provide the ability to define specific business rules and apply to built-in workflows.	P	X				With NICE DEMS solutions, workflows can be set up to help users manage the collection and processing of evidence through consistent, repeatable, agency-approved processes. Your investigators, officers, and other authorized personnel can initiate workflow requests through NICE DEMS; the system tracks and logs all requests and automatically notifies the investigator (or another designated user) when those requests have been fulfilled. Approval steps can be configured as a part of any NICE DEMS Workflow, to ensure proper oversight within the organization. Following are examples of default NICE DEMS Workflows. □ Initiate a request for CCTV video footage □ Initiate a request for evidence to a person associated with an Investigation □ Initiate a Public Appeal for information related to an in+l111cident □ Initiate a Request for Evidence (e.g. photographs) from another department Additional workflows can be added to meet your organizations specific needs. Examples of other workflows could include: □ Initiate a request for evidence processing from another department or agency (e.g. forensic crime lab) □ Initiate a request for evidence from another agency □ Initiate a request for a follow up (interview someone, collect evidence, etc.)
SE-8.3.2	Manage Workflows	The solution shall provide the ability to define specific business rules and create customized workflows.	M	X				See answer to 8.3.1 above. Additionally, NICE will work with County to understand customized workflows and can create form, field, filter, request, etc. workflows per the County's wishes.
SE-8.3.3	Manage Workflows	The solution shall provide the ability to trigger workflows that perform individual or a sequence of DEMS activities including but not limited to applying bates stamps, excerpts, redactions, transcriptions, translations, annotations, add tags/metadata, renaming files, file conversions and notifications.	P	X				NICE DEMS provides customizable workflows in support of consistent, repeatable processes for evidence collection and sharing. •It starts with tight linkage to your organization's existing Case Management platform for case folder creation and automated case assignment workflows in the NICE DEMS. Relevant case details and associations, subjects, vehicles, and property records are automatically added to NICE DEMS case folders. •Case Creation in NICE DEMS automatically triggers evidence collection workflows including evidence request workflows from partner Police Agencies and others as relevant for each case. •Case details from RMS trigger automated collection of evidence from other connected data sources. •Rapid evidence collection from other agency departments, businesses, communities, and individuals is available – on-scene and remotely •Automated alerts & notifications keep case owners abreast of case updates and completion of key workflow milestones. Disclosure workflows can also be implemented for evidence sharing. Finally, Evidence retention workflows are automated for hands free management of evidence per County compliance guidelines. •Workflows can also be created to trigger when items require redactions, transcriptions, translations, etc. All workflow activity is tracked.
SE-8.3.4	Manage & Generate Notifications	The solution shall provide the ability to customize notifications as needed.	P	X				NICE DEMS users have the ability to set up personalized alerts and notifications for over 200 various types of case and evidence activities. These notifications can be customized by selecting from the menu of all options by each user, turning them off/on, requesting an email only, requesting email and in-application notification, and forwarding the notification(s) to another user or group of users. Each users' notification settings are unique to that individual.
SE-8.3.5	Manage & Generate Notifications	The solution shall provide the ability to trigger alerts based on milestones, statuses and/or upcoming events, as defined by the user.	H	X				NICE DEMS triggers alerts based on system and end user generated case activity. NICE DEMS users have the ability to set up personalized alerts and notifications for over 200 various types of case and evidence activities. These alerts are not user defined but can be customized by turning them off/on, requesting an email only, requesting email and in-application notification, and forwarding the notification(s) to another user or group of users. Each users' notification settings are unique to that individual.
SE-8.3.6	Manage & Generate Notifications	The solution shall provide the ability generate notifications to the corresponding agency when new supplemental discovery is available.	P	X				NICE DEMS solutions provides an email and/or in application notification to the user when new evidence is available. Whenever the Sheriff shares to the District Attorney's NICE platform and then the District Attorney shares to the Public Defenders' NICE application, the user on each system will be notified that any new supplemental discovery is available. A link to the corresponding case folder will be included in the email and/or in-application notification for the user to navigate directly to the now available evidence. Sheriff's Office users will be notified whenever the DSG finds new evidence and automatically places it in the correct folder within their NICE system.
SE-8.3.7	Manage & Generate Notifications	The solution shall provide the ability to configure when and where notifications are sent.	P	X				Currently notifications are sent the users/roles/groups that are configured in a workflow. Updates to our default set up for notifications can be configured as we learn more about the County's workflows. Notifications can be configured to be received in the application, via email, or via text.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
SE-8.3.8	Manage & Generate Notifications	The solution shall provide the ability to notify users/groups/roles when new digital evidence is shared with them.	P	X				NICE DEMS solutions users have the ability to set up personalized alerts and notifications for various types of case and evidence activity, as means of increased productivity and rapid response to updates. A User can receive notifications when they are assigned a new case, when changes or updates are identified for evidence items related to their assigned cases, or when it is time for an officer to provide an update to an open case. Evidence-based notifications are provided to alert the user of activity regarding digital assets that are associated with their assigned cases. Notifications will alert a user when evidence is added to an assigned case folder, when metadata has been updated, when a digital asset has been edited and a child asset is created, when an evidence item is marked for deletion.
SE-8.3.9	Manage & Generate Notifications	The solution shall provide the ability to notify users/groups/roles when existing digital content is updated.	P	X				Notifications will alert a user when evidence is added to an assigned case folder, when metadata has been updated, when a digital asset has been edited and a child asset is created, when an evidence item is marked for deletion. Notifications are also sent to alert the user when digital assets from their assigned cases are downloaded. Other notifications can be set up to alert the user concerning the progress of requests that have been initiated including when the requests are read and when the requests are fulfilled or rejected.
SE-8.3.10	Manage & Generate Notifications	The solution shall provide the ability to notify users/groups/roles when a retention period is nearing expiration. (Requirement may also be satisfied by a dashboard or other display)	P	X				Once a digital evidence item is assigned a retention category, it is managed in NICE DEMS according to the rules associated to that category. An archival date or a deletion date is set along with dates for review. The item is flagged for archival or deletion based upon the date set by the retention policy. Designated users are notified for reviews and approvals or these users are provided the opportunity to update the retention date as needed. Prior to archiving or deleting, the system will prompt the user to confirm the user's desire to complete the archive/deletion. If a user confirms and then realizes that a mistake has been made, the user has the ability to contact the System Administrator to restore the digital asset back to active storage. There is a "regret bucket" for deletions that has a timeframe of 'xx' days as configured by the customer. Once 'xx' days have passed, a digital asset is permanently deleted from the system and cannot be retrieved.
SE-8.3.11	Manage & Generate Notifications	The solution shall provide the ability to generate manual notifications.	H			X		NICE DEMS users have the ability to set up personalized alerts and notifications for various types of case and evidence activity. There are over 200 notifications already built into the system. To date, this variety has satisfied every notification our customers have requested. Should the County want to add a notification that does not exist in the current offering, NICE is willing to work with the County to understand their need.
SE-8.3.12	Manage & Generate Notifications	The solution shall provide the ability to generate notifications via various channels of communication, including email, SMS, or in-application messaging. Proposer shall provide a list of supported notification channels.	D	X				All NICE DEMS alerts and notifications can be viewed in the Notifications Panel located in the user interface. NICE DEMS users can also request alerts via email or text message.
SE-8.3.13	Record & Maintain Audit Trail	The solution shall provide the ability to track and record all activities completed or attempted, including but not limited to: - When content is added, updated, moved, or deleted - When permissions are changed - When users/groups/roles are added, changed, or removed	M	X				NICE DEMS solutions automatically tracks all instances of access to each evidence item, logging user ID, date, time, and the specific action(s) taken with the evidence item (uploaded, accessed, download, share, update metadata, etc.), including details around each action. Following is an example list of case and evidence activities audited in NICE DEMS: Case Activity - case created; case accessed by user; case comment added by user; case details (metadata) modified by user; case downloaded by user; case access granted/revoked by user; case shared by user Evidence Activity – evidence uploaded; evidence virus check completed; evidence hash created/signed; evidence working copy created; evidence accessed by user; evidence details (metadata) modified by user; evidence clip created; evidence snapshot created; evidence redaction created; evidence bookmarks/comments added; evidence downloaded by user; evidence shared by user.
SE-8.3.14	Record & Maintain Audit Trail	The solution shall provide the ability to track all enhancements, edits, redactions and transactions associated with digital evidence.	P	X				NICE DEMS tracks all enhancements, edits, redactions, translations, notations, and all other actions on all evidence items, including the author of each change and its date and time.
SE-8.3.15	Record & Maintain Audit Trail	The solution shall provide the ability to generate audit reports of all historical tracking over all agencies or instances of the software	P	X				Every individual case and each evidence item stored in NICE DEMS has its own historical activity log and chain of custody report. This report is created from the information stored in the NICE activity logs. The information in the Chain of Custody report can be utilized in court proceedings to validate the authenticity of evidence items. System Administrators have access to a system master audit log in the NICE DEMS Administration Portal. This logs all system activity, both system and end-user generated. Administrators can access the master audit log and search for any type of specific audit activity. Search results can be exported in a .csv file format.
SE-8.3.16	Control Access to Evidence	The solution shall provide the ability to change the access and permissions on original and redacted digital evidence to ensure that confidentiality of content is maintained.	P	X				A redacted version on a digital evidence item can have different access rights than the parent item.
SE-8.3.17	Share Players and Codecs	The solution shall provide the ability to import, share and store proprietary players and codecs.	M	X				Proprietary players can be uploaded and stored alongside the video in NICE DEMS so that, if needed, the video with the proprietary player can be shared or downloaded for playing locally.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response Y	N	C	T	Comments or Page and Section number in the proposal where additional information can be found.
SE-8.3.18	Manage User Role	The solution shall provide the ability to create and modify a user role.	P	X				NICE DEMS solution's user roles can be created and modified via the NICE DEMS Admin Portal.
SE-8.3.19	Manage User Role	The solution shall provide the ability to assign a role to a user and restrict access based on the assigned role.	P	X				Roles can be assigned to users in the NICE DEMS Admin Portal. Access can be added or restricted based on user roles
SE-8.3.20	Manage User Role	The solution shall provide the ability to make security permission changes at the security group and user levels.	P	X				NICE DEMS solutions implements Rules-Based Access Control through its use of attribute-based access control (ABAC). ABAC allows access rights to be granted through controlled rules that can be very granular. These rules can grant access based on any attributes of users or other system factors. Rules can be created to limit access to certain cases or types of cases. Rules can also be created to limit what a user is able to do once provided access to a case/evidence. For example, the user can be granted view only access, or may be restricted from sharing. The ABAC rules can be configured to build Role-Based Access Control (RBAC) or more complex arrangements as required. The framework is flexible and can provide the level of access controls required by ISAB. NICE will work with ISAB to create ABAC mappings to existing or new ISAB user roles.
SE-8.3.21	Manage User Role	The solution shall provide the ability to assign users to teams based on digital evidence types so that incoming content is routed to and worked on by the appropriate teams.	D	X				NICE DEMS solutions users can be assigned to groups so that all users in that group have access to NICE DEMS requests that are routed to that group. NICE DEMS access controls and platform privileges can be established for that particular group. For example, the County can create a 911 group in NICE DEMS and configure the group to only receive and fulfill 911 requests. Users assigned to the 911 group will be able to re+H151ceive Investigate 911 requests and upload 911 audio to fulfill the requests. These users could also be configured for additional functionality as deemed appropriate by the customer.
SE-8.3.22	Manage Administrator Dashboard	The solution shall provide the ability to access a consolidated overview dashboard of the County digital evidence status, content (e.g. caseloads), alerts and customizable key metrics.	D	X				NICE DEMS solutions Administrator Portal provides all of the necessary tools to configure and maintain NICE DEMS for needed access and evidence availability. The Administrator Portal is where the designated System Administrator(s) can set-up and manage users, groups and user permissions. On the system level, the system administrator can: ☐Configure and modify Case and Evidence card views and metadata fields ☐Manage Evidence Retention Policies ☐Set up access control settings such as password login settings and logon messages ☐Create and manage security certificates ☐Configure the Welcome page for the Investigate Community Portal ☐Manage registered users for the Investigate Community Portal All metadata fields are labeled by the customer and can use the customer's vocabularies and taxonomies. NICE DEMS integrations inherit the taxonomies and vocabularies from the County's source systems including things like crime type lists from RMS tables, etc. which are then used by NICE DEMS for sorting, filtering, labeling on cards for cases & evidence, etc. A unified view of all evidence is created so that data from the various data sources are viewed and labeled according to County preferences. A system wide audit log is available in the NICE DEMS Administrator Portal. All activity in NICE DEMS is tracked and logged. This includes platform-generated activity, user-generated activity, and system administration activity. Each audit log entry details what action was performed, who performed the action, when it was performed, and any additional details on the associated digital evidence item. Data on digital evidence volumes, status, and other metrics is tracked as well. The user is able to find any subset of information using the search and filtering tools provided. The user can also export the data in a .CSV format to be imported to an external report generating platform if desired.
SE-8.3.23	Detect and Prevent Malware	The solution shall provide the ability for virus scanning, detection and control.	P	X				All media uploaded to NICE DEMS is scanned for viruses/malware. If malware is detected, uploading of the infected media is terminated. The user is notified and appropriate audit logs are created. If Santa Barbara County so desires, NICE DEMS can be configured to upload the infected media to a quarantined storage location where it can be accessed for download by those with appropriate access privileges. Media detected to be infected with malware is not able to be viewed or managed in NICE DEMS alongside other media.
SE-8.3.24	Detect and Prevent Malware	The solution shall provide the ability to notify the users/groups/roles of detected malware.	P	X				Users/groups/roles are notified of detected malware.
SE-8.3.25	Detect and Prevent Malware	The solution shall provide the ability to encapsulate detected malware in an encrypted form.	H			X		Currently, NICE DEMS terminates the upload process of any evidence item detected with malware. The user is notified. In an upcoming release targeted for Y2024, NICE DEMS will have ability to store/quarantine the evidence item and encapsulate the detected malware in an encrypted form.
SE-8.3.26	Generate Reports	The solution shall provide the ability to manually export data using different report output formats (e.g. Word, Excel, CSV, PDF, XML). Proposer shall provide a list of output formats.	P	X				NICE DEMS records information on data stored in the cloud, including the number of digital assets, the types of digital assets, and the size of digital assets stored. NICE Audit information is accessible via the System Administration Portal for users with the appropriate privilege assigned. The user is able to find any subset of information using the search and filtering tools provided (filter by date ranges, incident type, case status, etc.). The user can also export the data in a .CSV format to be imported to an external report generating platform. There are additional data reports that can be generated at a case level and exported in .PDF form.

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response				Comments or Page and Section number in the proposal where additional information can be found.
				Y	N	C	T	
SE-8.3.27	Standardize Integration	The solution shall provide the ability to integrate with other systems and databases through a standard API.	M	X				NICE DEMS solutions has been uniquely designed to require minimal end user action for evidence collected and managed in the platform. Once the NICE DEMS integrations are properly configured (using a variety of standard API's as needed) and connected to Santa Barbara County data sources, no further intervention from the end user is required. NICE DEMS case folders are automatically created through an integration with the agency's RMS. All data ingested into NICE DEMS will be automatically populated with the applicable metadata. NICE DEMS also supports the ability for other systems to integrate with NICE DEMS. The NICE DEMS API provides a set of pre-defined API calls to support sending and receiving (reading and writing) of digital evidence items and associated metadata. The API is available via a secure RESTful interface.
SE-8.3.28	Standardize Integration	The solution shall provide the ability to integrate with existing agency-owned case management and content management solutions. Proposer shall provide a list of currently supported standard Third-party integrations.	M	X				Case Creation - NICE DEMS Case folders are automatically created and assigned via integration with LVISAB's RMS. When a case is created and assignment in RMS, the RMS to investigate integration will trigger a case creation in Investigate and assigned to the appropriate detective. Folders are created for each case, and evidence items are located in their appropriate case folders. Case related metadata is associated with each case folder, and each evidence item has its own individual set of metadata. All case related information in RMS is shared via the integration so that all pertinent case details are accessible in Investigate. The integration keeps both platforms in sync with the most up to date information. Evidence Collection - Much of the evidence stored in Investigate is uploaded automatically via Investigate Integrations with existing agency-owned evidence data stores such as BWC video, 911 recording platforms, and CAD/RMS. Current Supported NICE Investigate Integrations: RMS NICHE RMS New World Intergraph RMS (Hexagon) Motorola Premier 1 RMS Northgate Connect RMS (API/WSDL) QED RMS EIS RMS iLeads CMS BEAST CMS Justware CMS LINX CMS JANO CMS CDI CMS (WIP) CAD Sopra/Steria STORM New World CAD Hexagon CAD (Intergraph) TriTech Total Command CAD TriTech Inform CAD Motorola Premier 1 CAD Capita Controlworks QED CAD SAAB CAD Tyler New World CAD Hexagon OnCall CAD (WIP) BWV Reveal Media BWV via DB Motorola Edesix B-CAM Getac BWV L3 BWV & in Car Video System Axon BWV via API (WIP) Voice recording NICE Inform Redbox Higher Ground Liberty Evenlide Digital Interview Room Recording David Horn (single stream / multi-stream) Indico Capita EvidenceWorks IRR iRecord

Req. ID	Level 1 Capability	Requirement	CSB Priority	Proposer's Response				Comments or Page and Section number in the proposal where additional information can be found.
				Y	N	C	T	

Comments column content:

Liberty via DB
Media Store/Crime Scene Photos/Mobile Photos, Forensics
Fotoware via API
ODIMS media store
Motorola PRONTO (via Fotoware)
Longarm via Folder watcher
Voice recording
Authentication/User Imports
Azure Active Directory
ADFS
NICHE Users
Motorola Premier One RMS User
In Car Recording
Cleartone
L3 BWV & in Car Video System

NICE offers a dedicated team of NICE DEMS integration experts who focus on connecting NICE DEMS to other data sources and applications. Integrating with Santa Barbara County existing case management and content management solutions is an integral part of the overall NICE DEMS solution that is being proposed.

Technical Requirements Overview

INTRODUCTION:

Technical requirements provide the criteria that will be used to assess the technical aspects of the DEMS, rather than specific business functional behaviors. The County requires the proposed solution to meet the technical requirements listed in this Appendix.
The list below represents the categories of technical requirements included within this RFP.

Level 0 Capability	Definition	DEMS Overview	Additional Info
Accessibility	The Accessibility category represents the availability and approachability of the DEMS to all future users, regardless of their impairments, characteristics or disabilities.	DEMS shall provide the ability to address the needs of the expected Administrative, Operations and Development members of the County.	N/A
Auditability	The Auditability category represents the traceability of all actions completed in the DEMS.	DEMS shall maintain a log of all activities attempted or completed in the solution. The log shall document data elements including but not limited to the following: date, time, user identity, parameter created/modified/deleted, and the user's machine IP address for each activity that is executed. The information shall support security audits, application usage trends for internal and external stakeholders.	N/A
Service Level Availability and Response Times	The Service Level Availability and Response Times category represents the operational continuity of how quickly the solution can recover from both unplanned outages as well as solution downtime planned downtime related to installation of upgrades. The failure rate or unplanned outages relates to the reliability of the solution and measures how often it is acceptable for the solution to fail.	It is the objective of County that the DEMS be highly reliable and able to be configured to provide maximum uptime and availability to all systems and users that depend upon its services. Due to the nature of the County's business processes, a minimal failure rate is essential for some of the components to minimize a disruption in services. The proposed solution is expected to support a desired up-time availability of 99.99%. In addition, the solution shall be configured so as to avoid single points of failure, so that the failure of any individual hardware component would cause the system to be unavailable. The solution shall be installed and configured based on Proposer provided best-practices which shall be designed to conform to required response times as defined in "Additional Info". Any disruption to normal operations shall be resolved quickly to restore the solution to normal running condition. The table in "Additional Info" provides additional information related to the Service Level Availability (Planned Outages), Failure Rate, Operational Continuity, and Backup & Recovery of the DEMS solution.	**Anticipated Response Times:** **Availability and Reliability Requirement / Response Time** DEMS — <3 seconds Third party components and Web Services — <3 seconds DEMS Reporting Services — <3 seconds **Service Level Availability (SLA):** **Availability and Reliability Requirement / % of Availability / Downtime Per Year / Downtime Per Month / Downtime Per Week** DEMS — 99.99% — 0h 48m 0s — 4m — 1m Third party components and Web Services — 99.99% — 0h 48m 0s — 4m — 1m DEMS Reporting Services — 99.99% — 0h 48m 0s — 4m — 1m
Capacity Limits	The Capacity Limits category represents the workload that the DEMS is expected to process.	The four criteria addressed include: • **Network Connections** - The number of connections expected between internal/external agency systems and the solution's components. This includes the sub-systems handling message services and external data synchronization. • **Concurrent Users** - The number of individuals (regular users and administration) expected to utilize the solution and it is sub-systems concurrently. • **Digital Evidence Volumes and Size** - Represents the immediate Digital Evidence volume needs, but does not represent future and full system volume needs. The volume of real-time events expected to be processed per day is of high importance for the total impact on the solution's performance. Transaction volumes are based on the number of arrest, documents, case filings and other key workload average indicators that occurred over the past several years at the County. Content shall be retained, based on a number of factors. The amount of content per case shall vary widely both in size and number of artifacts. • **Prioritization of System Functions** - The ability to set and change the priority of system functions to ensure performance standards are met. The system administrator shall be able to set and change priority, by solution function types, to ensure performance standards are met. For example if the archiving process is set to run during a certain period but at the same time the solution is experiencing unexpected peak usage, the archiving process shall be given a lower priority or maybe delayed.	**Concurrent Network Connections:** **Est. Number of Concurrent Network Connections / Min / Max** Number of estimated concurrent network connections — 5 — 2500 **Concurrent Users:** **User Roles / # of Users** *Normal Operations* *Maximum Users* - Total Maximum Users — 790 - Maximum Concurrent Users (assuming 50% of total) — 370 - DEMS Administrators (assuming 5% of total) — 40 **Case/Event Type:** **Case/Event Type / Estimated Volume / year** - District Attorney Received — 15,000 - District Attorney Filed — 8,600 - Sheriff Filings — 17,306 - Public Defender Representations — 16,000

Category	Description	Requirement	
Configuration Management	The Configuration Management category represents the process of maintaining the consistency and reliability of the DEMS performance and attributes throughout its lifetime.	This section describes requirements related to definition and management of solution configuration options.	N/A
Security	The Security category represents the requirements related to how end user identity shall be determined and controlled within the system.	This section includes requirements related to authorization, information security, alerts, and privacy considerations. Authorization is the ability for the application to control the functionality that the System/User is authorized to access. For each role, access control rules shall be defined to restrict the user to the functions that they are authorized to perform. Security alerts and reports refer to the solution's ability to provide a sufficient level of notification and summarization of security policy violations and breaches.	N/A
Usability	The Usability category represents the degree of intuitiveness and ease of use of the DEMS.	The Usability requirement addresses: • User Interaction - How easy it is for the user to interact with DEMS to perform required transactions. • User Navigation - How easy it is for the user to navigate and find information with DEMS.	N/A
Supportability	The Supportability category represents the solution's ability to be easily modified and maintained to accommodate typical usage or change scenarios.	The DEMS shall provide flexibility in the configuration of built-in workflows and business rules. It is required to be scalable and adapt to future changes in the justice agencies landscape.	N/A
Data Management	The Data Management category represents the solution's ability to process and store all data elements and logical data groupings required to provide the requested functionality to address logical data groupings, data retention, and data dictionary.	The Data Management requirement addresses: • Data Retention - Requirement relates to the availability of the data needed to be kept per legal requirements and longer if desired. • Data Import and Export — Support the import and export of data from/to multiple data sources. • Data Dictionary – A centralized repository of information which includes the meaning of the data, relationships to other data, origin, usage, and format of information • Data Structure and Relationships - Data modeling is required to define and analyze data requirements as well as to present the structures and relationships proposed within the solution. • Data Conversion - Expand, correct, and/or migrate the current data from the existing system(s) into the new system.	N/A
Design Constraints and Environment	The Design Constraints & Environment category represents the constraints imposed on the solution by compliance to County standards.	Due to the complex nature of Criminal Justice agencies and processes, it is essential for the DEMS to operate under all County, State and Federal constraints and policies.	N/A
Mobility	The Mobility category represents the mobility constraints imposed on the DEMS by compliance to County standards.	The DEMS shall support all County-approved mobile operating systems and associated browsers.	N/A
Reports	The Reports category represents the reporting capability requirements for the DEMS by compliance to County standards.	The DEMS shall be in compliance with all County and Criminal Justice Agencies reporting standards and procedures.	N/A

Technical Requirements

Req. ID	Requirement	CSB Priority	Proposer's Response				Comments or Page and Section number in the proposal where additional information can be found.
			Y	N	C	T	
	Accessibility						
AC-2.3.1	The solution's interfaces supporting its Administration, Operations, and Development shall be accessible via a web browser.	M	x				The NICE DEMS Administrator Portal is accessible via a web browser
AC-2.3.2	The solution's interface shall be built to ADA Rehabilitation Act 508 - Electronic and Information Technology Accessibility Standards.	M	x				NICE DEMS is compliant with WCAG (Web Content Accessibility Guidelines)
	Auditability						
AU-3.3.1	The solution shall provide the ability to search the audit log information by user, date, time, or other defined set of parameters.	M	x				A comprehensive system audit log tracks all activity in NICE DEMS. NICE DEMS tracks activity and maintains a full chain of custody audit log on each evidence item. The audit also provides a log of all user and platform activity. Each audit entry includes information on who completed the action and when the action occurred, along with any additional details associated with the action. Search and filter tools are available to assist the user in viewing subsets of the audit log based on parameters such as user, date/time, activity recorded, etc.) Audit logs are read-only in NICE DEMS. System audit logs can only be accessed by a System Administrator who has the appropriate privileges. Audit logs associated with a particular digital asset are accessible via the NICE DEMS user interface. The user must have the appropriate privileges to access the audit logs.
AU-3.3.2	The solution shall provide the ability to maintain audit records as either: active or archived, based on the end user configurable settings.	M	x				The NICE DEMS solution supports the ability to configure an automated retention policy that can maintain audit records as either: active or archived, based on the end user configurable settings.
AU-3.3.3	The solution shall provide the ability to maintain an audit log of end-user activity information for technical troubleshooting, security reporting and problem identification purposes.	M	x				A comprehensive system audit log tracks all activity in NICE DEMS. NICE DEMS tracks activity and maintains a full chain of custody audit log on each evidence item. The audit also provides a log of all user and platform activity. Each audit entry includes information on who completed the action and when the action occurred, along with any additional details associated with the action. Search and filter tools are available to assist the user in viewing subsets of the audit log based on parameters such as user, date/time, activity recorded, etc.) Audit logs are read-only in NICE DEMS. System audit logs can only be accessed by a System Administrator who has the appropriate privileges. Audit logs associated with a particular digital asset are accessible via the NICE DEMS user interface. The user must have the appropriate privileges to access the audit logs. This is available via the NICE DEMS Maintenance Portal; this portal is used by the NICE Support team and is not accessible by the customer. This information is available to the customer system administrator to use as they see fit (technical troubleshooting, security reporting, problem identification). NICE DEMS solution is monitored by the NICE OP(NOC) technical support team where audit log information is obtained.
AU-3.3.4	The solution shall provide the ability to log the following actions and identify who and when the action occurred:						
AU-3.3.4.1	Authorization success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.2	Access success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.3	Service/Script/Sub process execution success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.4	Query success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.5	Database connection success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.6	Communication failure, (e.g., database connectivity, web service connectivity, FTP connectivity).	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.7	Service creation, enable, disable, modification, and deletion	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.8	Service connection authorization failure/success	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.9	Service connection failure/timeout/error	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.10	Access to a Service/User account, file, directory or another system resource success or failure	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.11	Successful and unsuccessful attempts to create a user account, file, directory or another system resource	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.12	Successful and unsuccessful attempts to change a user account, file, directory or another system	M	x				The NICE DEMS solution logs this action.
AU-3.3.4.13	Successful and unsuccessful attempts to delete a user account, file, directory or another system resource	M	x				The NICE DEMS solution logs this action.

ID	Description			Response
AU-3.3.4.15	Successful and unsuccessful attempts to change account passwords	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.16	Successful and unsuccessful attempts to access (read) the audit log file	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.17	Authorization success or failure	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.18	Validation success or failure	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.19	Routing success or failure	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.20	Message out of sequence error	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.21	Associate a Level (Informational, Warning, Error, Critical, Success, Failure) to logged events	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.22	Any modification of data	M	x	The NICE DEMS solution logs this action.
AU-3.3.4.23	Anytime the data was read	M	x	The NICE DEMS solution logs this action.
AU-3.3.5	The solution shall provide the ability to export and archive the event logs.	M	x	Audit logs are stored for a customer configurable amount of time. Microsoft Azure provides transparent resilience for storage and queues which form the core of the NICE DEMS infrastructure. All data is synchronously replicated across three different storage nodes within the same Azure datacenter. There are redundant copies of all audit logs within a data center and can be stored in archive. Audit logs filtered by any number of metadata tags such as date/time, user, user action, system action, etc., can be exported at any time in CSV format
AU-3.3.6	The solution shall provide the ability to protect the audit log information from tampering or unauthorized access.	M	x	Audit logs are read-only in NICE DEMS. System audit logs can only be accessed by a System Administrator who has the appropriate privileges. Audit logs associated with a particular digital asset are accessible via the NICE DEMS user interface. The user must have the appropriate privileges to access the audit logs.
AU-3.3.7	The solution shall provide the ability to backup and restore the audit log to/from archival storage.	M	x	Audit logs are stored for a customer configurable amount of time. Microsoft Azure provides transparent resilience for storage and queues which form the core of the NICE DEMS infrastructure. All data is synchronously replicated across three different storage nodes within the same Azure datacenter. There are redundant copies of all audit logs within a data center. Audit Logs are accessible via the NICE DEMS System Administrator Portal for users configured with the appropriate privileges.
AU-3.3.8	The solution shall provide the ability to support notifications based on user-defined event triggers (e.g., notification generated for unauthorized User ID access attempts exceeding a predefined number of attempts).	M	x	NICE DEMS users have the ability to set up personalized alerts and notifications for over 200 various types of DEMS activity. These notifications can be customized by turning them off/on, requesting an email only, requesting email and in-application notification, and forwarding the notification(s) to another user or group of users. Each users' notification settings are unique to that individual.
AU-3.3.9	The solution shall provide the ability to track solution uptime by issuing log entries indicating solution startup and shutdown times.	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.10	The solution shall provide the ability to track transaction response times.	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.11	The solution shall provide the ability to record the following field and data attributes for an audit log event:	M		
AU-3.3.11.1	Type of record	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.2	What data was changed (table and data attributes)	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.3	Action Taken (i.e., viewed, printed, created, edited, deleted)	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.4	Date and Time	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.5	Source (e.g., System name, Username, internal process/task, Event Trigger)	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.6	Data Record information including but not limited to record returned, records added, records updated, search criteria, search results, and related unstructured data	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.7	Event message Source / Destination	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.8	Event Code and Description	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.9	User provided audit message.	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.10	User-definable Log Message	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.11	User-definable Log level	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.12	Machine name	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.13	Domain	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.14	Application / Service / Module	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.11.15	Status (Success, Failure)	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal

ID	Requirement	Priority	Mark	Notes
AU-3.3.11.16	If query, identification of query / stored procedure and input parameters.	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.11.17	Routing Indicator	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.11.18	Machine IP Address / MAC Address	M	x	Tracked via NICE DEMS System Master Audit Log located in the NICE DEMS Administration Portal
AU-3.3.12	The solution shall provide the ability to maintain an audit log record for the following data exchange activities to support the accountability, reconstruction of events and problem identification:			
AU-3.3.12.1	Request received (message)	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.2	Request sent (message)	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.3	Request delivered (acknowledgement if guaranteed delivery)	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.4	Request not delivered	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.5	Request pending for replay	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.6	Request for replay failed	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.7	Response received	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.8	Response not received (asynchronous or synchronous)	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.9	Response sent	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.10	Response delivered	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.11	Receive acknowledgement	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.12.12	Sent acknowledgement	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.13	The solution shall provide the ability to record all access attempts, whether granted or denied, and write transactions completed by all users.	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14	The solution shall provide the ability to record the following attributes for each data exchange activity to provide the current status of a transaction:			
AU-3.3.14.1	Type of message based on the header or content (i.e. person, etc.)	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.2	Date and Time	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.3	User-definable audit message	M		Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.4	Source system or user name	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.5	Interface name	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.6	Message identifier	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.7	Transaction identifier	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.14.8	Audit message	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.15	The solution shall provide the ability to generate an audit alert when a suspected security breach occurs	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.16	The solution shall provide the ability to search the audit log information by user, date, time, or other defined set of parameters.	M	x	Tracked via NICE DEMS Maintenance Portal
AU-3.3.17	The solution shall provide the ability to protect audit information and audit tools from unauthorized access, creation, modification, and deletion.	M	x	NICE DEMS audit logs are secured in a password-protected database with no way for users to edit the logs.
Service Level Availability and Response Times				
SL-4.3.1	The solution shall be designed to avoid single points of failure.	D	x	NICE DEMS is designed to avoid single points of failure in that if in the unlikely event one component fails, the entire system will not be shut down. Users are able to continue accessing and using other component of the system while the failure is resolved.
SL-4.3.2	The solution shall provide the response times as defined in Table 2: Anticipated Response Times.	H	x	NICE DEMS provides an initial response time <3 seconds.

ID	Requirement	Priority	Mark	Response
				NICE is constantly monitoring, and tuning NICE DEMS, operating in the Azure Cloud, to ensure the reliable daily use for the Customer. NICE is also making routine and scheduled updates to ensure the Customer have both the solution availability of 99.9% and the key feature set for their users as per the contracted agreement.
				An appointed NICE Service Manager will be responsible for the working with the Customer at their regular service review meeting to discuss and plan any outages in line with the agreed Service levels. A monthly report will highlight performance against the agreed Service Levels and KPIs for the monthly period and commit to taking remedial actions to correct any exceptions. Additionally, the report will include a broad range of usage metrics which includes, but is not limited to, the amount of data uploaded, shared, edited and stored.
				The Service Reporting reviews will also typically include validating and reviewing feedback from the Customer Users and managing the prioritization and timelines for delivery of new releases, etc. The performance of NICE as a supplier shall be measured in accordance with the agreed SLAs. The reporting will include:
				Measurement Target Report/Presentation data Percentage of agreed downtime < 0.1% downtime - Quarterly
SL-4.3.3	The solution shall be designed to meet the Planned Outage requirements for DEMS defined in Table 3: Service Level Availability (SLA).	H	x	Measurement Target Report/Presentation of data Agreed full downtime windows - No more than 6 per annum. •No of times system is down as part of planned activity. - Quarterly Customer notified that system is back fully operational within 15 minutes - 98% By exception Time lost through agreed downtime - 8 hrs. •Total time lost per full down time window - By exception. Unplanned system downtime - 0 •No of times system is down and is not due to planned activity - By exception. Unplanned downtime, lost < 0.01% •Total time lost and report ** - By exception •The number of agreed full (entire system including sharing portal) down time windows is set as 6. As part of this, however, it is recognized that there may be times where it is appropriate that the customer, through agreement with NICE, may choose to go above this. ** Report should detail research root cause analysis, lessons learned and action taken to prevent a reoccurrence. The SLA level of 99.9 % uptime/availability results in the following periods of allowed downtime/unavailability: Planned Time o Weekly: 1m 29s o Monthly: 44m 49s o Yearly: 8h 45m 56s
SL-4.3.4	The solution shall be designed to meet the Planned Outage requirements for Third Party Components and Web Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above Major upgrades may take longer than the SLA specifies but are a planned activity after hours.
SL-4.3.5	The solution shall be designed to meet the Planned Outage requirements for DEMS Reporting Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above Major upgrades may take longer than the SLA specifies but are a planned activity after hours.
SL-4.3.6	The solution shall be designed to meet the Unplanned Outage requirements for DEMS defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.7	The solution shall be designed to meet the Unplanned Outage requirements for Third Party Components and Web Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.8	The solution shall be designed to meet the Unplanned Outage requirements for DEMS Reporting Services defined Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above Major upgrades may take longer than the SLA specifies but are a planned activity after hours.
SL-4.3.9	The solution shall be designed to meet the Operational Continuity requirements for DEMS defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.10	The solution shall be designed to meet the Operational Continuity requirements for Third Party Components and Web Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.11	The solution shall be designed to meet the Operational Continuity requirements for DEMS Reporting Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above

ID	Requirement	Priority		Response
SL-4.3.12	The solution shall provide the ability to track solution uptime and transaction response times for both pre-formatted and ad-hoc queries.	M	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.13	The solution shall be designed to meet the Backup and Recovery requirements for DEMS defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.14	The solution shall be designed to meet the Backup and Recovery requirements for Third Party Components and Web Services defined in Table 3. Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.15	The solution shall be designed to meet the Backup and Recovery requirements for DEMS Reporting Services defined in Table 3: Service Level Availability (SLA).	H	x	Please refer to specifics in the response covered in SL-4.3.3 above
SL-4.3.16	The solution interfaces shall be available for use 24 hours, 7 days a week excluding scheduled maintenance periods.	M	x	Tracked via NICE DEMS solution Maintenance Portal
SL-4.3.17	The solution shall not include any construct or condition that would prevent administrators from achieving Recovery Point Objective (RPO) of one (1) minute and Recovery Time Objective (RTO) of one (1) hour.	H	x	Current RPO objective is 1 minute Abd RTO is 4 hours or less. We continually work to improve these numbers to meet customer requirements.
Capacity Limits				
CL-5.3.1	The solution shall provide the ability to accommodate the forecasted number of network connections in Table 4: Concurrent Network Connections above while maintaining required operational performance levels.	H	x	The NICE DEMS solution will be designed to properly support the forecasted number of network connections in Table 4: Concurrent Network Connections above while maintaining required operational performance levels.
CL-5.3.2	The solution shall provide the ability to accommodate each of the estimated User counts in Table 5: Concurrent Users above while maintaining required operational performance levels.	H	x	NICE DEMS solution is scalable to provide unlimited number of concurrent users. (5-2500 concurrent users is readily supported)
CL-5.3.3	The Third Party Components and Web Services solution shall provide the ability to accommodate the forecasted number of users in the table above while maintaining required operational performance levels.	H	x	Please refer to response CL-5.3.2 above.
CL-5.3.4	The solutions shall provide the ability to manage solution process priorities including routine settings and how exception priorities can be controlled and managed.	H	x	Solution process priorities and settings are all managed by NICE Operations Support personnel as a part of the NICE DEMS SaaS offering.
CL-5.3.5	The solution shall provide periodic reporting of performance measures for System capacity, performance, and usage.	H	x	This information can be provided from the NICE DEMS Reporting Database Service
CL-5.3.6	The solution shall provide the ability to increase and decrease its capacity with only a comparable increase in resources, with no degradation in performance, and with no change to system code required.	M	x	
CL-5.3.7	The solution shall provide the ability to accommodate the volumes specified in the table on Technical Requirement Overview Tab.	H	x	NICE DEMS solution is scalable as needed. NICE DEMS solution is scalable to accommodate and manage Santa Barbara County estimated case/event volume.
Configuration Management				
CM-6.3.1	The solution shall provide the ability to clearly identify or separate configuration settings which are specific to an individual environment so as to simplify the management and migration of these configuration settings from environment to environment (e.g., test vs. production).	M	x	NICE DEMS does not traditionally provide pre-implementation test systems and therefore has no need to migrate configuration settings from a test to production environment. However, during implementation, NICE and County will have the ability to clearly identify and separate configuration settings which are specific to their individuals. This is typically done by mimicking current access controls that exist in the County's Active Directory Federation Services. There are a set of system-wide configurations that will be established during the implementation phase which the administrators of NICE DEMS, only will be able to modify. Individual Users will be able to make a few small configurations (notifications, filters, keywords, etc.).

ID	Requirement			Response
CM-6.3.2	The solution shall provide the ability to use configuration variables as placeholders for configuration settings to support application deployment automation.	M	x	Please refer to specifics in the response covered in CM-6.3.1 response above
CM-6.3.3	The solution provide the ability to be configured and re-configured (through tools that do not require "code" modifications).	M	x	The NICE DEMS Administrator Portal allows for system, security, and DSG configuration without having to modify existing system code.
CM-6.3.4	The solution screens shall be highly re-configurable, providing ability to reposition and rename field labels, remove or "turn-off" unused fields, maintain data, and allow addition of custom-defined fields.	M	x	The NICE DEMS Administrator Portal allows for an easy configuration of fields and settings for: Case/Evidence Fields -Request -Fields/Types -Message Templates -System/Security Settings -Linked Systems -DSG Management
CM-6.3.5	The solution shall provide the ability to create and/or modify business rules which determine the acceptance/correctness of data.	M	x	The NICE DEMS solution allows for precise configuration and modification of evidence ingestion based on business rules and protocols of individual agencies with evidence source systems.
CM-6.3.6	The solution configuration shall be performed using a graphical user interface	M	x	The NICE DEMS solution provides a GUI interface for both main DEMS and Administration portals.
CM-6.3.7	The solution shall continue to function reliably and remain secure when individual components are changed.	M	x	The NICE DEMS solution provides a fully functional system that remains live while software updates are executed. Software updates do not impact system configurations.
CM-6.3.8	The Proposer shall provide change control process with approval stages required to change a configuration item attributes.	M	x	System administrators will have the ability to change a variety of configurations on their own without the need for assistance from NICE. For anything more complicated or that requires a change to code, NICE will provide technical guidance and change control documentation along with approval stages required when a change to the system is requested.
CM-6.3.9	The Proposer should provide a running record of current module configurations and the history of changes in the form of a report.	M	x	NICE DEMS solution provides an audit log of the current module configurations and the history of changes. These reports are available for download in a form of CSV file.
CM-6.3.10	The Proposer shall maintain County system configurations as Proposer supplied updates are provided and/or applied.	M	x	The NICE DEMS solution provides a fully functional system that remains live while software updates are executed. Software updates do not impact system configurations.
CM-6.3.11	The Proposer shall conduct regression testing for existing County system configurations as Proposer supplied updates are made.	M	x	NICE DEMS support teams conduct regression testing during their scheduled (MOP) Maintenace Operation Procedures. All reports from MOPs are documented.
CM-6.3.12	The Proposer shall follow Information Technology Infrastructure Library (ITIL) Change Management Best Practices or equivalent. This includes the following but is not limited to: change management dashboard, request for change (RFC), RFC screening, change management review, minor change, change advisory board, change approved, regression testing, and detailed release notes.	D	x	NICE DEMS solution support teams follow ITIL and Change Management Best Practices.
	Security			
SE-7.3.1	The solution shall provide the ability to maintain records as either: active, removed from view (expunged), archived, or purged (but must reflect County retention rules for query and reporting).	M	x	NICE DEMS can automatically manage evidence retention based on predefined rules. Retention rules can be set based on any metadata characteristic or a combination of characteristics of an evidence item. Once the retention rules are defined and updated in NICE DEMS, all evidence, upon upload into the system is assigned a retention category. Storage of an evidence item is then managed based on the assigned retention category and an appropriate deletion date is set. When a retention date is nearing, an evidence item will be marked as appropriate for deletion / to be expunged, archived, or purged. Reviews and approvals for deletion can be included as a part of any retention policy set in NICE DEMS. Prior to the deletion of an evidence item, a retention policy can be configured to send a deletion approval notice to a designated user who then has the ability to review and approve the deletion or extend the retention period of the evidence item as needed. The evidence item will only be deleted when the approval is provided.
SE-7.3.2	The solution shall provide the ability to log end-user activity information for audit, investigative, technical troubleshooting and problem identification purposes. The activity information collected should include but not be limited to records viewed, modified, and deleted.	M	x	A system-wide audit log is available in the NICE DEMS Administrator Portal. All activity in NICE DEMS is tracked and logged. This includes platform-generated activity, user-generated activity, and system administration activity. Each audit log entry details what action was performed, who performed the action, when it was performed, and any additional details on the associated digital evidence item.

ID	Requirement	Priority		Response
SE-7.3.3	The solution shall provide controls for access to data and solution functionality based on groups, roles, and permission levels.	M	x	NICE DEMS implements an attribute based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know". The control of access rights are established in Investigate via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role. It is also possible to create a connection to synchronize and inherit access control rules with a customer's existing records management system as a custom integration. The NICE DEMS System Administrator is responsible for working with the NICE system engineer to implement access rules for users. The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in NICE DEMS.
SE-7.3.4	The solution shall provide the ability to define system administrative security separate from content security access.	M	x	NICE will require one or multiple individuals at the County to be established as System Administrators. That individual(s) will have higher security clearances within the system including the ability to access the administration portal and configure access controls. This security access will be different and separate from an individual user who has content only access.
SE-7.3.5	The solution shall provide multiple levels of security access to folders and documents including: view and edit, view and annotate, view only, and no view.	M	x	NICE DEMS access privileges can be set up to have access to certain platform functionality such as view/edit/annotate/share/edit metadata/etc. per individual or per user role
SE-7.3.6	The solution shall provide the ability to limit the display of search results for users applied security rights and roles.	M	x	If a user does not have permission to view an item that is returned as a result of a search query, the NICE DEMS UI will block the user access to the evidence item and will provide information so that the user can contact the owner of the evidence item to request access. Access to the item can be granted by the owner.
SE-7.3.7	The solution shall provide Security and Authorization capabilities by connecting to Microsoft Azure Active Directory system using SAML 2.0 to allow for user access to be controlled through County processing.	M	x	NICE DEMS supports using your agency's ADFS SSO, or Active Directory Federation Services Single Sign-on, for end user access and authentication.
SE-7.3.8	The solution shall include all documentation necessary to complete tasks required to implement Security and Authorization for access and control of the solution.	H	x	NICE DEMS support teams will provide all necessary technical and support documentation to the end user.
SE-7.3.9	The solution shall include all documentation to support implementing access controls that comply with the relevant Federal and California State Security and Privacy policies.	H	x	NICE DEMS support teams will provide all necessary technical and support documentation to the end user.
SE-7.3.10	The solution shall support encryption and integrity checking of data in transmission and at rest (e.g., HTTPS / SSL / TLS), in compliance with NIST standards.	M	x	NICE DEMS adheres to CJIS/NIST established encryption requirements for data at transit and at rest, as well as including CJI in communications
SE-7.3.11	The solution shall support access to data via API	M	x	NICE DEMS solution provides access to data over the HTTPS protocol, with end users connecting via their Web Browser, and the Data Source Gateway (DSG) connecting to Web APIs which ingest data to make it available. The NICE Data Source Gateway is a software application service installed on the customer site, usually on a virtual machine.
SE-7.3.12	The solution shall provide auditability functions that shall comply with FBI CJIS Security Policy version 5.9.2 or later.	M	x	NICE DEMS solution adheres to and surpasses all 13 key areas of CJIS Policy FBI's Criminal Justices Information Services (CJIS) Policy covers 13 key areas which cloud service providers must address: 1) Information Exchange Agreements; 2) Security Awareness Training; 3) Incident Response; 4) Auditing and Accountability; 5) Access Control; 6) Identification and Authentication; 7) Configuration Management; 8) Media Protection; 9) Physical Protection; 10) Systems and Communications Protection and Information Integrity; 11) Formal Audits; 12) Personnel Security; and 13) Mobile Devices. The purpose of FBI CJIS security policies is to establish minimum security requirements to protect and secure various types of FBI Criminal Justice Information. NICE has earned the CJIS ACE Compliance Seal from Diverse Computing for NICE DEMSin 2016, following a rigorous 553-point review of the solution. NICE has recently begun the process of becoming re-certified for 2023 and future years as CJIS policies continue to evolve. Please refer to the enclosed white paper on NICE DEMS security for further detail.
SE-7.3.13	The solution must meet compliance standards of CJIS, HIPAA, FedRAMP, DoD, and NIST	M	x	The solution is hosted in Microsoft Azure Government cloud which is in compliance with applicable CJIS, HIPAA, FedRAMP, DoD and NIST standards. NICE is also compliant with the ISO27001 standard and is in the processes of obtaining the SOC2 Type II attestation report covering security, availability and confidentiality of the solution, scheduled to be completed by the end of 2023.
SE-7.3.14	Proposer must include a traceability matrix that identifies how the solution meets each requirement The solution shall remain compliant with the FBI CJIS Security Policy throughout the performance of this contract by applying changes and enhancements to the solution.	M	x	NICE will co-operate where required with mandatory CJIS audits in order to confirm its compliance in these policy areas applying changes and enhancements when required.
SE-7.3.15	The solution shall remain compliant with NIST encryption standards, at a minimum, for data in use by the solution.	M	x	NICE DEMS ensures that all data in transit is encrypted using TLS 1.2 bit encryption (FIPS 140-2 standard).
SE-7.3.16	The solution shall remain compliant with NIST encryption standards, at a minimum, for data at rest in a backup.	M	x	NICE DEMS ensures that all data in transit is encrypted using TLS 1.2. bit encryption (FIPS 140-2 standard), adhering to (AES256 standard) and (NIST)

ID	Requirement	Priority			Response
SE-7.3.17	The solution shall provide the ability to comply with multi-factor authorization.	M	x		All users attempting to access NICE DEMS must have a valid user profile with a user name / password combination per FBI CJIS-compliant complex password enforcement rules. NICE DEMS also supports 2-factor authentication and single sign on by using your agency's ADFS SSO, or Active Directory Federation Services Single Sign-on, which already provides two-factor authentication), as the NICE DEMS login. Client-side certificates can be used with TLS to prove the identity of the client to the server. As a second level of authentication, the user using the device would have to enter a valid user credential and password.
SE-7.3.18	The solution shall provide the ability to comply with strong passwords.	M	x		NICE password policy requires passwords to have the following attributes: -A minimum of 8 characters in length -At least one numerical and one alphabetical character -At least one special character -Disallows recently used passwords (past three passwords) -Account lock out after so many failed attempts (number of attempts to be configured by system administrator) -Admin configured number of days required for password changes
SE-7.3.19	The solution shall have an authorization mechanism that restricts a login account for access after a number of unsuccessful attempts within a given time period.	M	x		NICE DEMS Administrator Portal offers the following customizable settings: -Automatically and temporarily lock a user out of his/her account following a pre-specified number of failed login attempts. -Configure restrictions on the number of attempts and associated time period at which restrictions shall be enacted. -Self-help web page for resetting locked accounts -Unique login and password identifier.
SE-7.3.20	The solution shall provide configurable functionality for the number of attempts and the associated time period at which the restriction shall be triggered.	M	x		Please refer to specifics in the response covered in SE-7.3.20 above
SE-7.3.21	The solution shall provide the ability to trigger account access restrictions due to repeated unsuccessful login attempts by locking the login account and requiring the intervention of either a system administrator or a self-help web-page to reset the account.	M	x		Please refer to specifics in the response covered in SE-7.3.20 above
SE-7.3.22	The solution shall provide the ability to associate each user with a unique login identifier and associate each user login identifier with a password.	M	x		Please refer to specifics in the response covered in SE-7.3.20 above
SE-7.3.23	The solution shall provide the ability to define a session timeout based on security group or role.	M	x		Session timeout parameters are set in the System Administration Portal
SE-7.3.24	The solution shall provide the ability to prevent further access to the system in a user session by initiating a session lock after a County-defined time period of inactivity or upon receiving session lock request from the user.	H	x		NICE DEMS supports the ability for the Customer to configure their settings so that a session lock is initiated after a County-defined time period of inactivity or upon receiving session lock request from the user.
SE-7.3.25	The solution shall provide the ability to define password security requirements by security group or role.	H		x	Currently security password rules are configured on a system-wide basis.
SE-7.3.26	The solution shall provide the ability to restrict passwords to be not from a dictionary word or proper name.	M	x		User authentication is via sync with Customer's existing Active Directory. For local NICE DEMs accounts, password parameters can be set in the System Administration Portal.
SE-7.3.27	The solution shall provide the ability to restrict passwords to not be identical to the previous ten (10) or more passwords for the account.	M	x		Configurable via NICE DEMS Administrator Portal
SE-7.3.28	The solution shall provide the ability to restrict passwords to be a minimum length specified in County Password policy and CJIS policy.	M	x		Configurable via NICE DEMS Administrator Portal
SE-7.3.29	The solution shall provide the ability to display to users a County defined system use notification or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	M	x		Configurable via NICE DEMS Administrator Portal
SE-7.3.30	The solution shall provide the ability to notify the user, upon successful logon / access to the system, of the date and time of the last logon / access.	M	x		Configurable via NICE DEMS Administrator Portal

SE-7.3.31	The solution shall provide the ability to prevent further access to the system in a locked user session until the user reactivates access using established authorization procedures.	M	x	Configurable via NICE DEMS Administrator Portal
SE-7.3.32	The solution shall provide the ability to prevent further access to the system in a locked user session until the user reactivates access using established authorization procedures.	M	x	Configurable via NICE DEMS Administrator Portal
SE-7.3.33	The solution shall provide the ability to define a session timeout based on security group or role.	M	x	Configurable via NICE DEMS Administrator Portal
SE-7.3.34	The solution shall provide the ability to comply with County Policies for End-user authorization including but not limited to the following: Groups, Locations (Geo-Blocking), Roles, etc.	M	x	NICE DEMS implements an attribute-based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know". The control of access rights are established in NICE DEMS via access rules workflows that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.
SE-7.3.35	The solution shall provide the ability to produce immediate security alert notifications upon detection of a security policy violation.	M	x	Configurable via NICE DEMS Administrator Portal
SE-7.3.36	The solution shall provide the ability to produce a report documenting all security related items in the system by selectable duration (shift, day, month, etc.).	M	x	This report is produced by NICE support personnel and provided to the customer
SE-7.3.37	The solution shall provide the ability to configure the distribution of security alert notifications.	M	x	NICE DEMS is provided as a SAAS offering. As such, all security alerts are handled by NICE Support personnel. Communication with the customer will occur based on agreed upon notification policies.
SE-7.3.38	The Vendor awarded this bid, the solution, and all subcontractors must adhere to the COSB local policies located at https://ca-santabarbaracounty.civicplus.pro/3326/Technology-Security-Policies	M	x	NICE adheres to an internal set of Corporate security policies aligned with ISO27001.
SE-7.3.39	The Vendor awarded this bid, the solution, and all subcontractors must adhere to cybersecurity best practices as defined by NIST 800-53 r4 (or more current as it is released), the baseline security best practices for the County.	M	x	The solution is hosted in Microsoft Azure Government cloud which is in compliance with applicable CJIS, HIPAA, FedRAMP, DoD and NIST standards. NICE is also compliant with the ISO27001 standard and is in the processes of obtaining the SOC2 Type II attestation report covering security, availability and confidentially of the solution, scheduled to be completed by the end of 2023.
SE-7.3.40	The Vendor awarded this bid, the solution and all subcontractors must adhere to cybersecurity best practices as defined by Criminal Justice Information Services (CJIS), the baseline for law enforcement.	M	x	Agreed. NICE has personnel responsible for reviewing CJIS updates and actioning needed process and product enhancement as required and regularly conduct 3rd party audits to ensure CJIS compliance.
SE-7.3.41	Installation must pass NIST and/or CJIS security assessment prior to final payment – all remediations to pass security assessments are at the contractor's expense.	M	x	NICE is already CJIS assessed and certified via an independent 3-party evaluator. Re-testing is currently in progress, addressing the most recent updates to the latest published version of the CJIS standards.
SE-7.3.42	The Vendor awarded this bid, the solution and all subcontractors must adhere to 48 CFR 52.204 Basic Safeguarding of Covered Contractor Information Systems	M	x	NICE agrees to adhere to this requirement if awarded the bid.
SE-7.3.43	The solution must have a disaster recovery plan. In the response, the Proposer shall provide the disaster recovery plan including the testing procedures and testing cadence, areas of the system most susceptible to failure or disaster that may result in downtime, recovery processes or steps to take in the event of a downtime event, and recommendations for the County on how to comprehensively and effectively mitigate the risk of a downtime event	M	x	DR and BCM detailed (internal to NICE) documentation was updated last year and associated testing was performed. Customer facing sample plan is enclosed. The NICE SaaS Solution is based upon Microsoft Azure Technologies and leverages their resilience features. Microsoft Azure provides transparent resilience for storage and queues which form the core of the NICE SaaS Solution infrastructure. All data is synchronously replicated across three different storage nodes within the same Azure datacenter. The NICE SaaS Solution specific code runs as multiple load balanced instances of each of the front and back-end services and is designed to handle short term connection outages with automated retry policies.
	Usability			

ID	Requirement	Priority		Response
US-8.3.1	The solution shall provide both online and electronic versions of training material, and have a learning curve equal to one day or less for regular user and three days or less for admin.	H	x	NICE DEMS Training shall provide end users and system administrators the expertise and product knowledge needed to acquire the skills required to undertake day-to-day activities using NICE DEMS. Training shall be delivered in the following formats: -Train-the-Trainer sessions led by NICE to enable successful delivery of classroom-based training for the NICE DEMS Solution. This shall cover key knowledge points to be transferred in the classroom, trainer demonstrations, student exercises, end of module review quizzes, and best approaches for delivery. -Self-guided online training modules for use as new users are added to the platform as well as refresher training for existing users -In application Help documentation to assist the user with specific functionality as needed -Scheduled Webinar updates facilitated by NICE to provide training on functionality associated with new software releases -Quarterly touchpoints between NICE and select end users to obtain feedback and ensure maximum utilization of the system and its capabilities
US-8.3.2	The Proposer shall provide both online and electronic versions of their user manuals to provide new users and trainees with the initial information they need to use the solution.	H	x	Please refer to specifics in the response covered in US-8.3.1 above
US-8.3.3	The Proposer shall provide updates to the user manuals for new users and trainees with the initial information they need to use the solution.	H	x	Please refer to specifics in the response covered in US-8.3.1 above
US-8.3.4	The Proposer shall provide on-site "train the trainer" training at a sufficient level to prepare County trainers to conduct end user training. County trainers shall pass a vendor proficiency exam from the on-site "train the trainer" prior to being certified as a trainer.	H	x	Please refer to specifics in the response covered in US-8.3.1 above
US-8.3.5	The Proposer shall provide on-site or web based training for future versions of solution.	H	x	Please refer to specifics in the response covered in US-8.3.1 above
US-8.3.6	The Proposer shall describe the ongoing training programs available for the proposed solution and related components.	H	x	Please refer to specifics in the response covered in US-8.3.1 above
US-8.3.7	The solution shall have a common vernacular, consistent graphical user interface, and workflow.	H	x	NICE DEMS solution provides a common vernacular, workflow, consistent and a reliable GUI.
US-8.3.8	The solution shall provide time stamps normalized with Coordinated Universal Time (UTC) but must be displayed to the user in their current time zone.	H	x	NICE DEMS solution adheres with UTC standards.
US-8.3.9	The solution shall provide the ability to get key information within three clicks from any screen.	H	x	NICE DEMS Solutions provides global quick links for easy access within the dashboard.
US-8.3.10	The solution shall provide the ability to navigate and perform all system functions with only a keyboard shortcuts and function keys.	H	x	NICE DEMS solution provides the ability to use keyboard shortcuts and function keys.
US-8.3.11	The solution shall provide the ability to use the TAB key to move between fields.	H	x	NICE DEMS solution allows for use of TAB key within the NICE Application dashboard
	The solution shall provide the ability for users to access system features and functionality through a custom/configurable dashboard.	H	x	NICE DEMS solution provides for a unlimited custom/configuration options for its application dashboards.
Supportability				
SU-9.3.1	The solution shall be configurable, based on assigned authorization levels, by County administrative and operations users.	M	x	NICE DEMS user rights/access privileges are based on a Policy-Based Access Control (PBAC) model. This model allows flexible rules to be created to configure security access for specific users and groups, based on their roles (e.g. homicide detective, etc.) and rights (owner of a case or contributor). Also referred to as Attribute Access Control, this feature of NICE DEMS allows administrators to also set up rules that control which material can be accessed by which users (compliant with NIST Special Publication 800-162). It also supports restricting platform functionality based on user roles and rights.
SU-9.3.2	The solution shall support changes to internal business processes or workflows via Graphical User Interface (GUI) configurations, without requiring change to system code.	M	x	This is the responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3	The solution shall provide the ability to apply administrative configurations including but not be limited to:			

ID	Description			Response
SU-9.3.3.1	• Provisioning Accounts (Service and User)	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.2	• Defining Roles	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.3	• Configuring Logging and Audit controls	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.4	• Configuring subsystem integration	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.5	• Securing accessibility to subsystems	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.6	• Creating service ports	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.7	• Provisioning Storage	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.8	• Defining service privileges	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.3.9	• Assigning network interfaces to services	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations
SU-9.3.4	The solution shall provide the ability to apply operations configuration including but not be limited to:			
SU-9.3.4.1	• Defining startup and shutdown procedures	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.4.2	• Monitoring services	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.4.3	• Configuring High-Availability Architectures	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.5	The solution shall provide the ability to apply database configurations including but not be limited to:			
SU-9.3.5.1	• Reporting	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.5.2	• Logging	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.5.3	• User Stores	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.5.4	• Security	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.5.5	• Defining Security Roles for databases	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.6	The solution shall provide the ability to preconfigure the layout of the interface components (e.g., inboxes, task lists, search-and-retrieval functions and image display).	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.7	The solution shall provide the ability for the layout of the interface components to be automatically determined by the user's profile or role.	M	x	The UI will automatically reflect available capabilities based on the role of the user. If a user does not have access to certain functionality, it will be greyed-out in the UI. The UI will also show when a user is not permitted access to certain evidence items.
SU-9.3.8	The solution shall support configurable user interfaces allowing for the selection and positioning of user interface components.	M	x	Certain parts of the NICE DEMS UI can be configured to show desired metadata fields in various views in the user interface. We will work with the customer to identify what additional UI elements require the ability for UI configuration and provide the agreed to capability within 12 months.
SU-9.3.10	The solution shall provide troubleshooting and support documentation so that the County can effectively maintain and operate the system without direct vendor support.	M	x	The NICE DEMS solution includes a System Administration Portal that provides tools for the customer to manage User and System Configuration parameters without the need for direct vendor support.
SU-9.3.11	The solution shall include documentation defining the functionality of modules that comprise the solution that are available for assignment of access rights by role or group.	M	x	The documentation will be provided and reviewed with the customer. However, all access rights policies are configured and implemented by NICE Support personnel.
SU-9.3.12	The solution shall provide the ability to generate reports listing the roles or groups who have been granted access rights to available functions.	M	x	The NICE DEMS configured Access Control Policy details the access rights and privileges associated with user groups and roles. An Access Control Policy report can be generated as required.
SU-9.3.13	The solution shall provide the ability to restrict the use of maintenance tools to authorized personnel only.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.14	The solution shall provide certified test tools and scripts to verify solution stability and functionality.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.15	The solution shall provide the ability to receive third party updates (e.g., Windows Updates, Database Updates) without modifying the Proposer application's configuration.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.16	The solution shall provide the ability to ensure data integrity and quality control through concurrency mechanisms such as pessimistic or optimistic data locking.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.

ID	Requirement	Priority		Response
SU-9.3.17	The solution shall provide the ability to present an English text description of both the error and the suggested course of action to correct the problem, in the event of an error condition.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.18	The solution shall provide the ability to record errors encountered in batch processes and in online transactions. These records must be accessible to system administrators for analysis.	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations.
SU-9.3.19	The solution shall be updated regularly to support new file formats as industry standards change	M	x	Responsibility of the NICE DEMS Service Support team. The customer system administrator is not involved in these Administrative configurations. NICE typically perform 2 to 3 upgrades per year (major/minor). Sample release note is attached and sample notification is provided below.
	The solution shall provide advanced notice prior to any updates or patch application.		x	"Hello [name/s]: I would like to schedule your agency's upgrade to NICE Investigate (NICE Justice) R2.1 release. R2.1 comes with several feature enhancements that I know you are all keen to see, such as the new table view (your step towards virtual folders), configurable blocking of sharing based on field values that can be configured, improved video redaction, to name but a few.
SU-9.3.20	In the response, the Proposer shall provide information on the patch window, patch frequency, release notes sample, patch notification window, and a what the sample patch communication will look like.	M	x	Please see the latest Release Notes attached for more information on the above. I have worked out an optimum delivery schedule and ask that you approve the proposed upgrade dates for you, as follows:- Thursday 13th July, xx hrs. We will be seeking a 4 hour change window, although NICE DEMS (NICE Justice) should be back up and running in much less time. The system's sharing portal will be unavailable for the duration of the upgrade. I look forwards to hearing from you soon. Many thanks, [signature]"
SU-9.3.21	The solution shall support automatic uncompression of compressed files after they upload.	H	x	NICE DEMS solution supports automatic uncompression of compressed files after their upload.
SU-9.3.22	The solution shall support automatic compression of files as part of the download process.	H	x	NICE DEMS solution supports automatic uncompression of compressed files as part of the download process.
SU-9.3.23	The solution shall provide the option for the user to request that currently unsupported file formats become supported	M	x	NICE DEMS will transcode any new file formats that the customer requests. NICE currently can transcode over 95% of the known file types, including proprietary video.
Data Management				
DM-10.3.1	The solution shall provide the ability for administrative users to manage multiple different data retention policies based on business rules and data sources.	M	x	Data retention policies are configured and implemented by the NICE DEMS Technical Operations team per the requirements of the customer and can be based on business rules and data sources.
DM-10.3.2	The solution shall provide separate instance of digital evidence storage for each agency	M	x	NICE DEMS uses Microsoft Azure Storage and always stores multiple copies of agency data in order to protect it from the impact of planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Microsoft Azure offers multiple resilience models. NICE DEMS will work with you to assess the suitability of each option for your needs. Notably, all options have very high durability of objects (a minimum of 11 9's) over a given year.
DM-10.3.3	The solution shall provide the ability to retain data for unlimited periods of time.	M	x	NICE will work with Santa Barbara to identify which evidence data needs to be retained in archive storage for unlimited periods of time.
DM-10.3.4	The solution shall provide the ability for administrative users to manage the logical data groupings to be automatically archived and the archival retention duration for those groups based on business rules.	M	x	As part of the NICE DEMS SaaS offering, NICE Operations personnel are able to manage logical data groupings to be automatically archived and the archival retention duration based on business rules.
DM-10.3.5	The solution shall provide the ability, with authorization, to manually control and override rules related to archiving specific data items.	H	x	NICE DEMS has a built-in workflow that provides the ability for a user with the proper assigned role to manually control and override rules related to archiving specific data items.
DM-10.3.6	The solution shall provide the ability for administrative users to manage the logical data groupings to be in purged/sealed storage and the duration of the retention based on business rules.	M	x	As part of the NICE DEMS SaaS offering, NICE Operations personnel are able to manage logical data groupings to be automatically in purged/sealed storage and the duration based on business rules.
DM-10.3.7	The solution shall provide the ability for administrative users to retrieve or restore archived data, at will, over a period of time as per legal requirements.	H	x	Users with the proper assigned privileges can request retrieval of Archived data when needed.

ID	Requirement	Priority			Response
DM-10.3.8	The solution shall provide the ability to prioritize solution tasks including the archiving process to have a lower priority to ensure that it does not affect system performance during peak periods.	H	x		NICE Operations Support personnel have the ability to prioritize solution tasks including the archiving process to have a lower priority to ensure that it does not affect system performance during peak periods.
DM-10.3.9	The solution shall include a catalog of data specifications (data dictionary) that are available for import and export from / to the solution.	P	x		A data dictionary will be provided if required. However, as this is a SaaS offering, a data dictionary is not usually made available.
DM-10.3.10	The solution shall provide the ability to import and export meta data.	M	x		NICE DEMS provides for import/export of evidence metadata.
DM-10.3.11	The solution must provide the ability to configure the specific meta data that is imported/exported.	H	x		NICE DEMS solution allows for Admin users to select which evidence metadata is to be exported.
DM-10.3.12	The solution shall include a searchable, comprehensive data dictionary covering all data elements in all databases supporting the solution.	H	x		NICE DEMS solution provides comprehensive help page with easily searchable fields.
DM-10.3.13	The solution shall include documentation of the database schema including entity relationship diagrams or data structure diagrams; descriptions of the specific data elements that belong to each data structure; and a description of each data structure and the relationship to other data structures.	P		x	NICE DEMS database schema is typically not provided as this solution is a SaaS offering and customers have no direct access to the database.
DM-10.3.14	The solution shall provide the ability to update the data dictionary, either manually or automatically, as changes occur in the solution's databases.	H	x		This is handled by NICE DEMS R&D team as required for the SaaS offering.
DM-10.3.15	The Proposer shall accommodate routine changes, system updates, refinements, and additions to the data without causing any degradation in the performance and/or functionality of the system.	M	x		The NICE DEMS SaaS supports the ability to implement routine changes, system updates, refinements, and additions to the data without causing any degradation in the performance and/or functionality of the system.
DM-10.3.16	The Proposer shall identify the main data inputs and outputs of the proposed solution in both diagram and narrative format.	H	x		This is handled by NICE DEMS R&D team as required for the SaaS offering.
DM-10.3.17	The Proposer shall utilize existing Work In Progress data, contained in a variety of sources, to populate the new solution databases through automated export/import processes.	M	x		The NICE DEMS SaaS can utilize existing Work In Progress data, contained in a variety of sources, to populate the new solution databases through automated export/import processes
DM-10.3.18	The Proposer shall convert essential data identified by the County. Essential data elements required for the execution of the new solution which is missing or not available in current County databases shall be recorded manually or defaulted to County agreed to values.	M	x		As a part of the Solution Implementation process, all essential data identified by the County for the execution of the new solution will be converted to the NICE DEMS. Essential data elements which are missing or not available in current County databases shall be recorded manually or defaulted to County agreed to values.
DM-10.3.19	The Proposer shall identify and prevent duplicates from (	M	x		Each data elemented imported into the NICE DEMS has a key reference identifier. NICE DEMS checks for this key reference identifier upon ingest to prevent duplicates from being ingested.
DM-10.3.20	The Proposer shall ensure that the record integrity of the current data is protected, validated, and reliable for processing after conversion into the new system.	M	x		Upon ingest, the media is checked to ensure original hash is maintained, virus scan, make read only, working copy created. Subsequent edits are made on working copy. For redundancy - multiple copies of a data element are created in a single data center, with a full set of additional copies in a separate data center to protect against an entire data center failure.
DM-10.3.21	The solution shall include a process to identify, research, track and manually remove duplicates/potential duplicate data identified by matching key identifiers extracted from the source system.	M	x		Each data element imported into the NICE DEMS has a key reference identifier. NICE DEMS checks for this key reference identifier upon ingest to prevent duplicates from being ingested
DM-10.3.22	The Proposer shall use automated ETL tools to perform data conversion tasks.	M	x		NICE has an automated ETL process/tools as a part of the data transfer process. This is all provided as a part of the SaaS offering. No additional requirements needed by customer.
DM-10.3.23	The Proposer shall perform Work In Progress data conversion to the point where there is a predictable, successful outcome for each legacy system in sufficient time to validate, prior to system cut-over for go-live.	M	x		As a part of the Solution Implementation process, NICE Operations personnel will perform Work In Progress data conversion to the point where there is a predictable, successful outcome for each legacy system in sufficient time to validate, prior to system cut-over for go-live.
DM-10.3.24	The solution shall provide the ability to conduct full-text indexing for all digital evidence file types and formats, upon ingestion.	H	x		The NICE DEMS solution provides full-text indexing for all digital evidence file types and formats, upon ingestion.

ID	Requirement	Priority	Mark	Response
DM-10.3.25	The solution must have the ability for the County to recover all data. Proposer shall provide the data egress policy. (i.e. License deal ends)	M	x	The process of transferring data to the customer is covered under the contract and best-endeavor support will be provided to assist with this process at no extra cost. At the end of the contract the data will be transferred to the customer by transferring ownership of the Azure subscription. Once the subscription is transferred, the customer is responsible for all costs for the resources hosted within the subscription.
DM-10.3.26	The solution shall provide the ability to differentiate and store older data in cold tiered storage automatically.	H	x	The NICE DEMS solution supports the ability for the customer to define retention policy that will automatically move older data to a less expensive cold tiered storage.
DM-10.3.27	The solution shall provide the ability to export the content and associated metadata on demand, so as to preserve the association between the content and the metadata.	M	x	All content and associated metadata are linked in the NICE DEMS. This information is linked in the User Interface and can be easily viewed and exported together.
DM-10.3.28	The solution shall provide the ability to recover from a synchronization issue without loss of data or duplication of records.	M	x	The NICE DEMS Data Source Gateway is a software appliance that manages the import of data from external datasources. The DSG is designed to support full synchronization with external datasources and properly manage interruptions without loss of data or duplication of records.
Design Constraints and Environment				
DC-11.3.1	The solution shall support the use of data exchanges which conform with standards defined in the National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA), and LEXS for inter-communication between systems.	M	x	NICE DEMS utilizes data exchanges which conform with standards defined in the National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA), and LEXS for inter- communication between systems.
DC-11.3.2	The solution shall be a cloud based platform	M	x	NICE DEMS solution is a cloud-based Software-as-a-Service (SaaS), hosted within Microsoft's Azure cloud solution.
DC-11.3.3	The solution must be browser based and work on Windows clients using the following browsers: • Edge • Chrome • Firefox	M	x	NICE DEMS solution is accessible via Windows and MAC clients. Edge, Chrome and Firefox browsers can be used.
DC-11.3.4	The solution shall provide capability to connect to multiple identity providers and support SAML2.0	M		NICE DEMS can connect to multiple identity providers. We typically use OpenID connect but will support SAML, as needed.
DC-11.3.5	The solution shall provide ability to query data using third party reporting/analytics tools such as PowerBI and/or SSRS	D	x	NICE DEMS Stratus Reports Service provides the ability for third party reporting applications to create reports on the information held within NICE DEMS and other business applications. The design is based on an industry standard approach, making it natively compatible with existing market products, such as •Power BI •SSRS •Tableau •Zoho Analytics
DC-11.3.7	The solution shall provide or be compatible with operating system time synchronicity between all solution components.	H	x	NICE DEMS Solution implements bi-directional links between case management systems and other evidence source systems. Synchronization occurs in Real-time.
DC-11.3.8	The solution Application Program Interface (API) shall be fully documented with required and optional parameters, return types, side effects, and error or exception return types. The Proposer shall provide an API library, including the prerequisite software, that is needed or recommended in order to create interfaces which utilize the provided API for customization and integration with other systems.	M		All available NICE APIs are fully documented to support integrations with external systems that require data export from NICE DEMs.
DC-11.3.9	The Solution shall provide the ability to integrate with other external systems and databases through a standard API.	M	x	NICE DEMS solution can integrate external evidence source systems and pull databases with customized built API connectors.
DC-11.3.10	The Solution must be able to create evidence requests from law enforcement for specific files in disparate systems.	M	x	NICE DEMS solution can automatically or manually send requests to LE agencies for digital evidence.
DC-11.3.11	The Solution must provide the ability to track the status of the request sent to disparate systems.	M	x	NICE DEMS solution provides a notification feature that tracks the status of requests sent to evidence source systems.
DC-11.3.12	The solution shall provide the ability to schedule batch jobs in a flexible manner.	H	x	The NICE DEMS solution can schedule batch jobs in a flexible manner.
DC-11.3.13	The solution shall provide the ability to prioritize and sequence batch jobs.	H	x	The NICE DEMS solution can be set up to prioritize some batch jobs higher than others.

ID	Requirement				Response
DC-11.3.14	The solution shall provide the ability to rollback a batch job that has already completed.	H		x	Roll back of completed batch jobs is not supported at this time.
DC-11.3.15	The solution shall provide the ability to send notifications to designated users or roles upon failure of a batch job.	H	x		NICE DEMS Operations Support personnel are notified of any/all errors that may occur during batch file uploads.
DC-11.3.16	The solution shall provide the ability to restart a batch job which has stopped execution before completion.	H	x		NICE DEMS Operations Support personnel are able to restart batch jobs as required.
DC-11.3.17	The solution shall include instructions on how to recover in the event that a batch job has failed.	H	x		NICE DEMS Operations Support personnel have full documentation on procedures to follow in the event that a batch job fails.
DC-11.3.18	The solution shall ensure that appropriate access controls are applied to data based on the user requesting a report.	H	x		The NICE DEMS Access Control Policy is configured based on County specifications and will ensure appropriate access controls are applied to data based on the user requesting a report.
DC-11.3.19	The database management system on which the solution relies must provide atomic transactions	H	x		The NICE DEMS database management provides atomic transactions as required so as to prevent transactions with interfering with each other and ensure proper system behavior
DC-11.3.20	The database management system on which the solution relies must provide consistency, ensuring that any transaction shall bring the database from one valid state to another guaranteeing validity according to all rules (constraints, cascades, triggers or combination thereof).	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.21	The database management system on which the solution relies must provide isolation, ensuring that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially (one after another).	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.22	The database management system on which the solution relies must provide durability, ensuring that once a transaction has been committed it shall remain so, even in the event of hardware failure, power loss, crashes, or errors (in other words, transactions must be recorded in non-volatile memory).	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.23	The solution shall be implemented using at least, but not limited to, three (3) separate environments for development, test, and production.	D	x		The NICE DEMS SaaS Offering has separate development, test, and production environments.
DC-11.3.24	The solution shall provide an additional two (2) separate environments for staging and training.	D	x		There is a separate generic training environment which is good for early training overview sessions. However, we recommend that detailed training be done on the actual user environment to get the optimal training experience for end users.
DC-11.3.25	The Proposer shall use professionally and technically sound standards, techniques, and tools including, but not limited to:				Iso 27001; ISO 9001:
DC-11.3.26	Standards and techniques for controlling data synonyms, aliases, and versions.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.27	Standards for data characteristics.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.28	Data element design and domain standards for logical and physical data design, and standards for data management.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.29	Data design standards to ensure modularity, extensibility, flexibility, and efficient and consistent use of the data by the system.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.30	Standards for effective data searching and cross-referencing techniques.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.31	Standards to control data redundancy.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.32	Standards for data views, including internal, conceptual, and external views.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.33	Standards for data administration and database administration.	H	x		The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.34	Metrics, tests-of-correctness, and objective measurements of data quality.	H	x		The NICE DEMS support this so as to ensure proper system behavior.

ID	Requirement	Priority		Response
DC-11.3.35	Quality assurance inspection checkpoints within the system development life cycle.	H	x	The NICE DEMS support this so as to ensure proper system behavior.
DC-11.3.36	Formal software testing methodology.	H	x	The NICE DEMS support this so as to ensure proper system behavior.
Mobility				
MO-12.3.1	The solution shall provide the ability to support mobile browsers (e.g., Safari, Microsoft Edge, Chrome, Firefox).	H	x	NICE DEMS solution supports these mobile browsers: •Chrome mobile •Safari •Samsung Internet
MO-12.3.2	The solution shall provide the ability to support mobile operating systems (e.g., iPhone OS, Android OS).	M	x	NICE DEMS solution supports iPhone OS and Android OS mobile operating systems.
MO-12.3.3	The solution shall provide a mobile application for end user access	H	x	NICE DEMS solution offers the mobile application NICE Investigate Mobile to provide functionality targeted at officers out in the field with a mobile device. NICE Investigate Mobile provides a streamlined, intuitive and touch-optimized user experience with offline capability. NICE Investigate Mobile supports: • Viewing of 911 dispatches and associated media playback • Sending Business and Citizen requests for evidence • Directly collecting and uploading media evidence
Reports				
RE-13.3.1	The solution shall include predefined reports	H	x	NICE DEMS solution system audit Logs provide information on platform activity, this includes accessing a digital evidence folder, viewing digital evidence items, creating or modifying metadata, uploading, sharing, downloading digital evidence items, etc. This information provides management with insight into activity associated with open cases. Management can utilize this information to gauge overall effectiveness of the Investigative team.

NICE DEMS also logs all activity and information associated with Digital Evidence processing requests. The data logged can be used to determine if response targets are being met. An administrative user is able to query the System Audit Log and provide management information to report on adherence to SLAs.

Investigate records information on data stored in the cloud, including the number of digital assets, the types of digital assets, and the size of digital assets stored.

Investigate Audit information is accessible via the System Administration Portal for users with the appropriate privilege assigned. The user can find any subset of information using the search and filtering tools provided. The user can then export the data in a .CSV format to be imported to an external report generating platform.

NICE DEMS also has a maintenance portal that tracks network performance, storage capacity, and platform activity. Reports can be generated from this platform to share with management. We can discuss with Santa Barbara County on the types of reports required and will generate the reports and set rules for their distribution to identified personnel at agreed intervals.

With information collected in the NICE DEMS System Audit log and the NICE DEMS Maintenance Portal, NICE is able to provide Santa Barbara County with a range of management information linked to system use and performance and enable Santa Barbara County to generate needed reports. NICE DEMS also provides report views directly from within the Investigate interface.

Also, the NICE Stratus Reports Service provides the ability for third party reporting applications to create reports on the information held within NICE DEMS, and other business applications The design is based on an industry standard approach, making it natively compatible with existing market products, such as •Power BI •SSRS •Tableau •Zoho Analytics |
RE-13.3.2	The Provider shall supply a catalog of predefined reports that are supplied with the system, including description of output, sample output, and required and optional parameters.	H	x	Please reference RE-13.3.1 response above
RE-13.3.3	The Provider shall supply a catalog of data elements which can be included in reports.	H	x	Please reference RE-13.3.1 response above
RE-13.3.4	The Solution must be able to produce preconfigured and ad-hoc data reports and statistics.	H	x	Please reference RE-13.3.1 response above
RE-13.3.5	The solution shall ensure that appropriate access controls are applied to data elements based on the user requesting a report.	M	x	Please reference RE-13.3.1 response above
RE-13.3.6	The solution shall provide the ability to create user defined reports.	H	x	Please reference RE-13.3.1 response above

RE-13.3.7	The solution shall provide the ability to add user defined reports to the catalog of reports available for request.	H	x	Please reference RE-13.3.1 response above
RE-13.3.8	The solution shall provide the ability to schedule reports in a flexible manner.	H	x	Please reference RE-13.3.1 response above
RE-13.3.9	The solution shall provide the ability to distribute reports or send notification of report availability to end users.	H	x	Please reference RE-13.3.1 response above
RE-13.3.10	The solution shall provide performance reports that minimally indicate: · Average and peak response times by period; · Average and peak transaction throughput by period; · Error counts and rates by period.	M	x	NICE Support personnel will generate these reports and provide to customer at an agreed to interval.
RE-13.3.11	System must be able to provide insight into past data pa	H	x	Please reference RE-13.3.1 response above

Integrations

Stakeholder Agency/Department	Product	System Type	Description	URL to Product
Sheriff	DVMS, Command, Nexus	Safe Fleet/COBAN	In-Car and Body Camera Video management and archive systems. DVMS and Command are on Prem and Nexus is cloud storage	This integration provides body camera and in-car camera recordings (active and archived videos), as well as their associated metadata, to NICE DEMS. This will be a synchronized connection, updating in real time as information is updated in Safe Fleet/COBAN. Body camera and in-car recordings are matched to the NICE DEMS Case by leveraging the CAD incident ID or other identifying tags that can be used to programmatically establish attribution for the recordings. Note that customer assistance will be required to facilitate discussions with COBAN to provide NICE with required APIs and technical support to enable this integration.
Sheriff	Enterprise	Central Square	Criminal Records Management System (RMS) case management system for criminal, traffic and other law enforcement reports	This will be a direct integration to the CentralSquare RMS to provide RMS case information and incident details in NICE DEMS. It is a one-way integration, with NICE DEMS reading information from RMS. This will be a synchronized connection, updating in real time as information is updated in the RMS. The NICE Integration will provide: • The ability for the NICE DEMS SaaS Solution to create a digital case folder based on the creation of a case folder in Records Management. • The ability for NICE to extract key incident related information such as CAD incident ID, RMS case ID, incident type, status information, etc. and populate key information in NICE DEMS case folder. • The ability to locate Police reports and additional supplemental reports and add to NICE DEMS case folder. • The ability (if available via API or other mechanism) for NICE DEMS SaaS Solution to write back to Records Management the URL of the case folder once created; and • The ability to search all key information pulled from the Case management system from within the NICE DEMS SaaS Solution Note that County Sheriff's Office will need to assist NICE in obtaining technical support as needed.
Sheriff	ATIMS	ATIMS	Jail Record Management System (JMS) for inmate related data for all inmates from booking to release	This will be a direct integration to the ATIMS Jail management system to provide inmate information in the NICE DEMS SaaS Solution. This will be a synchronized connection, updating in real time as information is updated in the Incident management system.
Sheriff	Data Works Plus	Data Works Plus	Live Scan fingerprinting and mugshot systems, includes tattoo and facial recognition engines	If an API is provided for this system, NICE is able to build an integration. More information will be gathered during implementation phase. NICE also has a published API that will allow pushed information into this system, should this be a requirement of the County Sheriff.

Sheriff	Inform	Computer Aided Dispatch/911 system. Tracks 911 call data, routing of emergency services to and from incidents that come through our Public Safety Dispatch Center.	Central Square	This will be a direct integration to the CentralSquare Inform CAD to provide CAD incident information in NICE DEMS. It is a one-way integration, reading information from CAD. This will be a synchronized connection, updating in real time as information is updated in CAD. The NICE Integration will provide • The ability for NICE to extract key incident related information such as CAD incident ID, dispatched officers, incident type, etc. and populate key information in NICE DEMS case folder. • A CAD incident summary report generated from the available CAD information and included in NICE DEMS case folder. • The ability to search all key information in the CAD database from within NICE DEMS Note that County Sheriff's Office will need to assist NICE in obtaining technical support as needed.
Sheriff	911 call recorder	Records all 911 calls that come into the Public Safety Dispatch Center	AT&T	This integration provides the 911 call audio and meta-data to NICE DEMS. It is a read-only integration. County CAD Incident information is used to locate matching calls and place them in the associated NICE DEMS case folder.
Sheriff	Archived Criminal Records	Document Repository where completed case files are archived and stored	Laserfiche	This integration will support the collection of digital evidence that is currently stored in archived folders marked by case number on the County's Laserfiche archived records. The digital evidence will be placed into the appropriate NICE DEMS case folders based on the metadata provided in the naming of the folders and subfolders which identifies the related Prosecutor Case Management case. This will be a synchronized connection, updating in near real time as information is updated to the shared network drive folders. If this information is for historical cases, it will be added to those cases and sent to an archived state. Note that the County will need to assist NICE in obtaining technical support and folder structures as needed.
Sheriff	Inmate Phone System	Inmate phone system, records all inmate phone calls	GTL	This integration provides the GTL Inmate call audio and meta-data to NICE DEMS. County ATIMS and RMS case number (if available information) is used to locate matching calls and place in the associated NICE DEMS case folder.
Sheriff	Forensics Case Files	Digital evidence as related to photos, videos, documents, voice files etc.	Windows Files	This integration will support the collection of digital evidence that is currently stored in folders marked by case number on the County's Windows File system. The digital evidence will be placed into the appropriate NICE DEMS case folders based on the metadata provided in the naming of the folders and subfolders which identifies the related Prosecutor Case Management case. This will be a synchronized connection, updating in near real time as information is updated to the shared network drive folders. Note that the County will need to assist NICE in obtaining technical support and folder structures as needed.

Department	System	Vendor	System Description	Integration Description
Sheriff	Interview Recording System	iRecord	Interview recording system used by detectives when interviewing suspects and victims or other individuals related to a case.	This integration provides for the automated collection of Interview Room recordings tagged with case related metadata. The recordings are collected and placed into the appropriate NICE DEMS case folder based on case number identifier from the interview recording system. This will be a synchronized connection, updating in real time as information is updated in the Linear system. NICE does have a working relationship with iRecord already established as they are a partner company.
Sheriff	Custody DVR Systems	Misc.	Recording systems in our custody facilities	This integration provides available DVR videos and audio (if available) along with any meta-data to NICE DEMS. County ATIMS and RMS (if available information) case number will be used to locate matching recordings and place in the associated NICE DEMS case folder.
	eDefender	Journal Technologies Inc.	Content management system for case records	This will be a direct integration to the Case management (Journal Technologies) system to provide case information in the NICE DEMS SaaS Solution. If CMS allows, it is a two-way integration, reading information from the Case management system and writing back a URL to the NICE DEMS case (if API or other mechanism allows). This will be a synchronized connection, updating in real time as information is updated in the Case management system.

The NICE Integration will provide:
• The ability for the NICE DEMS SaaS Solution to create a digital case folder based on the creation of a case folder in Case Management.
• The ability for NICE to extract key case related information such as case ID, plaintiff and defendant details, case status information, related court assignments and details, etc. and populate key information in the NICE DEMS case folder.
• The ability (if available via API or other mechanism) for the NICE DEMS SaaS Solution to write back to Case Management the URL of the case folder once created; and
• The ability to search all key information pulled from the Case management system from within the NICE DEMS SaaS Solution
• Cases are able to go straight to archive if in a historical, closed state for retention. |
| Public Defender | | | | |
| Public Defender | Box.com | Box.com | cloud-based file storage and sharing solution that securely centralizes content. | This integration will support the collection of digital evidence that is currently stored in folders marked by case number on Box.com system. The digital evidence will be placed into the appropriate NICE DEMS case folders based on the metadata provided in the naming of the folders and subfolders which identifies the related Prosecutor Case Management case. This will be a synchronized connection, updating in near real time as information is updated to Box.com. Should the County decide to continue their use of Box.com, while it is not recommended, NICE is able to export to Box.com. Note that the County will need to assist NICE in obtaining technical support and folder structures as needed. |

District Attorney	Damion	Equivant	A case management system that facilitates processing LEA referrals from intake to case disposition.	This will be a direct integration to the Case management (Damion) system to provide case information in the NICE DEMS SaaS Solution. If the CMS allows, it is a two-way integration, reading information from the Case management system and writing back a URL to the NICE DEMS case (if API or other mechanism allows). This will be a synchronized connection, updating in real time as information is updated in the Case management system. The NICE Integration will provide: • The ability for the NICE DEMS SaaS Solution to create a digital case folder based on the creation of a case folder in Case Management. • The ability for NICE to extract key case related information such as case ID, plaintiff and defendant details, case status information, related court assignments and details, etc. and populate key information in the NICE DEMS case folder. • The ability (if available via API or other mechanism) for the NICE DEMS SaaS Solution to write back to Case Management the URL of the case folder once created; and • The ability to search all key information pulled from the Case management system from within the NICE DEMS SaaS Solution
District Attorney	eProsecutor	Journal Technologies Inc.	A case management system that facilitates processing LEA referrals from intake to case disposition.	This will be a direct integration to the Case management (Journal Technologies) system to provide case information in the NICE DEMS SaaS Solution. If the CMS allows, it is a two-way integration, reading information from the Case management system and writing back a URL to the NICE DEMS case (if API or other mechanism allows). This will be a synchronized connection, updating in real time as information is updated in the Case management system. The NICE Integration will provide: • The ability for the NICE DEMS SaaS Solution to create a digital case folder based on the creation of a case folder in Case Management. • The ability for NICE to extract key case related information such as case ID, plaintiff and defendant details, case status information, related court assignments and details, etc. and populate key information in the NICE DEMS case folder. • The ability (if available via API or other mechanism) for the NICE DEMS SaaS Solution to write back to Case Management the URL of the case folder once created; and • The ability to search all key information pulled from the Case management system from within the NICE DEMS SaaS Solution
District Attorney	CIDC MNI	SB County / Bruce Thomas	Internal name matching system across Law and Justice partner systems	More information is needed for this integration. In the event this system sets a standard for case name and syntax coordination, NICE is able to use this as a master file for case correlation.

Probation Department	Caseload Explorer (IMPACT)	AutoMon Inc	A web based case management system that is used to manage all adult and juvenile clients being investigated, held, or supervised by Probation.	This will be a direct integration to the Case management (Caseload Explorer (IMPACT)) system to provide case information in the NICE DEMS SaaS Solution. If the CMS allows, it is a two-way integration, reading information from the Case management system and writing back a URL to the NICE DEMS case (if API or other mechanism allows). This will be a synchronized connection, updating in real time as information is updated in the Case management system. More conversation will be required for this integration.

General Integration Statement:

NICE will make all of the above listed integrations available. NICE will index information from the connectors detailed in the sections below. Full

Attachment B to Statement of Work

a. **Subscription Term.**

1. Subscription Term. "Subscription Term" shall have the same meaning as "Term," as defined in Section 4 of this Agreement, above.

2. The Cloud Services are non-cancelable by COSB except as specifically set forth to the contrary under Section 19. Termination. If COSB elects to cease using the Cloud Services during the Subscription Term, COSB shall: (a) continue to be liable for all amounts payable under this Agreement for the remainder of the Subscription Term, including all amounts that are subject to a Minimum Commitment; and (b) not be entitled to any refunds.

3. Releases. New releases of the Cloud Services will be provided to COSB if and when they are generally commercially available. The fees for Professional Services required to implement or deploy a new release of the Cloud Services are included in the fees for the Cloud Services, except with respect to NICE Performance Management and NICE Sales Performance Management. Professional Services for any COSB-specific configurations will be at an additional cost.

4. NICE shall maintain one (1) Production environment of the Cloud Services to meet the service levels. NICE shall provide the necessary technical infrastructure and maintenance Services to deliver the Cloud Services.

5. **Availability**. NICE will maintain Availability of the applicable Cloud Services provided for in Section 1 above, as follows:

6. NICE will maintain Availability of the SaaS Solution in the Production environment as follows:

SaaS Solution	Service Levels for Availability	Hours of Applicability
NICE Investigate	99.9%	Extended Hours

    I.   *24X7/365 days

7. **COSB**   **Duties.**

COSB will appoint two (2) resources who have completed the NICE training in the operation and use of the Cloud Services ("**Designated Contact(s)**"), and shall act as NICE's primary point of contact regarding requests for technical assistance. The Designated Contact shall initiate a Support Case via the designated support channels provided in Table A-1 below. Prior to initiating a Support Case, the Designated Contact shall use reasonable efforts to attempt to diagnose and resolve the particular issue including using available self-help tools. The Designated Contacts are required to establish and maintain COSB's processes to provide first tier support for the Cloud Services, which includes: (a) a direct response to user inquiries concerning the performance, functionality, or operation of the Cloud Services; and (b) an attempt to diagnose and resolve problems or issues with the Cloud Services.

Table A-1	
Support Contacts	
For NICE WCX Solution Family	
http://wiser.nice.com	Recommended First Step
United States and Asia Pacific Region	+1 800-642-3611
Germany	+49 699 717 7114
United Kingdom	+44 0 148 977 1633
France	+33 141 38 5686

The Netherlands	+31 72 566 2222
All other locations	+972 9 775 3800

8. **Support Case**.

I. Support Cases are classified based upon the definitions outlined in Table A-2 below:

Severity Level	Definition	Examples
1. Critical (System Unavailable)*	Critical issue that severely impacts use of the SaaS Solution. II. No workaround.	A. The SaaS Solution is completely unavailable. B. The majority of users cannot login. C. Data integrity issues.
2. High (System Impaired)*	I. Major functionality is significantly impacted. II. No workaround.	A. Service interruptions to some but not all functionality. B. Alerts not being generated
3. Medium (Minor Impact)	Multiple users impacted by a moderate loss of the SaaS Solution. Critical or High impact on a non-Production SaaS Solution. III. A workaround exists.	A. Functional limitations which are not critical to COSB's daily operations (e.g. reports not being generated). B. Moderate degradation in function, or feature performance.
4. Low (Informational)	I. Minor loss of the SaaS Solution features. II. Inquiries III. Medium or Low impact on non-Production SaaS Solution.	There is no significant COSB impact. B. Non-Critical or minor loss of functionality or features.

*Reserved for the Production SaaS Solution only.

9. NICE's response to a Support Case will be handled, as follows:

Table A-3	
Support Case Severity	**Target Initial Response Times^**
S1	60 minutes
S2	4 hours during COSB's business day
S3	Next business day
S4	Next business day

^S1 times are based on 24x7x365, all other Support Case Severity levels are based on standard business hours, each as measured from the date of COSB's initial notification to NICE, as provided for in Section 5 of this Exhibit.

10. NICE shall use commercially reasonable efforts to perform maintenance Services on the SaaS Solution during the time frames provided in the table below ("**Maintenance Window(s)**").

Maintenance Windows Criticality	Advanced Notice	NICE Maintenance Windows (relevant data center time)
Standard	7 Days	Tuesday and Thursday 11:00 PM to 3:00 AM
Extended	30 Days	Sunday 2:00 AM to 10:00 AM
Emergency	Immediately following NICE's awareness of an issue.	Nightly 10:00 PM to midnight

12

Attachment C – Site Readiness Document
(Technical Description Document)

Contents

1 Introduction

This document serves two key purposes:

1. Provides relevant information to customers to support the comprehensive and timely preparation of their environments, processes and infrastructure ahead of the deployment of the NICE solution.

2. Records key items of information to be used by the NICE project team when configuring and preparing systems and environments. Information should be added to the relevant sections and the document returned to the NICE project team.

The document contains placeholders for NICE-supplied information which should be populated by a member of the NICE project team before providing to the customer. Any absent information should be sought from the NICE project team.

> NOTE: This document can potentially contain sensitive information such as IP addresses, usernames and passwords. Therefore, this document should be shared with NICE in a manner that is contingent with any required security policies.

1.1 *Readiness summary*

Several appendices are included in this document, each can hold information and confirmation that certain actions have been completed.

Appendix	Purpose
Appendix A – Authentication Readiness	Capture information for the linking of the NICE system to the customers Azure Active Directory and the different Active Directory Groups within
Appendix B – Network Readiness	Capture relevant IP address information for securing access to the NICE system by the customer's users
Appendix C – DSG Readiness	Capture information about the machines that the customer will setup to host the NICE Data Source Gateway software. This will be used to connect to data source endpoints and transfer metadata and media/files up to the NICE System
Appendix D..Z – Connector Readiness	Individual appendices for each connector that will be deployed by NICE to connect to the data source endpoints. The information captured will vary depending on the nature of the connector

2   Data Source Gateways (DSG)

This section details the requirements for installation of the NICE Investigate/Justice Data Source Gateway (DSG). The DSG is a Microsoft Windows service, installed and configured to collect data and media for NICE Investigate/Justice.

The DSG has "connectors" which correspond to an underlying data source (e.g. Records management system or CAD system). Machines used for hosting the DSG service are typically Virtual Machines.

Information related to the customer's DSG environment should be recorded in Appendix C.

2.1   Connector distribution

Number of connectors	Number of Machines Required
1-3	1
3-6	2
6-9	3

NOTE: Ranges are provided above as the connector distribution is based on varying factors. General recommendations are for connectors that will have high number or large size file throughput (e.g. body worn video) to be kept separate from similar connectors (e.g. DIR) and ideally on dedicated machines. The final decisions on DSG number and connector distribution are made in collaborative consultation between the customer and the NICE project team.

2.2   Machine specification

DSG machines should be commissioned to the following <u>minimum</u> requirements:

2.2.1   <u>Operating systems</u>

The following Operating Systems are supported:

Operating System
Windows Server 2016 (64 bit)
Windows Server 2019 (64 bit)
Windows Server 2022 (64 bit)

2.2.2   Machine specification

Item	Specification
CPU	4 cores or virtual cores @ 2Ghz
System RAM	16GB
HDD	200GB, 20GB free space
Network Interface	Ethernet TCP/IP: minimum speed 100 Mbps, 1Gbps recommended. configured as Full Duplex
.Net Framework	4.8 Runtime 6.0 Runtime

2.2.3   Machine permissions

The following permissions are required on the DSG machine for the DSG to operate:

2.2.3.1   Permission to access performance counters

The DSG reads statistics from the operating system performance counters to put in heartbeat messages to alert on low memory, CPU or disk space. The DSG service account needs to be added to the Performance Monitor Users.
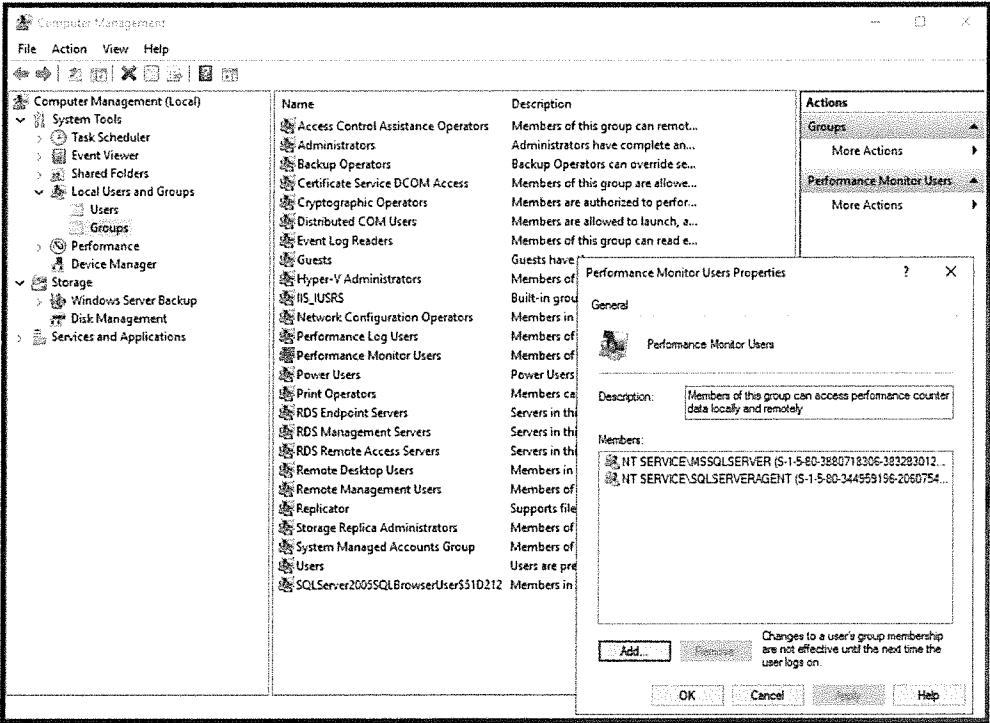
2.2.3.2 Registry permissions

The DSG writes a flag into the Registry on install to indicate the mode it needs to work in. Therefore, **the account used to install the DSG software** needs the requisite access for this. The DSG **service account** needs to be able to read the Registry.

2.3 Remote Access

NICE needs secure remote access to each DSG machine if they are to install, configure and troubleshoot the DSG software and configured connectors.

If applicable, ensure that remote access to the DSG machine is enabled and successful connection has been confirmed.

NICE will need to be made aware of the connection details and confirm successful connection.

2.3.1 User accounts

For DSG provisioning and administration, user accounts are required on the machine for support personnel. These accounts should have local administrator permissions to support administration of the service, run support tools, run provisioning tests and set up the configuration.

2.4 DSG Anti-Virus configuration

No specific anti-virus configuration is required for the DSG to run. The DSG uses a temporary folder for saving media files when they are being transferred to NICE Investigate/Justice, this should be removed from any virus scanning rules to prevent performance being affected

Path: **%LOCALAPPDATA%\Temp\DSG\.**

2.5 Outbound DSG Firewall policy

The NICE Data Source Gateway needs to access a number of Cloud-based endpoints (for each machine hosting a DSG). Ideally the Main Domain for the endpoint should be whitelisted to allow all requests to **evidencentral.com**

If the above Main Domain cannot be whitelisted, specific endpoints need to be opened for outbound connectivity:

NOTE: If <SiteName> is shown below, please contact the NICE project team to confirm which Site Name will be used for your implementation.

Endpoint	URL
DSG API	<SiteName>-**dsg-api**.<Main Domain>
DSG Blob Storage	<update prior to sending or request from NICE>

NOTE: **NICE recommends that URL naming is used for firewall configuration (as opposed to IP addresses). IP addresses can be provided for each named resource but IP addresses are not guaranteed to be static and may change**

NOTE: All URLs are via HTTPS using TLS 1.2 or higher

2.6 *Inbound DSG Firewall policy*

All communications between the DSG and Investigate/Justice are initiated by the DSG, therefore no inbound ports require opening.

2.7 *Access to Data Sources*

The DSG connects to third party servers to ingest data and media. For each DSG connection to a third-party system, access must be available across the method(s) required e.g. fileshare, database, API

2.7.1 Network access (LAN)

Ensure that the machine hosting the DSG can connect to all third-party data sources and all appropriate firewall ports are opened.

2.7.2 Login credentials

If required, ensure that any login credentials required for the DSG to access the third-party data sources are available and access with these credentials has been confirmed.

2.7.3 File share access

If required, ensure that the account the DSG service is running under can access any file shares that are required for third-party data sources.

3	**NICE Investigate/Justice Access**

This section covers the specific steps required to prepare the customer site for NICE Investigate/Justice environment access.

3.1   *Investigate/Justice Access restrictions*

3.1.1   IP Address Restrictions

By default, access to Investigate/Justice is restricted to the external IP addresses provided by the customer. This is the preferred method for restricting access to the Investigate/Justice Services. The IP addresses should be recorded in Appendix B in this document.

3.1.2   User Access Certificate

Access to NICE Investigate/Justice can be secured by client certificates (in addition to other access control mechanisms). Existing customer client certificates (user based) are supported however if required NICE can provide client certificates to be used.

Certificates can be rolled out to all users via the customers internal IT domain policy if required or installed manually on a per user basis.

3.2   *Access and permissions within the solution*

Individuals are granted (or denied) access to features and data using an Access Control Policy. Each logical grouping of permissions is represented as a "Role" or "Group" inside the NICE solution, and users can be members of mutiple Roles/Groups. Membership of a Role/Group is determined through a "mapping" of Active Directory Group Membership to NICE Role/Group membership. Multiple Active Directory Groups can (optionally) be mapped to a NICE Role/Group. The appropriate Active Directory Groups on the Customer's AD need to be identified (or created if not pre-existing) and the details provided to the NICE project team.

3.3   *User Authentication*

The solution supports connectivity to the customer's Active Directory for user authentication. Preferably this will be hosted in Azure (a.k.a. Azure Active Directory or AAD) but it may be locally hosted (a.k.a. Active Directory Federation Services or ADFS). If the solution needs to connect to ADFS, separate instructions will be provided by the NICE project team.

A number or URI's are required, provided by the NICE project team to be used in the configuration steps below:
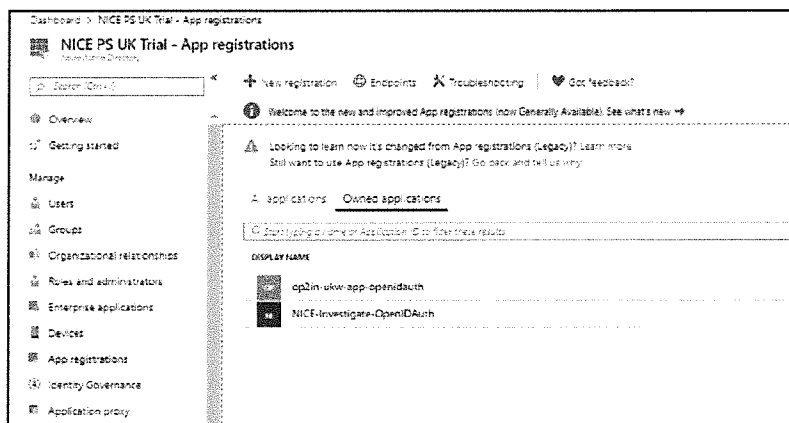
URI List

NOTE: Please contact the NICE project team if the above list is not populated

The following steps should be completed to register the NICE Application inside the customer's AAD.

3.3.1   Application Registration

> To register the application:

1. In the Azure Portal, under **Azure Active Directory**, navigate to **App Registrations** blade and click **New Registration**.

2. Complete the **Register an application** form, leaving the Redirect URI blank for now.

| NOTE: | Once the app is created, copy the Client ID to send to the NICE project team securely. |

3. Navigate to the **Authentication** blade of the new App Registration.

4. Click the **Add a platform** button, select **Web**,

5. Under **Implicit grant**, make sure the **ID tokens** box is checked.

6. Add all the redirect URIs supplied by the NICE project team, ensuring removal of any trailing '/' from those supplied, remembering to save changes.

7. In the resulting configuration section, enter the Logout URL supplied by by the NICE project team.
In the **Implicit grant and hybrid flows** section, ensure that the **ID tokens** box is checked and save changes.

8. Navigate to the Certificates and Secrets blade in the Azure Portal
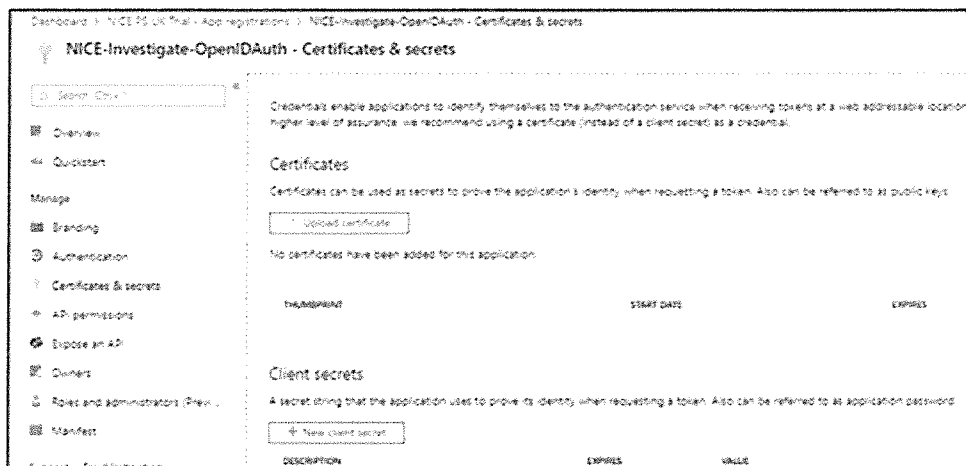
9. Create a **New client secret** and set/note the **Expiry Date**

NOTE:	NICE does not support using Certificates instead of Secrets.
NOTE:	Copy the **secret** to send to the NICE project team securely.

10. In the portal navigate to the **API Permissions** blade and the select **Add a permission**.

11. Select **Microsoft Graph** and then **Delegated Permissions**.

12. Search for **Group.Read.All**.

13. So that users do not have to give consent at sign in, ensure that the **Grant Admin consent** button under **Grant Consent** is clicked.
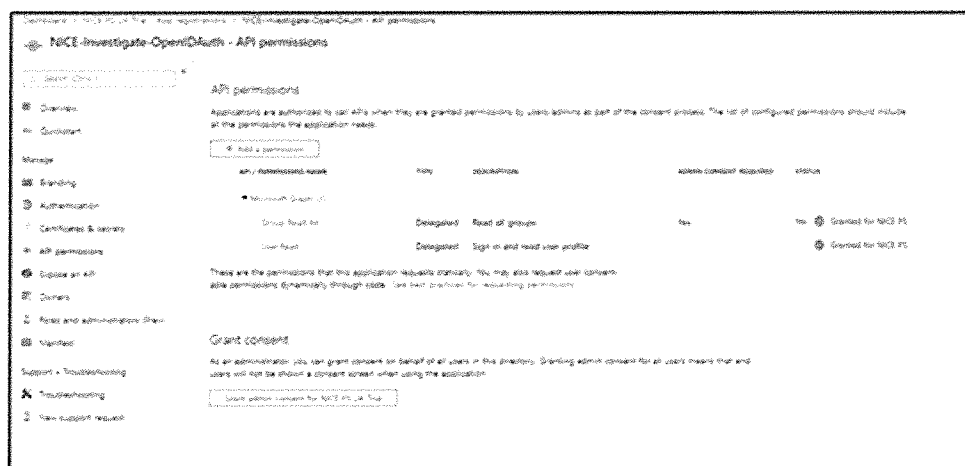
NOTE:	NICE recommends restricting access to the App Registration using a specific Azure AD security group. To apply this restriction, follow steps 14-20

14. In the portal navigate to the **Overview** blade and the **select the Managed application in local directory link in the Essentials section**.

15. Under **Manage**, select **Properties**

16. Locate the setting **User assignment required**? And set it to Yes

17. Under **Manage**, select the **Users and groups** and select **Add user/group**

18. Select the **Users and Groups** selector A list of users and security groups will be shown along with a textbox to search and locate a certain user or group. Use this screen to select the correct Azure AD security group.

19. Once the appropriate group is selected, choose **Select.**

20. Select **Assign**

3.3.2   Send information to NICE

21. Now that the Application has been created, send the following information securely to the NICE project team; Appendix A in this document can be used:

   – Application (client) ID

   – Client Secret (send as securely as needed)

   – Client Secret Expiry Date

   – Directory (tenant) ID

   – Object ID of each Azure AD Group used for NICE Investigate/Justice

   – A mapping of Azure AD group to NICE Investigate/Justice group/role

NOTE:	The Expiry of the Client Secret will be noted by NICE and recorded, however, update of the secret and provision of the new value, in good time before expiry, is the responsibility of the Customer

3.3.3   Investigate/Justice Authentication

Authentication via the customer's Azure-based Active Directory is the preferred mechanism. However, where this cannot be achieved immediately or AD integration is not possible, user authentication can be managed within Investigate/Justice via local logins and users can securely reset their passwords from login page.
Access control can either be automated using automated rules or can be managed from the Investigate/Justice Admin Portal where roles can be manually applied to grant access permissions.

3.4   Customer Network Configuration

3.4.1   Outbound Customer Firewall Rules

NICE Investigate/Justice, and other portals, are all accessed on the **evidencentral.com** domain. Ideally, this domain should be whitelisted to allow all requests to the domain.

If the domain itself cannot be whitelisted, then access would need to be enabled for a number of specific application endpoints within the product suite:

Product	Information
Global Whitelist (Main Domain)	evidencentral.com
NICE Investigate/Justice **Note: if \<SiteName\> is shown opposite, please contact NICE to confirm which Site Name will be used for your implementation**	\<SiteName\>-**admin**.\<Main Domain\> \<SiteName\>-**download**.\<Main Domain\> \<SiteName\>-**dsg-api**.\<Main Domain\> \<SiteName\>-**investigate**.\<Main Domain\> \<SiteName\>-**invfus-upload**.\<Main Domain\> \<SiteName\>-**login**.\<Main Domain\> \<SiteName\>-**mobile**.\<Main Domain\> \<SiteName\>-**mobileapi**.\<Main Domain\> \<SiteName\>-**sharing**.\<Main Domain\> \<SiteName\>-**upload**.\<Main Domain\>

NOTE: **NICE recommends that URL naming is used for firewall configuration (as opposed to IP addresses). IP addresses can be provided for each named resource but IP addresses are not guaranteed to be static and may change**

NOTE: All URLs are via HTTPS using TLS 1.2 or higher

3.4.2 Outbound Internet traffic filtering

Any Websense, or equivalent, policy needs to be relaxed to allow all web site assets from the **evidencentral.com** domain to be downloaded. If relaxation for the whole domain is not possible, then specific rules need to be relaxed to allow all the assets to be downloaded. E.g. assets with names such as "email", "upload", "share" and "download".

3.4.3 Inbound Customer Firewall Rules

By default, Investigate/Justice does not require ports to be opened in the customer firewall to allow it to talk to the customers site.
If ADFS is configured Investigate/Justice may need to contact the ADFS endpoint.

3.5 Browser Support

The various NICE Portals are supported on the following browsers:

Portal	Supported Browsers
Investigate/Justice Portal	Google Chrome, Microsoft Edge
Administration Portal	Google Chrome, Microsoft Edge
Mobile Portal	Google Chrome, Microsoft Edge, Safari, Samsung Internet (intended for use on Mobile devices only)
Download Portal	Mobile Devices – Google Chrome, Microsoft Edge, Safari, Samsung Internet Desktop Devices – Google Chrome, Microsoft Edge, Firefox, Safari

Sharing Portal	Mobile Devices -Google Chrome, Safari, Samsung Internet
	Desktop Devices – Google Chrome, Microsoft Edge, Firefox, Safari
Public Portal	Mobile Devices -Google Chrome, Safari, Samsung Internet
	Desktop Devices – Google Chrome, Microsoft Edge, Firefox, Safari
Business Portal	Mobile Devices -Google Chrome, Safari, Samsung Internet
	Desktop Devices – Google Chrome, Microsoft Edge, Firefox, Safari

3.6 *Hardware Specification (Client)*

Each device must have resources that meet the minimum requirements for the browser used to access the required NICE Portal(s)

3.7 *Bandwidth*

It is assumed that sufficient bandwidth and any contention have been discussed and verified prior to receiving this document.

(Rest of Page Intentionally Left Blank)

4 Appendix A – Authentication Readiness

Please complete the following table with Azure Active Directory connectivity information

Item	Value
Azure Active Directory Tenant ID	
Azure Active Directory Application (Client) ID	
Azure Active Directory Client Secret (or method of acquisition)	
Azure Active Directory Client Secret Expiry Date	

Please list all Azure Active Directory Groups (and their associated Object IDs) that will be used to authenticate users in the NICE environment

Azure Active Directory Group Name	Object ID

NOTE: Please add more rows to the above table as required

(Rest of Page Intentionally Left Blank)

5   Appendix B – Network Readiness

Please enter IP addresses (or ranges), and appropriate descriptions that should be allowed access to the NICE cloud-based environments.

IP Address	Description

(Rest of Page Intentionally Left Blank)

6   Appendix C – DSG Readiness

Please enter the IP addresses and machine names of all machines that will be used to hold NICE Data Source Gateways

IP Address	Machine Name

Please enter the name and password of the account that the DSG Service will run under

Domain Name (or "local")	Username	Password (or method of acquisition)

Please provide details of the remote access environment that NICE will use. Please include any necessary user names and passwords. Alternatively please indicate if there are external documents that contain this information (and where they can be found or when and by whom they will be provided)

Remote access details

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines have access to the Internet	
DSG machines have been built in line with the requirements and minimum specifications set out in this document	
DSG machines can be accessed by NICE personnel for installation and support purposes	
DSG service account is able to read the registry on the machine	

7 Appendix X – Connector Readiness

7.1 *Connector – Capita ControlWorks CAD*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
SQL DB Port	.	TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
Production/Live System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

8   Appendix X – Connector Readiness

8.1   *Connector – Capita EvidenceWorks DIR (via DB)*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137
Production/Live System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

9   Appendix X – Connector Readiness

9.1   *Connector – David Horn DIR*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
File share path		
File share access credentials		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137
Production/Live System		
File share path		
File share access credentials		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

10   Appendix X – Connector Readiness

10.1   Connector – Fotoware (via API)

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
Base API URL		
API Key		
Client ID		
Client Secret		
Production/Live System		
Base API URL		
API Key		
Client ID		
Client Secret		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

11   Appendix X – Connector Readiness

11.1   Connector – Generic Axon Evidence Partner API

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
Agency/Partner Id		
Base API URL		
Client ID		
Client Secret		
Production/Live System		
Agency/Partner Id		
Base API URL		
Client ID		
Client Secret		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

12   Appendix X – Connector Readiness

12.1   *Connector – Hexagon Intergraph CAD*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
Production/Live System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

13   Appendix X – Connector Readiness

13.1   *Connector – Indico DIR*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137
Production/Live System		
SQL DB Port		TSQL/TCP 1433
SQL Server Instance		
SQL Server DB Name		
SQL Server User		
SQL Server Password		
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

14   Appendix X – Connector Readiness

14.1   Connector – Motorola Edesix BWV

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
API Port		http/TCP 9080
API Base URL		
User Name		
Password		
Production/Live System		
API Port		http/TCP 9080
API Base URL		
User Name		
Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

15   Appendix X – Connector Readiness

15.1   Connector – NICE Inform

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
Data Source Name(s)		
Server Name(s)		
Server Address(es)		
Network Port		http/TCP 8086
Login Name		
Password		
Production/Live System		
Data Source Name(s)		
Server Name(s)		
Server Address(es)		
Network Port		http/TCP 8086
Login Name		
Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

16   Appendix X – Connector Readiness

16.1   *Connector – Niche RMS*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
DB server		
DB schema		
DB port		TSQL/TCP 1433
DB user		
DB password		
API server		
API port		http/TCP 80
API user		
API password		
Production/Live System		
DB server		
DB schema		
DB port		TSQL/TCP 1433
DB user		
DB password		
API server		
API port		http/TCP 80
API user		
API password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

17   Appendix X – Connector Readiness

17.1   *Connector – Niche RMS User Connector*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
DB server		
DB schema		
DB port		
DB user		
DB password		
Active Directory Domain		
Active Directory user		
Active Directory password		
Active Directory Root Container(s)		
Production/Live System		
DB server		
DB schema		
DB port		
DB user		
DB password		
Active Directory Domain		
Active Directory user		
Active Directory password		
Active Directory Root Container(s)		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

18   Appendix X – Connector Readiness

18.1   Connector – Redbox audio logger

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
API Port		http/TCP 1480
API Base URL		
User Name		
Password		
Production/Live System		
API Port		http/TCP 1480
API Base URL		
User Name		
Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

19   Appendix X – Connector Readiness

19.1   *Connector – Reveal BWV (DEMS 360)*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
API Endpoint		
Username		
Password		
SQL DB Port		TSQL/TCP 1433
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137
Production/Live System		
API Endpoint		
Username		
Password		
SQL DB Port		TSQL/TCP 1433
File share port(s)		SMB/TCP 445 NetBIOS/TCP 139 NetBIOS/UDP 138 NetBIOS/UDP 137

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

20   Appendix X – Connector Readiness

20.1   *Connector – SAAB (SAFE) CAD*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
Server (Elastic Search)		
Connection port		
Username		
Password		
Production/Live System		
Server (Elastic Search)		
Connection port		
Username		
Password		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

21   Appendix X – Connector Readiness

21.1   *Connector – Sopra Steria (Storm) CAD*

Please provide the following information:

Item	Response (or N/A)	Typical or default values
Pre Production/Test System		
DEMSFacade Endpoint		
Master User Name		
Master Password		
User Name		
Production/Live System		
DEMSFacade Endpoint		
Master User Name		
Master Password		
User Name		

NOTE: "Typical or Default" values are provided for reference only and should be verified with the data source provider

Please confirm the following actions have been completed:

Action	Confirmation (Y) or N/A
DSG machines holding this connector have an open network route to the data source (including access to the IP addresses or URLS and opening of required firewall ports)	

Attachment D – Box.com Integration Functionality Requirement

Integration from DEMS to Box
There are two primary scenarios for integrating from DEMS to Box.

Scenario 1- Evidence arrives initially
Step 1 - Evidence comes in to DEMS from outside (DA, etc.). Users will receive some kind of notification of this, preferably alerts in their CMS eDefender.
Step 2 – User enters metadata, description, etc. as required
Step 3 - User clicks a button to copy the selected file(s) to Box as soon as the file(s) arrives.
This step will require naming the file correctly and populating the Box metadata as needed. The naming convention is described below.
Automation is also needed to put police reports and all other Bates Stamped PDF documents into the Discovery folder in the Public Defender's instance of Box for the case. Everything else that is not a Bates Stamped PDF document is placed in the Discovery Media folder in the Public Defender's instance of Box for the case.
There are instances where folders with many files are shared. DEMS will need to separate out the files in the folder and put them in the correct locations.

Scenario 2 - Creation of snips, stills, etc. from files already loaded in DEMS
Step 1 - create the snip, still, etc.
Step 2 - Enter metadata, description, etc. as required
Step 3 - User clicks a button to copy the selected file(s) to Box
This step will require naming the file correctly and populating the Box metadata as needed. The naming convention is described below.

Box File Naming Conventions
The eDefender system contains an eDefender ID and a Box ID (among other pieces of data) for each case. For the integration to Box from DEMS being developed by COSB using the NICE Enhanced API as defined in Task 4 – Systems Integration Expectations, COSB will obtain the eDefender ID and the Box ID using the eDefender integration. COSB will use these data elements to determine where to put files in Box. As the integration copies the files to Box, it will also rename the files appropriately. The file naming conventions are:

For PDF files: Bates Stamp 1 - Bates Stamp 2_Disc #_Name.pdf
For other files: Disc #_Name.pdf

The Bates Stamps are obtained by scanning the PDF file and finding the Bates Stamp on the first page and the one on the last page. These are the bates numbers used in the file name.

The Disc # is provided by DA.

The Name portion of the file is also provided by DA.

Integration to DEMS from Box
There may be times where files stored in Box have to be uploaded to DEMS. Public Defender's

preferred approach to this is to have an upload button in DEMS where they can choose Box as the source of the files to be uploaded. This interface can be similar to a File Explorer type interface where Box appears as an option. From there, the user will have the ability to navigate to the appropriate Box location and select one or more files and/or folders to upload from Box to DEMS. The files will be uploaded without changing the file names.

(Rest of Page Intentionally Left Blank)

Attachment E – Sample System Security Plan

Table of Contents

Deliverable Expectations: NICE System Security Plan
Contractor shall provide the following Security sub-tasks and deliverables:

Task 3. Security Sub-Tasks and Deliverables

Task	Sub-Task	Descriptions	Deliverables
3.1	System Security Management	Contractor shall provide a System Security Plan that describes the security approach for DEMS. In addition, because of the expected interactivity with other entities, a comprehensive plan shall explain how DEMS will respect and coordinate, when necessary, with the security constraints of other entities.	The System Security Plan shall address, at a minimum, the following areas: • General Information about System Environment, Interconnections/Information Sharing, Applicable Laws or Regulations, Information Sensitivity, Responsible Parties, General System Description • Security Controls pertaining to Risk Assessment and Management, User Rules or Behavior, Implementation Phase, Operation and Maintenance Phase • Technical Controls pertaining to User Identification and Authentication, Logical Access Controls, Audit Trails **The Deliverable shall include a DED.**
3.2	System Security not user security (ongoing – as changes are made)	Establish Patch management processes and procedures that are transferred to the County after successful completion of DEMS installation.	Provide documentation and training on system and patch management including regular maintenance, upgrades, and response to zero-day exploits.
3.3	Third Party Compliance Attestation (ongoing – annual)	Complete a third-party compliance review and provide attestation that security compliance controls are followed.	The Third-Party Compliance Attestation will address at a minimum: • What they did • What they remediated • The Vendor will remediate anything that is non-compliant at no cost to County

Deliverable Expectations: NICE System Security Plan

Project Deliverable Number: *<Insert - TBD>*	Title of Deliverable: System Security Plan
Draft Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Draft Review & Comment Period:** *<Insert - TBD>*
Final Submission Due Date: *<Insert – TBD, as mutually agreed >*	**County Final Review & Comment Period:** *<Insert - TBD>*
Reviewed By Required: *<Yes/No – by whom –TBD as mutually agreed >*	**Deliverable Document Format:** *< Word / PDF>*
Deliverable Owner (County): *<Name, Role – TBD, as mutually agreed >*	**Deliverable Author (Vendor):** *<Name, Role - – TBD, as mutually agreed >*

Deliverable Description and Purpose:

NICE designed NICE DEMS from the ground up with security in mind, with Microsoft Azure Government as our cloud provider. The combination of NICE DEMS and the Microsoft Azure Government cloud offers law enforcement agencies a comprehensive, scalable, CJIS- compliant cloud-based investigative software solution for managing investigations, and storing and safeguarding digital evidence. The plan provides details of CJIS compliance.

Deliverable Scope / Content Expectations:

NICE will provide full documentation of Security related to your solution. The deliverables will include:

CJIS REQUIREMENTS AND NICE DEMS STEP-BY-STEP COMPLIANCE

13 POLICY AREAS

CJIS AUDIT READINESS

ANTIVIRUS, DATA BACKUP, PHYSICAL SECURITY

SECURE EVIDENCE MANAGEMENT SECURITY MANAGEMENT

ACCESS CONTROL AND USER AUTHENTICATION ACCESS TO EVIDENCE

Sample Enclosed:

NICE DEMS CJIS COMPLIANCE WHITE PAPER IS A STANDARDIZED DOCUMENT APPLICABLE TO ALL CUSTOMERS. IT WAS USED AS A SOURCE FOR THE INFORMATION PROVIDED HEREIN.

| References / Standards	FBI CJIS standards, NICE Software Testing and Quality Standards based on ISO 9001 guidelines, mutually agreed solution scope – detailed in functional & technical compliance matrixes (Appendix B-1) and any other project deliverables included in the contract between NICE and ISAB, related to the subject DEMS project.

Deliverable Criteria	Acceptable: The document is in full compliance with the approved DED and required content areas documented above.
	Rework Required: The document substantially in compliance with the approved DED and required content areas documented above. However, there are omissions or errors that need to be corrected before the document can be approved.
	Unacceptable: The document was not in compliance with the approved DED and required content areas documented above. There were significant omissions in content and or errors that need to be addressed before the document can be fully reviewed.

Security Management Plan

NICE designed NICE DEMS from the ground up with security in mind. And, this is why we chose Microsoft Azure Government as our cloud provider. The combination of NICE DEMS and the Microsoft Azure Government cloud offers COSB stakeholder agencies a comprehensive, scalable, CJIS-compliant cloud-based investigative SaaS solution for managing investigations, and storing and safeguarding digital evidence.

Details of the security designed into the NICE DEMS SaaS offering is provided in the following sections. At a high level, this Security Plan for COSB addresses all aspects of the DEMS solution including physical security, security of compute resources and storage, network security, security management, and security of the application development process. All security processes are in compliance with Industry Standards bodies guidelines.

PHYSICAL SECURITY
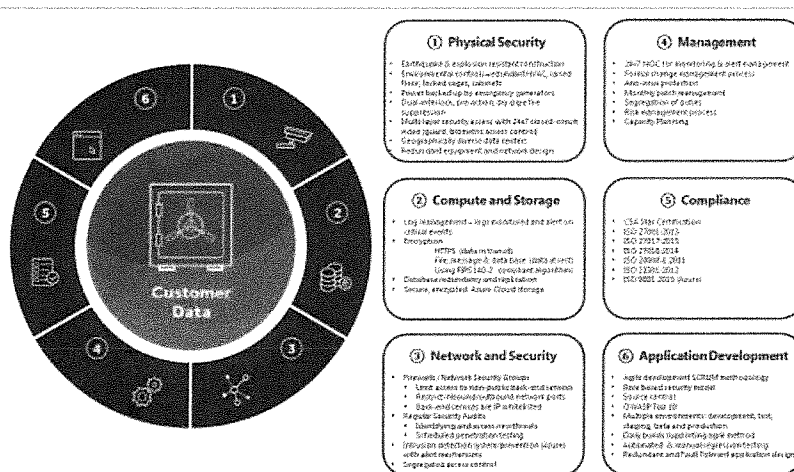
Information herein is proprietary information and trade secrets of NICE Ltd

NICE

- Earthquake & explosion resistant construction
- Environmental controls–redundant HVAC, raised floor, locked cages, cabinets
- Power backed up by emergency generators
- Dual-interlock, pre-action, dry-pipe fire suppression
- Multi-layer security access with 24x7 closed-circuit video (guard, biometric access control)
- Geographically diverse data centers
- Redundant equipment and network design

COMPUTE AND STORAGE SECURITY

36

- Log management – logs monitored and alert on critical events
- Encryption
- HTTPS (data in transit)
  - File, message, and database (data at rest)
  - FIPS 140-2 compliant algorithms
- Database redundancy and replication
- Secure, encrypted Azure Cloud storage

NETWORK SECURITY

- Firewalls / Network Security Groups
- Limit access to non-public back-end services
- Restrict inbound/outbound network ports
- Back-end services are IP whitelisted
- Regular Security Audits are conducted
- Identifying and assess new threats
- Scheduled penetration testing
- Intrusion detection system/prevention (Azure) with alert mechanisms
- Segregated Access Control

SECURITY MANAGEMENT

- 24x7 NOC for monitoring & alert management
- Formal change management process
- Anti-virus protection
- Monthly patch management
- Segregation of SaaS duties with access controls
- Risk management process
- Capacity Planning

SECURE APPLICATION DEVELOPMENT

- Agile development SCRUM methodology
- Role based security model
- Source control
- OWASP Top 10
- Multiple environments: development, test, staging, beta and production
- Daily builds supporting agile method
- Automated & manual regression testing
- Redundant and Fault Tolerant application design

COMPLIANCE

- CSA Star Certification
- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 20000-1:2011
- ISO 22301:2012
- ISO 9001:2015 (Azure)

Microsoft Azure Government – A Secure Foundation

Already used by more than a hundred government agencies, the Microsoft Azure Government platform is the trailblazer in the government cloud market. It was the first hyperscale infrastructure cloud platform contractually committed to meeting the FBI's Criminal Justice Information Services (CJIS) requirements for federal, state and local governments. The Microsoft Azure Government platform is inherently secure, as its use is restricted to qualified federal, state, local and tribal government agencies and their screened providers.

Additionally, Azure Government addresses the stringent security and compliance requirements for other key government regulations, such as the United States Federal Risk and Authorization Management Program (FedRAMP), the Department of Defense Enterprise Cloud Service Broker (ECSB), and the Health Insurance Portability and Accountability Act (HIPAA).[i]

Law enforcement agencies looking to take advantage of NICE DEMS's powerful digital policing and investigative capabilities delivered through the Microsoft Azure Government cloud platform can be confident in the solution's ability to protect sensitive case evidence.

This DEMS Security Plan outlines the many aspects of the integrated NICE DEMS/Microsoft Azure Government solution designed to keep your case evidence secure, while helping you comply with the FBI's CJIS requirements.

13 AREAS OF DEMS SECURITY CJIS: 13 KEY POLICY AREAS

The FBI Criminal Justice Information Services (CJIS) Security Policy includes a number of technical safeguards designed to protect and secure FBI Criminal Justice Information. But CJIS compliance is not just about technology, it's also about processes and people. Hosted software solutions cannot achieve CJIS compliance on their own merits; they must be operated within and by organizations that adhere to prescribed CJIS policies, processes and procedures.

The FBI defines 13 key areas that cloud service providers must address to be aligned with CJIS requirements which are summarized in more detail below.

More detailed information on these key policy areas can be found in the FBI CJIS Security Policy Resource Center on the FBI website at https://www.fbi.gov/services/cjis/cjis-security- policy-resource-center.

NICE has commissioned an independent consultant, Diverse Computing, Inc., whose team of Audit and Compliance Experts (ACEs) is working with NICE to ensure that NICE DEMS supports each of key FBI CJIS requirement areas.

ADDRESSING THE 13 KEY FBI CJIS POLICY AREAS

As noted above the FBI's Criminal Justices Information Services (CJIS) Policy covers 13 key areas which cloud service providers must address: 1) Information Exchange Agreements; 2) Security Awareness Training; 3) Incident Response; 4) Auditing and Accountability; 5) Access Control; 6) Identification and Authentication; 7) Configuration Management; 8) Media Protection; 9) Physical Protection; 10) Systems and Communications Protection and Information Integrity; 11) Formal Audits; 12) Personnel Security; and 13) Mobile Devices.

The purpose of FBI CJIS security policies is to establish minimum security requirements to protect and secure various types of FBI Criminal Justice Information.

NICE not only adheres to these policies, it has taken a conservative approach (based on the recommendations of the International Association of Chiefs of Police) by applying CJIS policy to all data collected, analyzed and shared through NICE DEMS, including data that by definition falls outside of the scope of CJIS security policy.

More information on how NICE and Microsoft Azure Government address each of the key 13 policy areas is included in the detailed table in Appendix A, starting on page 18.

NICE's hosting partner, Microsoft, has already signed CJIS Security agreements in many states.

38

Upon request, NICE can provide documentation to show how NICE DEMS complies with your state's specific CJIS security requirements.

MINIMIZING OPEN FIREWALL PORTS AND SECURITY RISK

Your agency's firewall serves a vital purpose – it protects your trusted, secure internal network from outside security risks. The more ports (holes) you open on your firewall, the more vulnerable your network is, and the easier it is for hackers to penetrate holes in firewalls are also directional. Generally speaking, inward holes (that allow inbound connections) present a higher security risk than outward holes (that enable outbound connections between your network and some external source). Any nefarious individuals wanting to breach your network from outside need to find an inward hole to launch an attack.

For this reason, NICE DEMS *does not require any inward firewall holes* to access any systems on your network. All communications are initiated from within your network, outward to the NICE DEMS cloud, and those communications are encrypted.
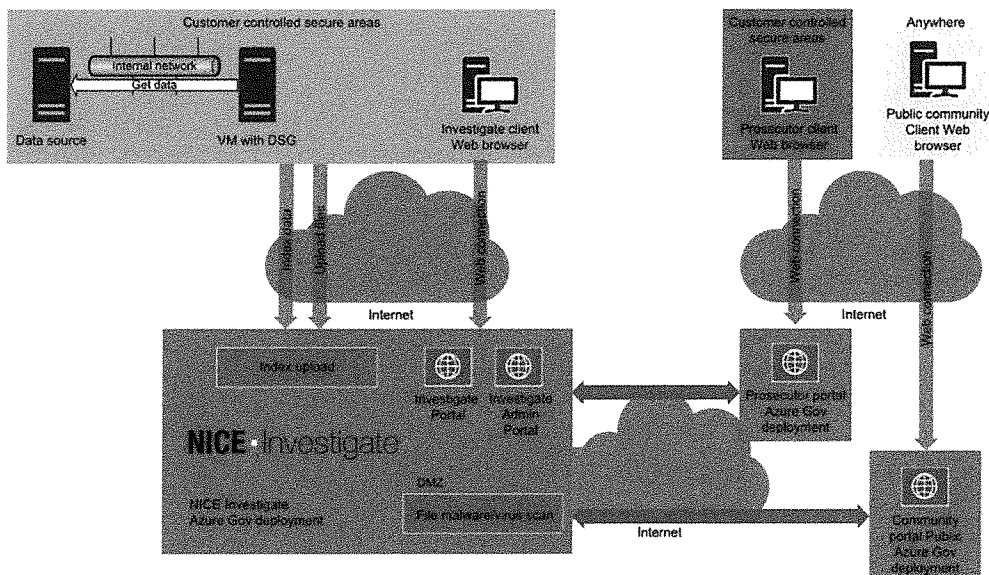
STRONG ENCRYPTION PROTECTS YOUR DATA

NICE DEMS ensures that all data in transit outside of secure areas is encrypted using TLS 1.2.256 bit encryption (FIPS 140-2 standard). Similarly, all case evidence that agency investigators share with prosecutors via NICE DEMS's Prosecutor Portal is secured by encryption as well. Data at rest is encrypted and secured by NICE's hosting partner, Microsoft, at ultra-secure data center locations within the Azure Government network.

Below is a schematic that illustrates this concept. It shows the agency secure areas and the Microsoft Azure Government cloud secure areas with encrypted data transfer between them. In addition, public and community-generated data (for example crowdsourced data or uploaded third party video) is stored in the Microsoft Azure public cloud, and is virus scanned before it's transferred to the Microsoft Azure Government cloud. This ensures that all information entering the Microsoft Azure Government cloud is virus-free and doesn't pose a danger to the secure system.

In this NICE DEMS solution architecture, the colored rectangles are secure, and the blue interconnects are encrypted. Public uploads reside in the public cloud initially until they are transferred into a secure cloud via DMS and virus scan. The main blue rectangle – NICE DEMS – is where all stored data is encrypted.

LOCKING DOWN ACCESS TO SENSITIVE CASE EVIDENCE

- **Account Management, Access Enforcement and Access Control Criteria** – Only agency officials with administrator rights to NICE DEMS can establish and activate user accounts. If specific users leave the agency, or their roles changes, administrators can modify, disable, and remove those user accounts accordingly. NICE DEMS user rights/access privileges are based on a Policy-Based Access Control (PBAC) model. This model allows flexible rules to be created to configure security access for specific users and groups, based on their roles (e.g. homicide detective, etc.) and rights (owner of a case or contributor). Also referred to as Attribute

Access Control, this feature of NICE DEMS allows administrators to also set up rules that control which material can be accessed by which users (compliant with NIST Special Publication 800-162).

- **Access Control Mechanisms** – Pre-established user rights in NICE DEMS dictate what cases and evidence items a user can access and the specific things the user can do (e.g. add evidence, create bookmarks, contribute comments, or simply view what's inside a virtual case folder). NICE DEMS also ensures that all data in transit is protected through encryption.

- **Unsuccessful Login Attempts** – The NICE DEMS system offers a customizable setting to automatically and temporarily lock a user out of his/her account following a pre- specified number of failed login attempts.

- **Session Lock** – Similarly, there is a customizable session timeout setting that will lock a user out after a pre-specified number of minutes of inactivity to prevent inadvertent viewing when a device is left unattended.

- **Remote Access & Publicly Accessible Computers** – Agencies can restrict access to defined IP ranges, so users can only access NICE DEMS from approved office locations. Additionally, any device accessing NICE DEMS requires a X.509 device security certificate (this feature can be disabled where agencies have existing network access control systems in place), thus ensuring that NICE DEMS can only be accessed from authorized devices. Each agency can control which devices are issued certificates and limit access to only those mobile devices with suitable protection (e.g. encryption). All remote connections occur via an encrypted (FIPS 140-2 certified) path. All remote users accessing DEMS must be identified prior to access and authenticated prior to or during the session.

- **Identification and Authentication** – All users attempting to access NICE DEMS must have a valid user profile, and access to NICE DEMS is controlled by a user name / password combination, with FBI CJIS-compliant complex password enforcement rules. If required, NICE DEMS can also support two-factor authentication (also known as Advanced Authentication) in two manners. NICE DEMS supports two-factor authentication and single sign on by using your agency's ADFS SSO, or Active Directory Federation Services Single Sign-on, *which already provides two-factor authentication),* as the NICE DEMS login. When a user with an active profile in NICE DEMS signs on to ADFS, NICE DEMS will automatically transfer any claims assigned to the user from the ADFS to NICE DEMS. If your agency does not use ADFS SSO then NICE DEMS can support two-factor authentication in an alternate manner. As noted above, NICE DEMS provides agencies with the option to limit which devices access the service by means of client certificates. Client-side certificates can be used with TLS to prove the identity of the client to the server. As a second level of authentication, the user using the device would have to enter a valid user credential and password.

  - Users, user groups, and user roles are created and managed in the DEMS Administration Portal by a COSB assigned DEMS System Administrator(s). We recommend a minimum of one System Administrator per Stakeholder Agency.

  - Users can be created by synching with the county's Active Directory database. Rules and roles can also be obtained by interfacing with the county's Active Directory database or other identified HR database.

  - Users access shall be authenticated using X.509 certificates and a username and password. IP whitelisting can also be implemented as required.

WORKING WITH INTEGRATIONS AND SECURITY ISSUES WITH 3RD PARTY VENDORS

There are several ways that NICE DEMS can collect information from your core systems. The first method is via integration API, where the vendor of the core system provides an API so that NICE DEMS can access the system in a manner approved by the vendor.

NICE DEMS can also pull data from read-only copies of databases, or database warehouses. This eliminates the need to interface with live production systems. NICE DEMS can also pull data from views provided on live databases.

Finally, NICE DEMS can pull data from file shares (for example folders containing crime photos). Agencies may choose to implement different methods for different core systems.

A successful implementation will require integrations with many data sources from different vendors. Each data source may bring its own security issues to be addressed. NICE will work with COSB and if necessary other vendors to work through these

security issues to identify and deploy a solution.

SECURE EVIDENCE MANAGEMENT

NICE DEMS provides a baseline set of security controls providing appropriate protection against typical threats such as unauthorized access to the service; upload of malicious content to DEMS; unauthorized access and distribution of assets in DEMS.

All information is handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack.

- Hosted in the Microsoft Azure Government data centers. This cloud platform and application are CJIS certified and provide enhanced security policies for access control and maintenance.

- Encryption at rest of all collected digital evidence along with any metadata using strong AES-256 encryption.

- Virus checking of all data uploaded to DEMS to protect against malicious content being uploaded.

- User access is via secure HTTPS browser connections with 2-factor authentication for login

- Attribute based access controls for accessing digital evidence

- Chain of custody reports proving the authenticity of collected evidence

PROTECTION FROM POTENTIAL OUTSIDE THREATS

The NICE DEMS platform is comprised of three main application portals: The Public Portal, the Investigation Portal and the Prosecution Portal.

The Public Portal allows citizens to electronically and securely photos and video with police departments. It also provides businesses and residents with a virtual place to easily register their private CCTV cameras so that investigators have a better understanding of what cameras are located within the area of an incident. Knowing where the cameras are and who owns them, an investigator can send out an electronic request to have the video footage uploaded to the secure portal.

Crowdsourced evidence can offer some of the best leads in investigations. But because these files come from outside your secure network environment, they can contain malware or viruses, thus posing a threat to other secure digital evidence in the Microsoft Azure Government cloud.

NICE DEMS solves this problem by making sure that all crowdsourced public content is staged outside of the Microsoft Azure Government secure cloud, where it is automatically virus scanned. Only then can it be selected by a detective and uploaded to the secure Microsoft Azure Government cloud.

ADDRESSING ACCESS CONTROL THROUGH USER ROLES/RIGHTS

Policy-based Access Control Model

FBI CJIS Access Control Policy (5.5.2.1) notes that, in order to mitigate the risk to CJI, agencies should adhere to a "Least Privilege" approach which limits access to CJI to only authorized personnel with the need and the right to know. Essentially this means that the agency should enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.

Limiting access to case evidence to those who have a need to know is absolutely critical. When evidence gets into the wrong hands it can compromise a case. Additionally, in high profile cases, prematurely disclosing evidence through the media can victimize a victim all over again.

NICE DEMS's user rights/access privileges are based on a Policy-Based Access Control (PBAC) model which restricts access based on a specific user's role within the organization, and his/her need to access specific data (e.g. as the owner of a case, contributor to a case, or supervisor). Access can be further restricted based on specific cases (e.g. homicide case ABC), or specific types of cases (e.g. all homicide cases).

NICE DEMS implements an attribute-based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know".

The control of access rights is established in DEMS via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.

41

It is also possible to create a connection to synchronize and inherit access control rules with a customer's existing records management system as a custom integration.

The NICE DEMS System Administrator is responsible for working with the NICE system engineer to implement access rules for users.

The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in DEMS.

User access to cases, evidence, and features within NICE DEMS is controlled by a Security Access Control Policy. Access control rules shall be defined by the customer during the Planning Phase of the project.

LOCKING DOWN SENSITIVE CASE FILES

In many states, there are laws governing confidentiality for cases involving certain types of crimes, particularly those involving children/juveniles and sex crimes. High profile cases involving celebrities may also be sensitive.

Case owners have the ability to mark any case they are managing as 'sensitive.' This will lock down the case, restricting access solely to the case owner. So even if the agency had designated all homicide detectives as contributors to all homicide cases, they would not be able view or contribute to any cases marked as 'sensitive' based on the NICE DEMS user access rules engine. Finally, individuals from the subscribing agency can also be designated as administrators of the NICE DEMS system. Administrators are able to add users to the system, assign roles and rights, change roles and rights, and delete users. Police departments are highly dynamic environments and it's not uncommon for investigators to transfer in or out, or even transition to other divisions with completely different geographies. NICE DEMS enables your administrator to update user roles and rights as needed.

SHARING EVIDENCE WITH EXTERNAL USERS

The final step in the process of building a case typically involves sharing the case and its evidence (or in the early stages portions of the collected evidence) with a prosecutor for case direction advice, and ultimately for filing consideration. In NICE DEMS this is done through the prosecutor portal. But before a District Attorney (DA) or intake person at the DA's office can be granted access to view any portion of the case, he/she first needs to be registered and approved as a user. NICE DEMS's x.509 certificate provides an extra level of security by restricting access to only users on authorized devices.

As a registered user, a DA can log in to the secure prosecutor portal and set up a user name and password.

NICE DEMS offers similar flexibility in setting up external user access privileges, as it does for internal users. The NICE DEMS system is flexible enough to allow your agency to provide access to specific DAs on a case-by-case basis, or to set up rules for which types of cases (e.g. felony, domestic violence, sexual assaults) can be accessed by which DAs, or groups of DAs who typically handle those cases.

Once these rights are established, investigators (case owners) can share cases or selected case evidence with DAs or intake personnel, providing they are registered and approved users. The investigator can share a virtual case folder with a DA by emailing a link to a secure portal (with a snapshot of the digital case) which the DA can then open and review. The DA must log on to the prosecutor portal (from an approved device with a proper X.509 certificate) to view the case contents. The DA's access privileges only allow him/her to view the case and attached evidence; he/she cannot download, edit, delete or change any of the virtual case folder contents.

It's also important to note that the DA is not directly accessing any data in the Microsoft Azure Government cloud; instead, he/she views a snapshot copy of the virtual case folder and contents through the prosecutor portal and does not have direct access to the original case or its evidence. All information received by the DA through the remote connection is SSL encrypted. Finally, all user activity on the NICE DEMS system, involving both internal and external users, is thoroughly tracked by NICE DEMS and can be audited if necessary.

PROTECTING CHAIN OF CUSTODY

In a legal context, chain of custody refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

To maintain chain of custody, you must preserve evidence from the time it is collected to the time it is presented in court. To prove the chain of custody, and ultimately show that the evidence has remained intact, prosecutors generally need service providers who can testify: 1) that the evidence offered in court is the same evidence they collected or received; 2) to the time

and date the evidence was received or transferred to another provider; 3) that there was no tampering with the item while it was in custody.

A chain of custody ensures that the data presented is "as originally acquired" and has not been altered prior to admission into evidence.

Chain of custody is especially important for electronic evidence because it can be more easily altered.

Chain of custody is the foundation the prosecution needs to establish for certain types of exhibits to be admitted into evidence.

Defense strategies often rely on bringing the chain of custody into question. If the strategy's successful, the case could be compromised or thrown out.

Whether physical or digital evidence, it's essential to track chain of custody. Today, when physical evidence is booked into the evidence room, all the details surrounding who recovered it, where, when, etc., are entered, documented and tracked in your agency's evidence tracking system. Digital evidence copied onto CDs, DVDs or USB drives is handled the same manner.

NICE DEMS does not replace your evidence tracking system for logging and tracking physical evidence, but it does simplify the process of handling and securing digital evidence and tracking its chain of custody. Here's how.

Instead of copying digital evidence onto CDs, DVDs, and USB drives, and locking it in an evidence room, with NICE DEMS, digital case folders and their digital evidence contents are securely stored in the Microsoft Azure Government Cloud.

The NICE DEMS system automatically tracks whenever any authorized system users access a digital case folder or any of its digital evidence contents in an event log. It also tracks what they did and when they did it – for example if they viewed a piece of evidence, downloaded it, copied it, annotated it, or shared it, and even who they shared it with.

The chain of custody event logs can be viewed online or printed in a report format for court if needed. Only someone who has been assigned access to a case (e.g. case owner or contributor) can access the chain of custody report for an evidence item in the case.

NICE DEMS's chain of custody event logs are tamper-proof. Event logs are protected by block chains which link and lock data (for each instance where evidence was viewed /touched/etc.) to the next instance in a chronological sequence. This ensures chain of custody event logs can't be edited.

Furthermore, when digital evidence is added to DEMS NICE, there is no way for an investigator to edit or modify the original digital evidence. Instead, NICE DEMS creates working copies of the evidence that the investigator can work with as he/she builds the case. For example, an investigator can insert comments, redact video/audio, and annotate working copies of digital evidence. NICE DEMS tracks chain of custody for all working copies, as well as tracking the chain of custody for the original digital evidence.

DETAILED AUDIT TRAILS AND ACTIVITY LOGS

The FBI Criminal Justice Information and other sensitive evidence used in investigations can be highly sensitive and confidential. Your agency must be able to audit exactly who has accessed data, when, how, and for what purpose.

NICE DEMS's Chain of Custody function tracks all user actions related to a digital case folder or any of its digital evidence contents to ensure evidence integrity. The NICE DEMS Audit Trail, on the other hand, tracks and logs *all* activity on the system.

CJIS Security Policy (5.4.1 Auditable Events and Content - Information Systems), specifies that audit records must be generated and logged for specific types of events, including:

- Successful and unsuccessful system log-on attempts;

- Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource;

- Successful and unsuccessful attempts to change account passwords;

- Successful and unsuccessful actions by privileged accounts;

- Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

NICE DEMS automatically logs and maintains a record of all of these activities. These records can be reviewed by a designated administrator or security officer within the agency.

This individual can review the audit records to look for indications of inappropriate or unusual activity or to DEMS suspicious

activity or suspected violations, and then report their findings to appropriate officials, who can then take necessary actions. According to CJIS Security Policy 5.4.3 (Audit Monitoring, Analysis and Reporting), this audit review/ analysis should be conducted at a minimum once a week.

If a security concern comes up outside of the ongoing audit review/analysis process, a designated security officer with proper system access can use NICE DEMS 's audit logs to re-trace any related activity necessary to complete his/her investigation. CJIS Security Policy 5.4.5 (Protection of Audit Information) also stipulates that the audit information should be protected from modification, deletion and unauthorized access. NICE DEMS's audit logs are secured in a password-protected database with no way for users to edit the logs.

CJIS AUDIT READINESS

As noted above, agencies with access to FBI CJIS systems and information are subjected to formal audits. NICE DEMS tracks and logs all user activity and provides audit trail reporting that can help your agency demonstrate its compliance with specific CJIS requirements.

For example, one CJIS requirement states that user accounts be disabled when a user is no longer employed with the agency. Your agency can use the NICE DEMS audit trail to demonstrate that the user's account was disabled on the day that individual left the organization.

The audit log can also demonstrate that all required auditable events (per CJIS 5.4.1) have in fact been logged.

ANTIVIRUS SOFTWARE AND OTHER BUILT-IN PROTECTION MECHANISMS

As noted earlier, NICE DEMS leverages both the Microsoft Azure "public" and Microsoft Azure Government clouds to manage data at various stages of an investigation. NICE uses third-party anti-malware software to scan, identify and remove viruses, spyware and other malicious software and provide real time protection. All data is virus scanned before it is transferred to a secure area.

Other built-in protection mechanisms include:

- **Automatic & transparent security updates** – As your Software as a Service (SaaS) providers, NICE and its hosting partner, Microsoft, are responsible for managing all software and security updates. Integrated deployment systems manage the distribution and installation of security patches.

- **Intrusion detection & DDoS** – To protect the Microsoft Cloud, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the continuous monitoring and penetration-testing processes of Azure. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks.

- **Penetration testing** – NICE and its hosting partner Microsoft conduct regular penetration testing to improve NICE DEMS security controls and processes. By constantly challenging the security capabilities of the service, we stay ahead of emerging threats.

DATA BACKUP AND INHERENT DISASTER RECOVERY

NICE's hosting partner, Microsoft, protects your agency's data through Geo-Redundant Storage (GRS) which replicates the data across two geographically distributed Microsoft Azure Government datacenters (located over 500 miles apart). Geo-replication ensures the digital evidence crucial for investigations will always be available, even in the most unpredictable of circumstances. This level of disaster recovery is difficult if not impossible for most individual agencies to achieve on their own.

In addition to ensuring business continuity, there are other inherent advantages to using a Software as a Service Provider instead of self-hosting on-site, including: fewer headaches *(think of endless rolling hardware upgrades; and the additional real estate, operational, maintenance, and security costs/challenges that come with managing your own data center)*, and think about paying for everything up front vs. the ability to "pay as you go," and only for what you need.

STATE-OF-THE-ART PHYSICAL SECURITY

Finally, the Microsoft Azure Government data centers are physically constructed, managed, and monitored to protect data and services from unauthorized access and other threats, via:

- **24-hour monitored physical security** – Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

- **Monitoring and logging** – Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.

- **Security** – Datacenters are secured using physical, logical and procedural controls. Important controls include secured access control to the datacenter, second person screened escorts, aisle cameras, and secured cabling. All security controls are audited and logged.

- **Screened personnel** – Operations and support are performed by personnel in the United States, who have been background screened.

- **Continental United States** – All customer data, content, and organizational data (both at rest and in transit); all hardware, networking and other physical infrastructure; and all personnel reside in the Continental United States (CONUS).

PLANNING TOGETHER FOR A SECURE SERVICE OFFERING

Digital evidence is growing every day and becoming increasingly difficult for police departments to manage. The combination of NICE DEMS and the Microsoft Azure Government cloud can provide your County Agencies with a comprehensive, scalable, CJIS- compliant cloud-based investigative software solution for managing investigations, and storing and safeguarding digital evidence.

This DEMS Security Plan has detailed the many aspects of the integrated NICE DEMS/Microsoft Azure Government solution designed to keep your case evidence secure, while helping your agency comply with the FBI's CJIS requirements.

During the Project Planning Phase, the DEMS Security representative will review this information with the designated customer Security representative(s) to ensure a through understand of all security aspects of the DEMS SaaS solution. Areas of concern with respect to potential gaps in this security plan will be documented, mitigation plans will be developed and tracked to resolution.

We have included a Security Test Plan from a previous Customer project to show the various security aspects tested prior to system turnover to the customer..

EXHIBIT B - PAYMENT ARRANGEMENTS: Periodic Compensation (with attached Schedule of Fees)

A. For CONTRACTOR services to be rendered under this Agreement, CONTRACTOR shall be paid a contract amount, including cost reimbursements, not to exceed **$1,554,550 for years 1-5, with optional extensions for up to two additional years, bringing the total contract amount to $2,315,007.**

B. Payment for services and /or reimbursement of costs shall be made upon CONTRACTOR's satisfactory performance, based upon the scope and methodology contained in **EXHIBIT A** as determined by COUNTY.

C. Annually CONTRACTOR shall submit to the COUNTY DESIGNATED REPRESENTATIVE an invoice or certified claim on the County Treasury for the service performed over the period specified. These invoices or certified claims must cite the assigned Board Contract Number. COUNTY REPRESENTATIVE shall evaluate the quality of the service performed and if found to be satisfactory shall initiate payment processing. COUNTY shall pay invoices or claims for satisfactory work within 30 days of receipt of correct and complete invoices or claims from CONTRACTOR.

D. COUNTY's failure to discover or object to any unsatisfactory work or billings prior to payment will not constitute a waiver of COUNTY's right to require CONTRACTOR to correct such work or billings or seek any other legal remedy.

E. **SaaS Solution.** COSB hereby purchases a subscription to the following **NICE DEMS** SaaS Solution, and non-recurring charge implementation Services from NICE:

F. **NICE DEMS** SaaS Solution (includes "**Investigate SaaS Solution**", "Justice SaaS Solution" and "Defense SaaS Solution") as further described in the SOW attached hereto as Attachment 1 and incorporated herein by this reference.

G. NICE DEMS SaaS fee includes:
- Unlimited geo-redundant storage for all digital evidence related to cases.
- Unlimited automatic transcription – all playable video/audio will be transcribed upon ingestion.
- Advanced evidence redaction tools
- Case capacity as follows (see section K for monthly capacity):

End of Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6 *	Year 7 *
Case Import (Active)	7,000	0	0	0	0	0	0
Case Import (Archive)	0	0	0	0	0	0	0
Active Cases	24,000	24,000	24,000	24,000	24,000	24,000	24,000
Archived Cases	7,000	31,000	41,000	51,000	61,000	63,700	65,100
Deleted Cases	-	(1,167)	(14,000)	(14,000)	(14,608)	(21,408)	(22,717)
Total Managed Cases	31,000	55,000	65,000	75,000	85,000	87,700	89,100

- * Denotes optional years as described in Section 4 of the Agreement, above.
- The capacity in this table is the capacity for each year of the Term
- COUNTY can increase the Case Capacity at the current agreed upon rate on an annual basis.
- COUNTY will not be charged for deleting Cases
- Additional active cases beyond what's included in the above table will be charged at $ 1.25 per case/month; archive cases beyond what's included in the above table will be charged at $0.25 per case/month.

H. Archive cases that are returned to active state will be considered to remain in the active state for a minimum of 6 months.

I. **Invoicing.** The total amount due for the Investigate SaaS Solution Term fees (Years 1-5) are One Million, Five Hundred and Fifty Four Thousand,

Five Hundred and Fifty Dollars ($1,554,550) to be invoiced as follows:

Fee Type	Subscription Term – Years 1 - 5 (Years 6 - 7*)							Invoice Date
	Fees Year 1	Fees Year 2	Fees Year 3	Fees Year 4	Fees Year 5	Fees Year 6*	Fees Year 7*	
NICE DEMS Cloud Service Fees	$153,900	$252,000	$281,550	$299,550	$317,550	$328,432	$332,025	Initiation Date, and annually thereafter
NICE DEMS Test Environment	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	Initiation Date, and annually thereafter
Total NICE DEMS Term Fees	**$203,900**	**$302,000**	**$331,550**	**$349,550**	**$367,550**	**$378,432**	**$382,025**	**Initiation Date, and annually thereafter**

*Denotes optional years as described in Section 4 of the Agreement, above.

NICE will invoice for additional Cases in accordance with Section L, below. Invoicing will start one year following the Initiation Date and continue quarterly in arrears during the Subscription Term.

J. **System Case Capacity.** Within a given year during the Subscription Term, any increase or decrease in capacity from the previous year is adjusted monthly, in equal amounts. For example, if at the end of year 1 the system has capacity for 24,000 Cases and at the end of year 2 it has capacity for 36,000 Cases, there is capacity for 12,000 additional Cases, divided evenly across 12 months. The first month of year 2 therefore has 25,000 Case capacity, the second month has 26,000, and so on. The 12th month, the end of year 2, has 36,000 Case capacity.

If, during a month, the number of active Cases in the system exceeds the Case capacity, a charge is made for each additional Case for that month. If the number of archive Cases exceeds the archive Case capacity, a charge is made for each additional archive Case. However, if the active Case total is less than the capacity, the spare capacity of active Cases is used to reduce the number of additional archive Cases.

For example, during a month that has 2,000 active Case capacity and 4,000 archive Case capacity:

- Up to 2,000 active Cases and up to 4,000 archive Cases exist: no additional charge
- 2,100 active Cases and up to 4,000 archive Cases: monthly charge for 100 additional active Cases
- 1,800 active Cases and 4,200 archive Cases: no charge, as the unused capacity of 200 active Cases offsets the over-capacity of 200 archive Cases
- 1,800 active Cases and 4,300 archive Cases: monthly charge for 100 additional archive Cases

Included monthly System Case Capacity breakdown as follows:

	Month	Active cases in system	Archived cases in system		Month	Active cases in system	Archived cases in system
Year 1	1	10,000	583	Year 2	13	24,000	9,000
	2	10,000	1,167		14	24,000	11,000
	3	11,250	1,750		15	24,000	13,000
	4	12,667	2,333		16	24,000	15,000
	5	14,083	2,917		17	24,000	17,000
	6	15,500	3,500		18	24,000	19,000

	7	16,917	4,083		19	24,000	21,000
	8	18,333	4,667		20	24,000	23,000
	9	19,750	5,250		21	24,000	25,000
	10	21,167	5,833		22	24,000	27,000
	11	22,583	6,417		23	24,000	29,000
	12	24,000	7,000		24	24,000	31,000

	Month	Active cases in system	Archived cases in system		Month	Active cases in system	Archived cases in system
Year 3	25	24,000	31,833	Year 4	37	24,000	41,833
	26	24,000	32,667		38	24,000	42,667
	27	24,000	33,500		39	24,000	43,500
	28	24,000	34,333		40	24,000	44,333
	29	24,000	35,167		41	24,000	45,167
	30	24,000	36,000		42	24,000	46,000
	31	24,000	36,833		43	24,000	46,833
	32	24,000	37,667		44	24,000	47,667
	33	24,000	38,500		45	24,000	48,500
	34	24,000	39,333		46	24,000	49,333
	35	24,000	40,167		47	24,000	50,167
	36	24,000	41,000		48	24,000	51,000

	Month	Active cases in system	Archived cases in system		Month	Active cases in system	Archived cases in system
Year 5	49	24,000	51,833	Year 6	61	24,000	61,225
	50	24,000	52,667		62	24,000	61,450
	51	24,000	53,500		63	24,000	61,675
	52	24,000	54,333		64	24,000	61,900
	53	24,000	55,167		65	24,000	62,125
	54	24,000	56,000		66	24,000	62,350
	55	24,000	56,833		67	24,000	62,575
	56	24,000	57,667		68	24,000	62,800
	57	24,000	58,500		69	24,000	63,025
	58	24,000	59,333		70	24,000	63,250
	59	24,000	60,167		71	24,000	63,475
	60	24,000	61,000		72	24,000	63,700

	Month	Active cases in system	Archived cases in system
Year 7	73	24,000	63,817
	74	24,000	63,933

75	24,000	64,050
76	24,000	64,167
77	24,000	64,283
78	24,000	64,400
79	24,000	64,517
80	24,000	64,633
81	24,000	64,750
82	24,000	64,867
83	24,000	64,983
84	24,000	65,100

(Rest of Page Intentionally Left Blank)

EXHIBIT C – INDEMNIFICATION AND INSURANCE REQUIREMENTS

INDEMNIFICATION

CONTRACTOR agrees to indemnify, defend (with counsel reasonably approved by COUNTY) and hold harmless COUNTY and its officers, officials, employees, agents and volunteers from and against any and all third party claims, actions, losses, damages, judgments and/or liabilities arising out of this Agreement from any cause whatsoever, including the acts, errors or omissions of any person or entity and for any costs or expenses (including but not limited to attorneys' fees) arising in connection with, any of the following: (i) the gross negligent acts or omissions, willful misconduct and/or fraud of or on behalf of CONTRACTOR or any of its Affiliates or their respective Personnel, or anyone for whose acts any of them may be liable; (ii) bodily injury or death, damage to tangible personal or real property or any other related damage; (iii) any breach of any Applicable Law by CONTRACTOR or any of CONTRACTOR's Personnel; (iv) any CONTRACTOR's Personnel, CONTRACTOR Affiliates or Subcontractors asserting rights or claims under the Agreement; and (v) Claim alleging the infringement of such third party's U.S. patent or copyright by the Services or Software. The foregoing indemnity shall not apply if the infringement arises out of: (a) specifications or designs furnished by COUNTY and implemented by CONTRACTOR at COUNTY's request; (b) the Services or Software being modified by, combined with, added to, interconnected with or used with any equipment, apparatus, device, data, software or service not supplied or approved by NICE in writing; (c) the modification to Services or Software by any person or entity other than CONTRACTOR; or (d) use of Services or Software other than in accordance with its Documentation.,. CONTRACTOR'S indemnification obligation applies to the extent of COUNTY'S sole negligence or willful misconduct.

NOTIFICATION OF ACCIDENTS AND SURVIVAL OF INDEMNIFICATION PROVISIONS

CONTRACTOR shall notify COUNTY immediately in the event of any accident or injury arising out of or in connection with this Agreement. The indemnification provisions in this Agreement shall survive any expiration or termination of this Agreement.

INSURANCE

CONTRACTOR shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the CONTRACTOR, its agents, representatives, employees or subcontractors.

A. Minimum Scope of Insurance
Coverage shall be at least as broad as:

1. **Commercial General Liability (CGL):** Insurance covering CGL on an "occurrence" basis, including products-completed operations, personal & advertising injury, with limits of $1,000,000 per occurrence and $2,000,000 in the aggregate.

2. **Automobile Liability:** Insurance covering, Code 1 (any auto), or if CONTRACTOR has no owned autos, Code 8 (hired) and 9 (non-owned), with limit of $1,000,000 per accident for bodily injury and property damage.

3. **Workers' Compensation:** Insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of $1,000,000 per accident for bodily injury or disease. **(Not required if CONTRACTOR provides written verification that it has no employees)**

4. **Errors and Omissions** Insurance appropriate to the CONTRACTOR'S profession, with limit of $1,000,000 per occurrence or claim, $2,000,000 aggregate.

5. **Cyber Liability Insurance:** Cyber Liability Insurance, included in the E&O policy with limits of $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the CONTRACTOR in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data

recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

B. Other Insurance Provisions

The insurance policies are to contain, or be endorsed to contain, the following provisions:

1. **Additional Insured** – COUNTY, its officers, officials, employees, agents and volunteers are to be covered as additional insureds on the CGL policy but only to the extent of liabilities falling within CONTRACTOR's indemnity obligations pursuant to the terms of this Agreement. General liability coverage can be provided in the form of an endorsement to the CONTRACTOR'S insurance at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10 and CG 20 37 if a later edition is used).

2. **Primary Coverage** – For any claims related to this Agreement, the CONTRACTOR's Commercial General Liability insurance coverage shall be primary insurance as respects the COUNTY, its officers, officials, employees, agents and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, officials, employees, agents or volunteers shall be excess of the CONTRACTOR'S insurance and shall not contribute with it.

3. **Notice of Cancellation** –

4. **Waiver of Subrogation Rights** – To the extent permitted by law, CONTRACTOR will require its insurer(s) issuing the CGL / WC coverage to waive its rights of recovery or subrogation against the COUNTY, but only to the extent of liabilities falling within CONTRACTOR's indemnity obligations under this Agreement.

5. **Deductibles and Self-Insured Retention** –The COUNTY may require the CONTRACTOR to purchase coverage with a lower deductible or retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention.

6. **Acceptability of Insurers** – Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California.

7. **Verification of Coverage** – CONTRACTOR shall furnish the COUNTY with certificates of insurance and amendatory endorsements as required by this Agreement. The certificates and endorsements are to be received and approved by the COUNTY before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the CONTRACTOR'S obligation to provide them. The CONTRACTOR shall furnish evidence of renewal of coverage throughout the term of the Agreement.

8. **Failure to Procure Coverage** – In the event that any policy of insurance required under this Agreement does not comply with the requirements, is not procured, or is canceled and not replaced, COUNTY has the right but not the obligation or duty to terminate the Agreement. Maintenance of required insurance coverage is a material element of the Agreement and failure to maintain or renew such coverage or to provide evidence of renewal may be treated by COUNTY as a material breach of contract.

9. **Subcontractors** – CONTRACTOR shall require and verify that all subcontractors maintain insurance usual and customary for the product or service provided.

10. **Claims Made Policies** – If any of the required policies provide coverage on a claims-made basis:
i. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.

ii. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of contract work.

iii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the CONTRACTOR must purchase "extended reporting" coverage for a minimum of five (5) years after completion of contract work.

11. Special Risks or Circumstances – COUNTY reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Agreement. CONTRACTOR agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of COUNTY to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of COUNTY.

(Rest of Page Intentionally Left Blank)

EXHIBIT D - HIPAA BUSINESS ASSOCIATE AGREEMENT (BAA)

This Business Associate Agreement ("BAA") supplements and is made a part of the Agreement between COUNTY (referred to herein as "Covered Entity") and CONTRACTOR (referred to herein as "Business Associate").

RECITALS

Covered Entity wishes to disclose certain information to Business Associate pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI") (defined below).

Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH Act"), and 45 CFR Parts 160 and 164, Subpart C (the "Security Rule"), Subpart D (the "Data Breach Notification Rule") and Subpart E (the "Privacy Rule") (collectively, the "HIPAA Regulations").

As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require Covered Entity to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations (C.F.R.) and contained in this BAA.

In consideration of the mutual promises below and the exchange of information pursuant to this BAA, the parties agree as follows:

A   Definitions

1.   Breach shall have the meaning given to such term under the HITECH Act [42 U.S.C. Section 17921].

2.   Business Associate shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.

3.   Covered Entity shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

4.   Data Aggregation shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

5.   Designated Record Set shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

6.   Electronic Protected Health Information means Protected Health Information that is maintained in or transmitted by electronic media.

7.   Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

8.   Health Care Operations shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

9.   Privacy Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

10. Protected Health Information or PHI means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].

11. Protected Information shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on Covered Entity's behalf.

12. Security Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

13. Unsecured PHI shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

B. Obligations of Business Associate

1. Permitted Uses. Business Associate shall not use Protected Information except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and this BAA. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by Covered Entity. However, Business Associate may use Protected Information (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for Data Aggregation purposes for the Health Care Operations of Covered Entity [45 C.F.R. Sections 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].

2. Permitted Disclosures. Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and this BAA. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by Covered Entity. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Information, to the extent the third party has obtained knowledge of such breach [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

3. Prohibited Uses and Disclosures. Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates [42 U.S.C. Section 17935(a)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act, 42 U.S.C. section 17935(d)(2); however, this prohibition shall not affect

payment by Covered Entity to Business Associate for services provided pursuant to the Agreement. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement, the BAA, or the HIPAA Regulations.

4. Appropriate Safeguards. Business Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Agreement or this BAA, including, but not limited to, administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, in accordance with 45 C.F.R. Sections 164.308, 164.310, and 164.312. [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. Business Associate shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. Section 164.316 [42 U.S.C. Section 17931].

5. Reporting of Improper Access, Use or Disclosure. Business Associate shall report to Covered Entity in writing of any access, use or disclosure of Protected Information not permitted by the Agreement and this BAA, and any Breach of Unsecured PHI, as required by the Data Breach Notification Rule, of which it becomes aware without unreasonable delay and in no case later than 60 calendar days after discovery [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)].

6. Business Associate's Subcontractors and Agents. Business Associate shall ensure that any agents and subcontractors to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI and implement the safeguards required by paragraph (c) above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. Business Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e)(1)).

7. Access to Protected Information. To the extent that the Covered Entity keeps a designated record set then Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within five (5) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under state law [Health and Safety Code Section 123110] and the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 CF.R. Section 164.504(e)(2)(ii)(E)]. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e).

8. Amendment of PHI for Business Associate who is Required to Maintain a Record Set. If Business Associate is required to maintain a designated record set on behalf of the Covered Entity the Business Associate shall within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity [45 C.F.R. Section 164.504(e)(2)(ii)(F)].

9. Accounting Rights. Within ten (10) days of notice by Covered Entity of a request for an accounting of disclosures of Protected Information, Business Associate and its agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R.

Section 164.528, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c), as determined by Covered Entity. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that Business Associate maintains an electronic health record and is subject to this requirement. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall within five (5) days of a request forward it to Covered Entity in writing. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in Sections B.2 of this BAA [45 C.F.R. Sections 164.504(e)(2)(ii)(G) and 165.528]. The provisions of this subparagraph shall survive the termination of this Agreement.

10. Governmental Access to Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services (Secretary) for purposes of determining Business Associate's compliance with the Privacy Rule [45 C.F.R. Section 164.504(e)(2)(ii)(H)]. Business Associate shall provide to Covered Entity a copy of any Protected Information that Business Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary.

11. Minimum Necessary. Business Associate (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use, or disclosure [42 U.S.C. Section 17935(b); 45 C.F.R. Section 164.514(d)(3)]. Business Associate understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

12. Data Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information.

13. Business Associate's Insurance. Business Associate represents and warrants that it purchases commercial insurance to cover its exposure for any claims, damages or losses arising as a result of a breach of the terms of this BAA.

14. Notification of Possible Breach. During the term of the Agreement, Business Associate shall notify Covered Entity within twenty-four (24) hours of any suspected or actual breach of security, or any access, use or disclosure of Protected Information not permitted by the Agreement or this BAA or unauthorized use or disclosure of PHI (each of the foregoing, a "breach") of which Business Associate becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. A breach shall be treated as discovered by Business Associate, and Business Associate shall be deemed to be aware of a breach, as of the first day on which such breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate Business Associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of Business Associate (determined in accordance with the Federal common law of agency). Business Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations. [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section164.308(b)]

Breach Pattern or Practice by Covered Entity. Pursuant to 42 U.S.C. Section 17934(b), if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach

or violation of the Covered Entity's obligations under the Agreement or this BAA or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Agreement or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary. Business Associate shall provide written notice to Covered Entity of any pattern of activity or practice of the Covered Entity that Business Associate believes constitutes a material breach or violation of the Covered Entity's obligations under the Agreement or this BAA or other arrangement within five (5) days of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

Audits, Inspection and Enforcement. Within ten (10) days of a written request by Covered Entity, Business Associate and its agents or subcontractors shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this BAA for the purpose of determining whether Business Associate has complied with this BAA; provided, however, that (i) Business Associate and Covered Entity shall mutually agree in advance upon the scope, timing and location of such an inspection,(ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with this BAA, nor does Covered Entity's (i) failure to detect or (ii) detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the Agreement or this BAA, Business Associate shall notify Covered Entity within ten (10) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.

C. Termination

1. Material Breach. A breach by Business Associate of any provision of this BAA, as determined by Covered Entity, shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement, any provision in the Agreement to the contrary notwithstanding [45 C.F.R. Section 164.504(e)(2)(iii)].

2. Judicial or Administrative Proceedings. Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

3. Effect of Termination. Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by Covered Entity, Business Associate shall continue to extend the protections of Section B of this BAA to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. [45 C.F.R. Section 164.504(e)(ii)(2(I)]. If Covered Entity elects destruction of the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

D. Indemnification

If Business Associate fails to adhere to any of the privacy, confidentiality, and/or data security provisions set

forth in this BAA or if there is a Breach of PHI in Business Associate's possession and, as a result, PHI or any other confidential information is unlawfully accessed, used or disclosed, Business Associate agrees to reimburse Covered Entity for any and all costs, direct or indirect, incurred by Covered Entity associated with any Breach notification obligations. Business Associate also agrees to pay for any and all fines and/or administrative penalties imposed for such unauthorized access, use or disclosure of confidential information or for delayed reporting if it fails to notify the Covered Entity of the Breach as required by this BAA.

E.   Disclaimer

Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

F.   Certification

To the extent that Covered Entity determines that such examination is necessary to comply with Covered Entity's legal obligations pursuant to HIPAA relating to certification of its security practices, Covered Entity or its authorized agents or contractors, may, at Covered Entity's expense, examine Business Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to Covered Entity the extent to which Business Associate's security safeguards comply with HIPAA, the HITECH Act, the HIPAA Regulations or this BAA.

G.   Amendment to Comply with Law

The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Agreement or this BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that Covered Entity must receive satisfactory written assurance from Business Associate that Business Associate will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule or other applicable laws. Covered Entity may terminate the Agreement upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend the Agreement or this BAA when requested by Covered Entity pursuant to this Section or (ii) Business Associate does not enter into an amendment to the Agreement or this BAA providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

H.   Assistance in Litigation of Administrative Proceedings

Business Associate shall make itself, and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement or this BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is named adverse party.

I.   No Third-Party Beneficiaries
Nothing express or implied in the Agreement or this BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any

rights, remedies, obligations or liabilities whatsoever.

J. Effect on Agreement

Except as specifically required to implement the purposes of this BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

K. Entire Agreement of the Parties

This BAA supersedes any and all prior and contemporaneous business associate agreements between the parties and constitutes the final and entire agreement between the parties hereto with respect to the subject matter hereof. Covered Entity and Business Associate acknowledge that no representations, inducements, promises, or agreements, oral or otherwise, with respect to the subject matter hereof, have been made by either party, or by anyone acting on behalf of either party, which are not embodied herein. No other agreement, statement or promise, with respect to the subject matter hereof, not contained in this BAA shall be valid or binding.

L. Interpretation

The provisions of this BAA shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this BAA. This BAA and the Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

Federal Clauses
Exhibit E

<u>Additional Federal Clauses Applicable for Federal Funding under this Agreement:</u> (2 CFR §

200.326; 2 CFR Part 200, Appendix II, Required Contract Clauses)

1. REMEDIES FOR NONCOMPLIANCE

In the event COUNTY determines, in its sole discretion, that CONTRACTOR is not in compliance with the terms and conditions set forth herein, COUNTY may:

A. Require payments as reimbursements rather than advance payments;

B. Withhold authority to proceed to the next phase until receipt of evidence of acceptable performance within a given period of performance;

C. Require additional, more detailed financial reports;

D. Require additional project monitoring;

E. Requiring CONTRACTOR to obtain technical or management assistance; or

F. Establish additional prior approvals.

2. EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this Agreement, CONTRACTOR agrees as follows:

A. CONTRACTOR will not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin. CONTRACTOR will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. CONTRACTOR agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

B. CONTRACTOR will, in all solicitations or advertisements for employees placed by or on behalf of CONTRACTOR, state that all qualified applicants will receive considerations for employment without regard to race, color, religion, sex, or national origin.

C. CONTRACTOR will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of CONTRACTOR'S commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

D. CONTRACTOR will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

E. CONTRACTOR will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the

administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

F. In the event of CONTRACTOR'S noncompliance with the nondiscrimination clauses of this Agreement or with any of the said rules, regulations, or orders, this Agreement may be canceled, terminated, or suspended in whole or in part and CONTRACTOR may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions as may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

G. CONTRACTOR will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (7) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. CONTRACTOR will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance: Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency CONTRACTOR may request the United States to enter into such litigation to protect the interests of the United States.

3. CLEAN AIR ACT

A. CONTRACTOR agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

B. CONTRACTOR agrees to report each violation to the California Environmental Protection Agency and understands and agrees that the California Environmental Protection Agency will, in turn, report each violation as required to assure notification to the COUNTY, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

C. CONTRACTOR agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

4. FEDERAL WATER POLLUTION CONTROL ACT

A. CONTRACTOR agrees to comply with all applicable standards, orders or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

B. CONTRACTOR agrees to report each violation to the California State Water Resources Control Board and understands and agrees that the California State Water Resources Control Board will, in turn, report each violation as required to assure notification to the COUNTY, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

C. CONTRACTOR agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

5. DEBARMENT AND SUSPENSION

    A. CONTRACTOR certifies to COUNTY that it and its employees and principals are not debarred, suspended, or otherwise excluded from or ineligible for, participation in federal, state, or county government contracts. CONTRACTOR certifies that it shall not contract with a subcontractor that is so debarred or suspended.

    B. This certification is a material representation of fact relied upon by COUNTY. If it is later determined that CONTRACTOR did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the California Governor's Office of Emergency Services and COUNTY, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

    C. This Agreement is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such CONTRACTOR is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

    D. CONTRACTOR must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

    E. CONTRACTOR shall to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. CONTRACTOR further agrees to include a provision requiring such compliance in its lower tier covered transactions.

6. BYRD ANTI-LOBBYING AMENDMENT, 31 U.S.C. § 1352 (AS AMENDED)

    CONTRACTOR shall file the required certification attached as Exhibit , *Certification for Contracts, Grants, Loans, and Cooperative Agreement (Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (As Amended)*, which is incorporated herein by this reference. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient.

7. PROCUREMENT OF RECOVERED MATERIALS

    A. A. In the performance of this Agreement, CONTRACTOR shall make maximum use of products containing recovered materials that are EPA- designated items unless the product cannot be acquired—

        i. Competitively within a timeframe providing for compliance with the contract performance schedule;

        ii. Meeting contract performance requirements; or

        iii. At a reasonable price.

    B. Information about this requirement, along with the list of EPA-designate items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program.

8. <u>CHANGES</u>

   A. Notice. The primary purpose of this clause is to obtain prompt reporting of COUNTY conduct that CONTRACTOR considers to constitute a change to this contract. Except for changes identified as such in writing and signed by COUNTY, the Contractor shall notify the COUNTY in writing promptly, within five (5) calendar days from the date that the Contractor identifies any Government conduct (including actions, inactions, and written or oral communications) that the CONTRACTOR regards as a change to the contract terms and conditions. On the basis of the most accurate information available to the Contractor, the notice shall state

      i. The date, nature, and circumstances of the conduct regarded as a change;

      ii. The name, function, and activity of each Government individual and CONTRACTOR official or employee involved in or knowledgeable about such conduct;

      iii. The identification of any documents and the substance of any oral communication involved in such conduct;

      iv. In the instance of alleged acceleration of scheduled performance or delivery, the basis upon which it arose;

      v. The particular elements of contract performance for which CONTRACTOR may seek an equitable adjustment under this clause, including:

- What line items have been or may be affected by the alleged change;

- What labor or materials or both have been or may be added, deleted, or wasted by the alleged change;

- To the extent practicable, what delay and disruption in the manner and sequence of performance and effect on continued performance have been or may be caused by the alleged change;

- What adjustments to contract price, delivery schedule, and other provisions affected by the alleged change are estimated; and

      vi. CONTRACTOR'S estimate of the time by which COUNTY must respond to CONTRACTOR'S notice to minimize cost, delay or disruption of performance.

   B. Continued Performance. Following submission of the required notice, CONTRACTOR shall diligently continue performance of this Agreement to the maximum extent possible in accordance with its terms and conditions as construed by the CONTRACTOR.

   C. COUNTY Response. COUNTY shall promptly, within ten (10) calendar days after receipt of notice, respond to the notice in writing. In responding, COUNTY shall either--

      i. Confirm that the conduct of which CONTRACTOR gave notice constitutes a change and when necessary direct the mode of further performance;

      ii. Countermand any communication regarded as a change;

      iii. Deny that the conduct of which CONTRACTOR gave notice constitutes a change and when necessary direct the mode of further performance; or

      iv. In the event the Contractor's notice information is inadequate to make a decision, advise CONTRACTOR what additional information is required, and establish the date by which it should be furnished and the date thereafter by which COUNTY will respond.

D. Equitable Adjustments.

    i. If the COUNTY confirms that COUNTY conduct effected a change as alleged by the CONTRACTOR, and the conduct causes an increase or decrease in the CONTRACTOR'S cost of, or the time required for, performance of any part of the work under this Agreement, whether changed or not changed by such conduct, an equitable adjustment shall be made --

- In the contract price or delivery schedule or both; and

- In such other provisions of the Agreement as may be affected.

    ii. The Agreement shall be modified in writing accordingly. The equitable adjustment shall not include increased costs or time extensions for delay resulting from CONTRACTOR'S failure to provide notice or to continue performance as provided herein.

9. ACCESS TO RECORDS

The following access to records requirements apply to this Agreement:

A. CONTRACTOR agrees to provide COUNTY, the California Governor's Office of Emergency Services, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the CONTRACTOR which are directly pertinent to this Agreement for the purposes of making audits, examinations, excerpts, and transcriptions.

B. CONTRACTOR agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

C. CONTRACTOR agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the Agreement.

10. USE OF U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) LOGO

CONTRACTOR shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre- approval

11. COMPLIANCE WITH FEDERAL LAWS, REGULATIONS, AND EXECUTIVE ORDERS

This is an acknowledgement that FEMA financial assistance will be used to fund this Agreement. CONTRACTOR will only use FEMA funds as authorized herein. CONTRACTOR will comply will all applicable federal law, regulations, executive orders, FEMA policies, procedures, and directives.

12. NO OBLIGATION BY FEDERAL GOVERNMENT

The Federal Government is not a party to this Agreement and is not subject to any obligations or liabilities to the non-Federal entity, CONTRACTOR, or any other party pertaining to any matter resulting from the Agreement.

13. PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS OR RELATED ACTS

CONTRACTOR acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the CONTRACTOR'S actions pertaining to this Agreement.

14. MANDATORY DISCLOSURE

CONTRACTOR must disclose, in a timely manner, in writing to the COUNTY all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the award. CONTRACTOR is required to report certain civil, criminal, or administrative proceedings to the System for Award Management (SAM) located at www.sam.gov. Failure to make required disclosures can result in any of the remedies described in 2 CFR §200.338 Remedies for noncompliance, including suspension or debarment. (See also 2 CFR part 180 and 31 U.S.C.3321.)

15. DOMESTIC PREFERENCES FOR PROCUREMENTS

A. As appropriate and to the extent consistent with law, the CONTRACTOR should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all subcontractor agreements.

B. For purposes of this section:

    i.   "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

    ii.   "Manufactured products" means items and construction materials composed in whole or in part of nonferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

<u>EXHIBIT F - CERTIFICATION FOR CONTRACTS, GRANTS, LOANS, AND COOPERATIVE AGREEMENTS</u>
(Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (As Amended))

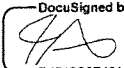The undersigned CONTRACTOR certifies, to the best of his or her knowledge, that:

<u>No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.</u>

If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form- LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
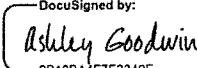
The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31, U.S.C. § 1352 (as amended by the Lobbying Disclosure Act of 1995). Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

CONTRACTOR certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, CONTRACTOR understands and agrees that the provisions of 31 U.S.C. § 3801 et seq., apply to this certification and disclosure, if any.

DocuSigned by:

[signature] D4212C6E49AB4B1...   [signature: Ashley Goodwin] 9B18BA4F7E3349E...

Signature of Contractor's Authorized Official
John Rennie   Ashley Goodwin

General Manager, Public Safety Finance, Americas

Name and Title of Contractor's Authorized Official

12/9/2024 | 7:54 AM PST   12/9/2024 | 12:09 PM EST

Date

66