ATTACHMENT B

PROPOSED CLASS SPECIFICATION FOR

ASSISTANT DIRECTOR OF INFORMATION TECHNOLOGY/

CHIEF INFORMATION SECURITY OFFICER

COUNTY OF SANTA BARBARA

ASSISTANT DIRECTOR IT/CHIEF INFORMATION SECURITY OFFICER

DEFINITION

Under general direction of the Director of Information Technology, directs the Countywide information security programs designed to provide the protection and confidentiality of data, along with other information assets of the County of Santa Barbara, and performs other related duties as required. Oversees Information Technology (IT) Department operational divisions, as assigned. As a member of the Information Technology Department's executive staff, this classification may be assigned to perform the duties of the Director of Information Technology or other executive-level position in the department in the absence of the incumbent(s).

DISTINGUISHING CHARACTERISTICS

The Assistant Director of Information Technology /Chief Information Security Officer (CISO) is a single executive-level position classification and reports to the Director of Information Technology. The Assistant Director of IT/CISO is distinguished from the Assistant Director of Information Technology classification by having countywide responsibility for formulating and promulgating policy for, and developing, managing, and integrating countywide information security and privacy related programs designed to protect all County information systems and data. The Assistant Director of IT/CISO directs and supports countywide information security and related privacy efforts through departmental information security professionals, requiring strong organizational and team leadership skills to facilitate interdepartmental compliance and to ensure departmental IT security staff fully integrate appropriate security and privacy practices.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from the Director of Information Technology. Exercises direct supervision of departmental IT staff.

EXAMPLES OF DUTIES:

These examples are not intended to reflect all duties performed within the job.

1. Oversees the development and implementation of Countywide information security policies and procedures to protect the County from internal and external IT threats and vulnerabilities.
2. Represents the CISO to County departments, information technology advisory bodies, and other committees or agencies involving County policies, plans, methodologies, roles, and programs related to security, privacy, and confidentiality of data and information technology assets.
3. Chairs the countywide Information Security Committee; advises and supports departmental information security professionals responsible for overall department compliance with healthcare (including HIPAA), criminal justice, financial and personnel-related informational privacy protections related to their functional areas; monitors industry trends and best practices and disseminates this information to other information security professionals; monitors and reports to the Information Technology Director and County Executive Officer on the status of information

security risks and response readiness across departments countywide; and may oversee departmental information security audits, as directed.

4. Directs the preparation of short and long-term strategies for optimizing the County's information security plan, and formulates and recommends Countywide policies for detecting, deterring, and mitigating information security threats.
5. Directs and participates in the identification of security risks, development, and implementation of security management practices, and the measurement and monitoring of security protection measures.
6. Directs the handling of information security breaches and related incidents, including overseeing the activation of incident response teams, and acts as the central point of contact for IT-related incidents or violations.
7. Conducts security risk assessments and business impact analyses across all County departments to ensure a comprehensive countywide IT security posture.
8. Serves as a subject matter expert and internal consultant on the data security implications of proposed new major information technology projects and programs, and makes recommendations to the Board of Supervisors and affected departments regarding computer operations, logical access controls, system development, and data communications security.
9. Reviews and recommends the professional development curriculum for County IT security and privacy staff to ensure adequate and appropriate training standards in information security and protection measures and coordinate related training and awareness programs.
10. Directs the development and promotion of security and privacy awareness training and education for all levels of the County organization structure on an ongoing basis.
11. Develops effective disaster recovery and business continuity policies, standards, and implementation plans to ensure appropriate IT security measures are addressed and business-critical services are recovered in the event of a declared disaster.
12. Leads the development, implementation, and compliance monitoring of IT security agreements, business associate agreements, chain-of-trust agreements, and Memoranda of Understanding (MOUs) involving access to or exchange of County information to ensure all security concerns are addressed, including compliance processes for areas such as HIPAA, Criminal Justice Information Systems (CJIS), and other federal and state privacy requirements.
13. Leads vendor activities, writes evaluate proposals, and negotiates contracts for Countywide information security related software, equipment, and services, and presents recommendations for funding and approvals.
14. Performs assigned duties consistent with the classification of Assistant Director of Information Technology including, but not limited to, planning, directing, managing, supervising, and coordinating daily activities and operations of the IT Department including coordination of departmental policy, budgetary, personnel and workload matters, representing the Department to the Board of Supervisors, other departments, agencies, private organizations, and others; acts for the Director when required; and performs related duties as assigned.
15. Selects, trains, motivates, and evaluates assigned personnel; provides or coordinates staff training; works with employees on performance issues; responds to staff questions and concerns; makes discipline recommendations to the Director of IT.
16. Maintains current knowledge of applicable federal and state information security laws and standards to facilitate County adaptation and compliance.

MINIMUM QUALIFICATIONS

Education and Experience

The knowledge, skills, and abilities listed below may be acquired through various types of training, education, and experience. A typical way to acquire the required knowledge and abilities would be:

- Equivalent of a bachelor's degree from an accredited four-year college or university in computer science, information technology, information security, management information systems (MIS), electronics engineering, voice or data communications, public or business administration, or a related field; and
- Seven (7) years of progressively responsible management experience that includes two (2) years of experience as a Chief Information Security Officer or equivalent role concentrated on information security, and four (4) years of which have included the management of a full-service information technology division or department including the oversight of major programs and the supervision of staff.

Licenses and Certificates

One or more of the following certifications is preferred:

- National Institute of Standards and Technology (NIST)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Cloud Security Professional (CCSP)

Possession and maintenance of a valid California driver's license and the ability to meet automobile insurability requirements of the County or the ability to provide suitable transportation needs as a condition of continued employment.

Knowledge of: County information system resources and applications. Modern information technology solutions, concepts, and methods. Standard security practices, network architecture, routing and Transmission Control Protocol/Internet Protocol (TCP/IP) protocols; risk and threat assessment processes and practices; business continuity planning, documentation, and evaluation; managing the evidentiary process; the use of third party applications and native scripts and languages; maintaining the chain-of-custody process and procedures; applicable federal, state, and local cybersecurity laws, codes, regulations, and standards, including data protection laws, HIPAA data security, and emerging cybersecurity regulations and policy issues; principles and methods used in the analysis and development of information security systems and procedures; currently accepted information security standards, guidelines, and theories; and advanced computer technology equipment operation, capacity, and capability; general healthcare, criminal justice, financial, personnel and other applicable information privacy protections; California Public Records Act.

Principles and practices of leadership, motivation, team building, and conflict resolution; Administrative principles and practices, including goal setting, program development, implementation, evaluation, and supervision of staff; Public agency budget development, contract administration, County-wide administrative practices, and general principles of risk management related to the functions of the

assigned area; organizational and management practices as applied to the analysis and evaluation of projects, programs, policies, procedures, and operational needs, and principles and practices of county government administration; methods and techniques for the development of presentations, contract negotiations, business correspondence, and information distribution; research and reporting methods, techniques, and procedures; principles and techniques for providing a high level of customer service by effectively working with the public, vendors, contractors, and County staff; principles and techniques of effective oral presentations; applicable federal, state, and local laws, codes, regulations, and standards; Business systems, equipment, and applications relevant to the area of assignment.

Ability to:

Assist in developing and implementing goals, objectives, policies, procedures, work standards, and internal controls for the department and assigned program areas; organize, direct, and implement a variety of programs and services that are conducted by the Information Technology Department; assist in preparing and administering large and complex budgets and allocating limited resources in a cost-effective manner; provide administrative and professional leadership and direction for the department and the County, understand, interpret, apply, explain, and ensure compliance with federal, state, and local policies, procedures, laws, and regulations, plan, organize, direct, and coordinate the work of supervisory, professional, technical, and administrative support staff, and delegate authority and responsibility; select, train, motivate, and evaluate the work of staff and train staff in work procedures; research, analyze, and evaluate new service delivery methods, procedures, and techniques; effectively represent the County and the department in meetings with governmental agencies, contractors, vendors, and various businesses, professional, regulatory, and legislative organizations; conduct complex research projects, evaluate alternatives, make sound recommendations, and prepare effective technical staff reports; understand, interpret, and apply all pertinent laws, codes, regulations, policies and procedures, and standards relevant to work performed; effectively represent the department and the County under diverse circumstances in meetings with individuals, governmental agencies; community groups; and various business, professional, and regulatory organizations; use tact, initiative, prudence, and independent judgment within general policy, procedural, and legal guidelines; establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

ADDITIONAL INFORMATION

May be required to work a varied schedule of hours, which may include evenings, weekends, and holidays.

Completion of a background investigation to the satisfaction of the County may be required for some assignments.