STATE OF CALIFORNIA CYBERSECURITY TASK FORCE WORKFORCE DEVELOPMENT AND TRAINING

Development of a consistent definition and criteria for cybersecurity expertise to serve the State of California.

OBJECTIVE 1

June 2015

If you have questions about this document, please contact:

Gary Dias, CISSP

Department of Health Care Services

Table of Contents

I. EXECUTIVE SUMMARY 1
II. INTRODUCTION 2
III. METHODOLOGY 3
IV. THE THREAT LANDSCAPE 4
V. THE WORKFORCE LANDSCAPE 7
A. CHALLENGES TO RECRUITING AND RETAINING CYBERSECURITY PROFESSIONALS 8
B. CYBERSECURITY ROLES 14
1. CURRENT CALIFORNIA IT ROLES AND COMPETENCIES 14
2. PROPOSED CYBERSECURITY ROLES AND COMPETENCIES 16
C. FUNCTIONAL CATEGORIZATION BY PERSPECTIVE 19
1. COMPETENCY CATEGORIZED BY FUNCTIONAL PERSPECTIVE: CURRENT 20
2. COMPETENCY CATEGORIZED BY FUNCTIONAL PERSPECTIVE: PROPOSED 23
D. CYBERSECURITY CAREER PROGRESSION 30
1. SAMPLE CYBERSECURITY CAREER PROGRESSION 30
2. SAMPLE CYBERSECURITY CAREER LADDER 31
VI. RECOMMENDATIONS 32
VII. NEXT STEPS 33
APPENDIX A: COMPETENCY AND FUNCTIONAL FRAMEWORK: EBK 34
APPENDIX B: NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES:FSA 36
APPENDIX C: A MAPPING of FSA to EBK 39
APPENDIX D: A MAPPING of EBK to FSA 45
APPENDIX E: SAMPLE MINIMUM QUALIFICATIONS 51
APPENDIX F: SAMPLE CLASS SPECIFICATIONS 54
APPENDIX G: COMPENSATION COMPARISON: CYBERSECURITY POSITIONS 66
APPENDIX H: HISTORICAL INFORMATION SECURITY ANALYST SALARIES 67
APPENDIX I: BILLS FOR CYBER SECURITY TASK FORCE CONSIDERATION 69
APPENDIX J: REFERENCES 70
ACKNOWLEDGEMENTS: 71

Figures and Tables

Figure 1 Mapping Diagram: Roles to Competencies to Functions 19
Figure 2: Sample Cybersecurity Career Progression 30
Figure 3: Sample Cybersecurity Career Ladder 31

Table 1: Current California IT Positions Competency & Functional Matrix 28
Table 2: Proposed California IT Positions Competency & Functional Matrix 29

I. EXECUTIVE SUMMARY

The State of California Department of Human Resources states that workforce planning is *having the right number of people with the right skills in the right jobs at the right time. Workforce planning is the business process that aligns staffing with the strategic missions and critical needs of the department. Workforce planning helps departments anticipate and plan for change. A well prepared department attracts, develops, and retains employees with the competencies needed in the future.*

This report illustrates the critical need to create a new classification series for Cybersecurity Professionals. This stems from the urgent need to ensure that the State is capable of recruiting and retaining a highly skilled Cybersecurity Workforce with the skills necessary to: protect the data of our citizens, continue to securely maintain the systems that provide services to our constituents, and protect the information technology infrastructure of our State.

This report makes the following recommendations to support that objective:

1. Create a new Cybersecurity Professional classification - Adopt a new classification series of Cybersecurity Professionals and create a career ladder for highly skilled staff.

    a. A new Cybersecurity classification series allows the State to be competitive in recruiting and retaining Cybersecurity Professionals.

    b. Endeavoring to create a highly skilled Cybersecurity Workforce will garner Union support for this classification series as increased recruitment and retention of Cybersecurity Professionals will reduce the State's dependence on outside vendors and consultants in this highly technical and specialized field.

2. Information Technology (IT) Capital Planning and Security Funding – All IT investments must demonstrate that costs for appropriate IT privacy and security controls and staffing are explicitly incorporated into the life cycle planning of all systems. Budget proposals should also include line items for vulnerability assessments and penetration testing.

3. Information Security training and awareness for all – All personnel who access confidential information are required to complete initial and annual information security and privacy training. Information security training and education needs to be integrated into the classification specifications for ALL State public servants and incorporated into duty statements throughout State service; more attention needs to be placed on role-based security training for information technology classifications.

II. INTRODUCTION

The State of California places a very high priority on information technology (IT) security, recognizing that an effective IT Security Program is necessary to protect its IT investments and its data. Cybersecurity involves the articulation and enforcement of security policies for information and communications systems and the implementation of associated technical solutions, mechanisms, and programs. The security of a system generally reflects not only how well that system was constructed, but also how it is configured, the organizational policies and practices that govern its operation, the degree to which organizational members follow these policies, and the capabilities and interests of potential adversaries.

The effort to establish a safer and more secure cyberspace will require improvement in many areas, including a Cybersecurity Workforce that has the capacity and capability to do the job; better tools and techniques that enhance the efficiency and effectiveness of cybersecurity workers; better tools and approaches for risk identification and assessment; better systems design; better systems-development practices; greater incentives to encourage the deployment of better cybersecurity technologies and practices; improvements in end-user behavior through training; and organizational, industry, national, and international measures to deter bad actors.

The effort to establish a safer and more secure cyberspace will require drastic improvements in many areas, and addressing the rapidly changing environment and threats in the cybersecurity realm requires specialized skillsets to defend against more sophisticated and destructive attacks.

This report focuses on building a Cybersecurity Workforce with the right knowledge, skills, and abilities to protect our State information assets. Competition to hire individuals with these skills comes not only from other State and local government entities, but the United States Federal government and private sector, both within the United States and internationally. In fact, all of the statistics coming from the Federal government and private industry show they are challenged to keep pace with their cybersecurity needs due to the higher demand for highly skilled Cybersecurity Professionals.

The State of California can no longer ignore the dire need for a special classification for Cybersecurity Professionals to protect against the constant and ever-changing threat landscape. It seems that every day the news contains a report about another security breach; against a state department, the Federal government, and even industry-leading corporations that provide security tools worldwide.

III. METHODOLOGY

The workgroup took the following steps in compiling this report:

- **Conducted research and gathered information from a variety of authoritative sources** - including previous studies, whitepapers, and reports that focused on the Cybersecurity Workforce and leveraged insights gleaned from them.
  (Appendix J: References)

- **Reviewed Federal Cybersecurity Workforce framework studies** (Information Technology Security Essential Body of Knowledge (EBK) (Appendix A) and National Initiative for Cybersecurity Education (NICE), Framework Specialty Area (FSA) (Appendix B) - Upon closer examination, the more recently developed FSA framework appears to be in flux and is geared more towards creating a national groundswell for cybersecurity education and professionalism. The EBK framework, in contrast, was more mature and was the foundation for subsequent studies and whitepapers focusing on the State government Cybersecurity Workforce.

- **Created a crosswalk** of EBK and FSA competencies.
  (Appendix C: A Mapping of FSA to EBK and Appendix D: A Mapping of EBK to FSA)

- **Conducted a gap analysis** of job specifications of current IT security staff (Information Systems Analyst and Systems Software Specialist series) versus proposed Cybersecurity Professional classifications.
  (Section V: The Workforce Landscape, Appendix G: Compensation Comparison: Cybersecurity Positions)

- **Developed recommendations** - In further support of this Objective 1 plan, the recommendations from the NICE, National Association of State Chief Information Officers (NASCIO), and the State Government Security Workforce Development, was used to develop a strategy to ensure that the State of California can deploy a Cybersecurity Workforce that can meet the ongoing, and ever-changing, cybersecurity challenges and protect its citizenry.
  (Section VI. Recommendations)

IV. THE THREAT LANDSCAPE

The following examples and excerpts[1] are meant to convey to the reader the overall sense in the country that cyber-attacks are rapidly growing and evolving and that we lack the necessary Cybersecurity Professionals and skillsets to thoroughly protect our systems. Cyber-attacks continue to increase in magnitude from threat actors that include criminal organizations and nation state supported hackers. These threats are becoming more sophisticated and have the potential to impact *any* organization or individual. We have chosen incidents that highlight the far-reaching and enduring consequences a successful attack can have.

The State of California is not exempt from these threats and is facing unprecedented cybersecurity challenges. On a daily basis, state entities face these same threats and are desperately having to defend themselves. There is a dire need to shore up the State's cyber-defenses, and no matter what strategic and tactical approaches are taken, a skilled cybersecurity workforce is a fundamental prerequisite to ensuring the greatest chance of success.

June 4, 2015 Federal Data Compromised at OPM and Interior

Massive breach of federal personnel data at agency handling security clearances.

WASHINGTON (AP) — Hackers broke into the U.S. government personnel office and stole identifying information of at least 4 million federal workers.

The Department of Homeland Security said in a statement Thursday that at the beginning of May, data from the Office of Personnel Management and the Interior Department was compromised.

"The FBI is conducting an investigation to identify how and why this occurred," the statement said.

A U.S. official who declined to be identified said the data breach could potentially affect every federal agency. One key question is whether intelligence agency employee information was compromised.

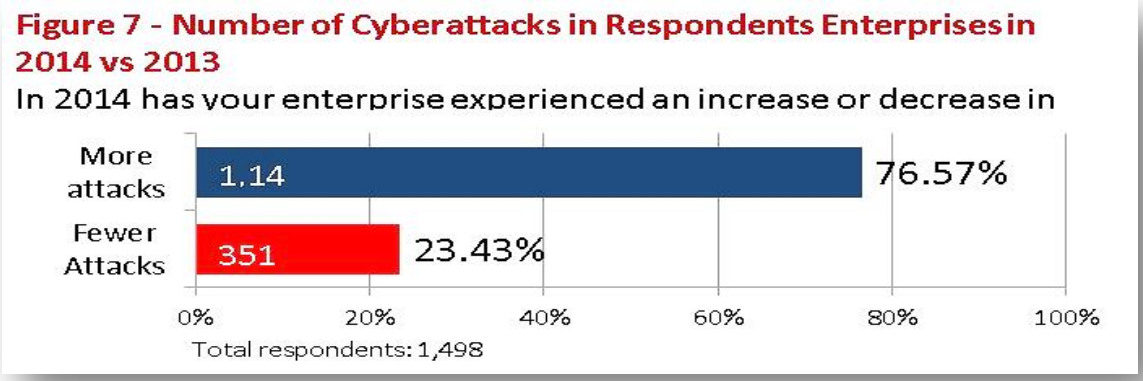
[1] Specific State of California incident metrics have not been included due to the confidential nature of the data.

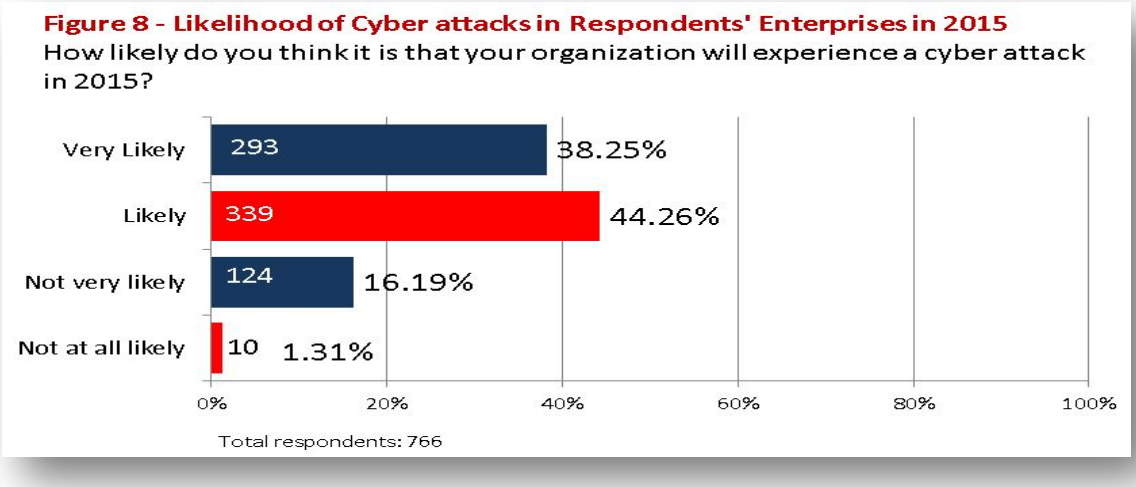
June 11, 2015 Foreign Agents Hack Kaspersky Security Firm

TECH NEWS - In a strange twist of fate, Kaspersky Lab has been attacked by hackers. The company, which is one of the world's largest software security outfits, said Wednesday that the breach was both sophisticated and stealthy, implying that the hackers were working on behalf of a national government.

Threats, State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey

It is no surprise that the cyberthreat is real. Enterprises are finding cyberattacks to have increased in both frequency and impact. More than three-quarters of the survey respondents (77 percent) reported an increase in attacks in 2014 over 2013 (figure 7). Even more—82 percent— predicted that it is "likely" or "very likely" they will be victimized in 2015 (figure 8).





Cybersecurity threats are not slowing down. More than three-quarters of respondents reported an increase in attacks in 2014 over 2013 and they expect the number to rise again in 2015. The report data reveal that almost 25 percent of respondents are experiencing phishing attacks daily and 30 percent are dealing with insider damage and theft of IP at least quarterly. Additionally, the majority (over 82%) of respondents expect to experience a cyberattack in 2015. Enterprises need to address the fact that cybersecurity issues can lead to risk for the business, which could have a very negative effect both financially and reputationally.

It is evident from the previous excerpts how devastating a major breach can have on an organization's reputation and finances. Much more concerning is the potential effects to the millions of individuals whose data has been compromised. The California State government has an obligation to its citizens to practice due diligence in protecting their privacy and must be more assertive and proactive in enhancing its security posture. Training, recruiting, and retaining a skilled workforce is one major step in that direction.

V. THE WORKFORCE LANDSCAPE

This document provides the groundwork to modernize the classification structure and associated position descriptions to address the community needs of the State of California Cybersecurity Workforce. It describes how current State represented classifications are used and provides a recommendation for new State classifications that are more appropriately aligned with the highly specialized skills of cybersecurity functions.

This chapter is divided into four sections:

A. Challenges to Recruiting and Retaining Cybersecurity Professionals
B. Cybersecurity Roles
    1. Current State of California Information Technology Roles
    2. Proposed State of California Cybersecurity Roles
C. Functional Categorization by Perspective
    1. Current State of California Information Technology Roles
    2. Proposed State of California Cybersecurity Roles
D. Cybersecurity Career Progression
    1. Sample Cybersecurity Career Progression
    2. Sample Cybersecurity Career Ladder

A. CHALLENGES TO RECRUITING AND RETAINING CYBERSECURITY PROFESSIONALS

The National Initiative for Cybersecurity Education (NICE) developed the Workforce Framework to categorize and define cybersecurity work; led by the Department of Homeland Security (DHS), NICE raises public awareness, provides a foundation for the recruitment, training, and retention of Cybersecurity Professionals, and promotes cybersecurity education.

Concurrently, the National Association of State Chief Information Officers (NASCIO) released a report:

NASCIO State IT Workforce: Facing Reality with Innovation, 2015 President's Initiative

"Likewise, as cybersecurity continues to be the most pressing issue for CIOs, there is a real challenge to recruit and retain cyber professionals with the skill sets needed for effective cybersecurity protection. Growth in cyber managed services, for example, is also skyrocketing as outsourcing has become more accepted." [2] *(Page 2)*

"Perhaps the most eye-opening observation in the entire set of responses is the following: when asked if the state's salary rates and pay grade structures present a challenge in attracting and retaining IT talent, an overwhelming 91.8% answered yes. What intensifies the severity of this response is that in the 2011 NASCIO workforce report, 78.6% answered yes." (Page 9).

"When states were asked which skills and disciplines present the greatest challenges in attracting and retaining IT employees, application development, programming and support received 57.1%; architecture received 55.1%, while security was the top answer with 67.3%." (Page 10)

"The fact that security was the top response is not surprising. In the 2014 Deloitte-NASCIO Cybersecurity Study State Governments at Risk: Time to move forward, nine in ten respondents reported the biggest challenge in attracting talent to state cybersecurity positions comes down to salary." (Page 11)

[2] Deloitte/NASCIO 2014 Study: State Governments at Risk: Time to move forward
http://www.nascio.org/DeloitteNASCIO2014CybersecurityStudy/

Cybersecurity Workforce Handbook, A Practical Guide to Managing Your Workforce, Council on CyberSecurity October 2014

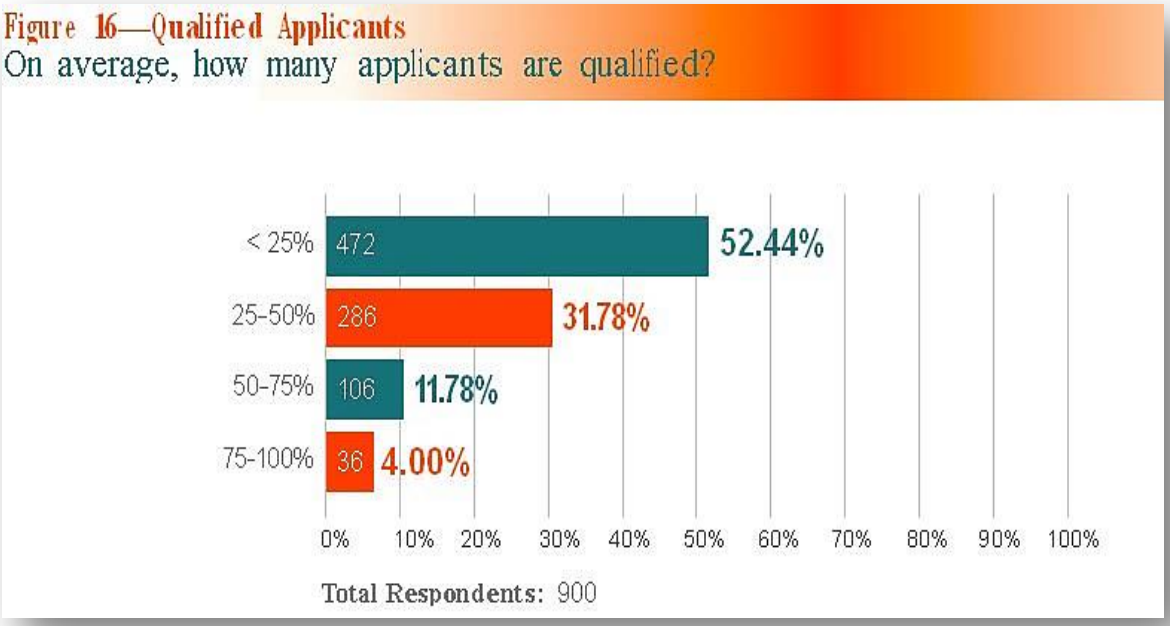
A defining characteristic of well-secured enterprises is the involvement of highly capable, technically sophisticated Cybersecurity Professionals who possess the right mix of knowledge, skills, and abilities to identify, protect, detect, respond, and recover from cyber attacks. There is a tremendous need for, and painful shortage of, Cybersecurity Professionals who can bring to bear hands-on skills to counter the sophisticated and ever-evolving threats presented by other highly-capable and technically sophisticated, but nefarious, actors around the world.

Despite double digit annual growth of the workforce in recent years, shortages remain. An effective workforce plan, in support of a sound cybersecurity strategy, requires a balance of well-rounded IT operators and sophisticated Cybersecurity Professionals who can successfully tackle the most complex challenges.

> *"91.8% of CIO's indicate that the state's salary rates and pay grade structures present a challenge in attracting and retaining IT talent with the security discipline presenting the greatest challenge."*

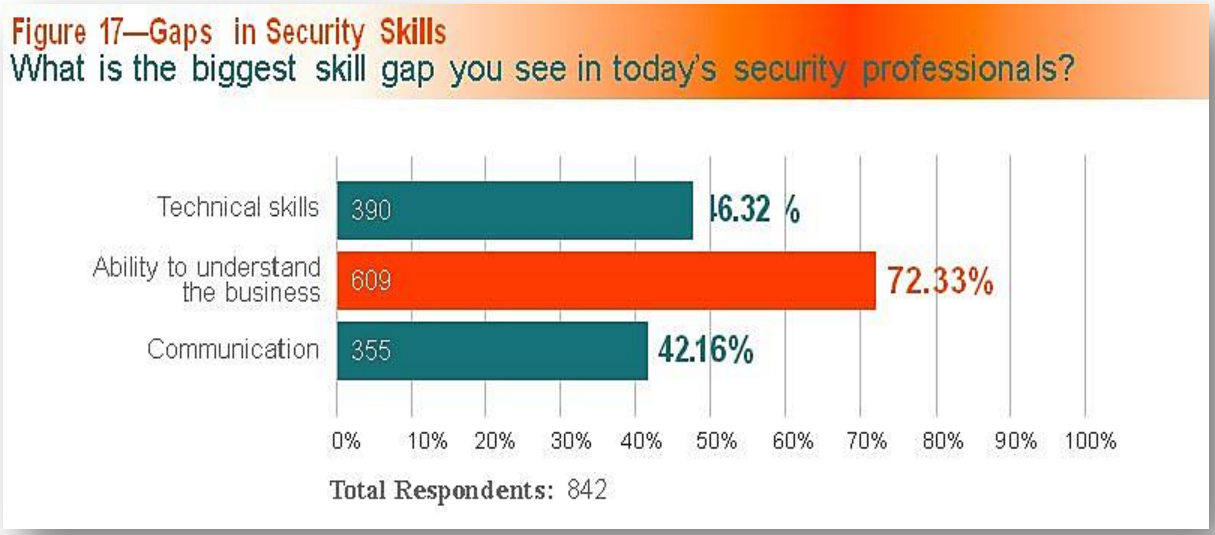
State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey

Ernst & Young's "Global Information Security Survey 2014" points out that it is "very difficult to hire the specialists necessary to perform the analysis on threat intelligence data, draw relevant and actionable conclusions, and enable decisions and responses to be taken." State of Cybersecurity: Implications for 2015, An ISACA and RSA Conference Survey



Respondents reported that, among the factors that support a candidate's qualification for a position, hands-on experience is the most important. Working against the candidate is lack of a certification—the second most frequently reason for considering a candidate not qualified. Of course, even candidates who are considered qualified are not always hired. When asked why qualified candidates may not be hired, respondents reported that the flexibility of the job requirements and starting salaries are the two biggest roadblocks to obtaining skilled new employees.

Among hired individuals, security professionals continue to see a skills gap. Survey participants overwhelmingly reported that the largest gap exists in security practitioners' ability to understand the business; this is followed by technical skills and communication (figure 17).



Finally, there were more than a few key survey questions that received a response of "I don't know." Cybersecurity cannot tolerate an inability to recognize when enterprise information assets have potentially been compromised. Less than half of the respondents indicated that their enterprise had established a Security Operations Center (SOC). A SOC can swiftly identify incidents that will impact the enterprise and respond promptly, so perhaps this offers a logical quick-win activity for enterprises wishing to enhance their security readiness. Enterprises are offering professional development to security staff, so that is a step in the right direction.

The 2013 (ISC)^2 Global Information Workforce Study found an ever widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world.

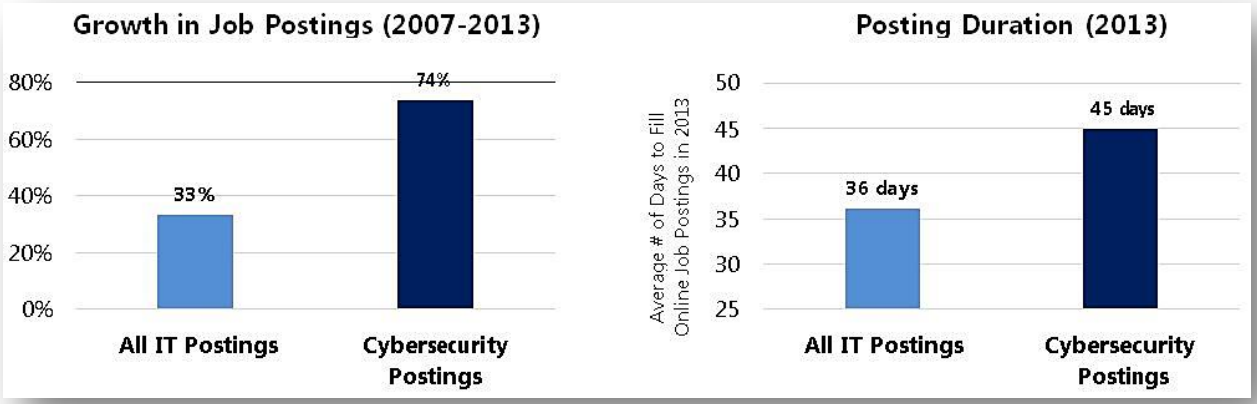
MARKET OVERVIEW: CYBERSECURITY JOBS

The Market for Cybersecurity Jobs Is Large and Growing

- *In 2013, there were 209,749 postings for cybersecurity-related jobs nationally. Cybersecurity jobs account for nearly 10% of all IT jobs.*
- *Cybersecurity postings have grown 74% from 2007-2013. This growth rate is over 2x faster than all IT jobs.*

Demand for Cybersecurity Talent Is Outstripping Supply

- *Cybersecurity job postings took 24% longer to fill than all IT job postings and 36% longer than all job postings.*
- *The demand for cybersecurity talent appears to be outstripping supply. In the US, employers posted 50,000 jobs requesting Certified Information Systems Security Professional (CISSP), recruiting from a pool of only 60,000 CISSP holders.*

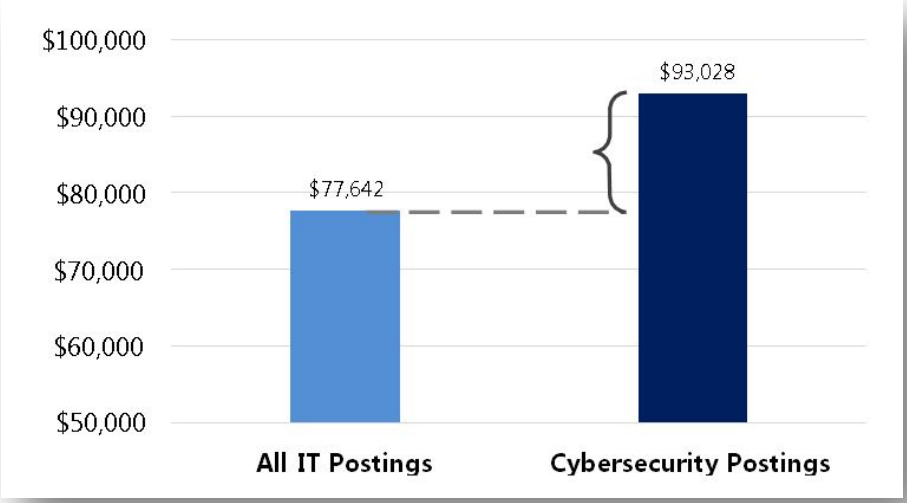


Note: California is ranked #1 in the Nation for total number of cybersecurity job postings by State (27,084), a 64% Growth from 2007-2013

CYBERSECURITY JOBS OFFER INCREASED SALARIES

Cybersecurity Jobs Pay a Premium

On average, cybersecurity salaries offer a premium of over $15,000 over the salaries for IT jobs overall.



Cybersecurity is changing so quickly that organizations can fail to plan for the necessary workforce or make poor hiring decisions, impeding the ability to implement effective security measures like the Critical Controls. Through proper deployment and efforts to optimize the workforce in an ongoing manner, the security posture of the enterprise as a whole can be improved and sustained.

Concerns about the gap in the workforce are not new; however; the issue is now acute. The 2013 (ISC)^2 study also shows an increase in threats driven by the rapid introduction of new technologies that don't have security "baked in" the product development process. In addition, the number of organized attacks is increasing as hackers move from individuals flexing their own skills to interconnected groups of criminals who share information and conduct coordinated attacks.

B. CYBERSECURITY ROLES

1. CURRENT CALIFORNIA INFORMATION TECHNOLOGY (IT) ROLES[3] AND COMPETENCIES

The following California IT classifications have historically been utilized for the majority of information security staffing needs. These classifications do not align with the highly specialized skills of cybersecurity functions.

i. INFORMATION SYSTEMS ANALYST SERIES

Classes in this series are used to perform a variety of analytical activities in support of information technology systems, such as microcomputers, multifunction automated office systems, and teleprocessing networks and/or systems. Incumbents develop problem solutions using information technology methods; conduct feasibility studies; act as project managers over information technology system projects; work on analysis and support of multifunction office systems; provide information center services and information technology system services; develop information processing standards and procedures; act as lead person or supervisor over the technical personnel in the performance of information system tasks; and do other related work.

- Assistant Information Systems Analyst
- Associate Information Systems Analyst (Specialist)
- Associate Information Systems Analyst (Supervisor)
- Staff Information Systems Analyst (Specialist)
- Staff Information Systems Analyst (Supervisor)
- Senior Information Systems Analyst (Specialist)
- Senior Information Systems Analyst (Supervisor)

Knowledge and Abilities

All Levels:

Knowledge of: Information technology systems (software) programming, equipment, and its capabilities and interfaces between hardware and software; and the requirements for the installation and implementation of the most complex information technology software systems.

Ability to: Write complex programs; develop detailed program specifications; analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions; apply creative thinking in the design and development of methods of processing information with information technology systems; establish and maintain cooperative relationships with those contacted in the course of the work; work under pressure; communicate effectively; prepare effective reports; coordinate the activities of technical personnel.

[3] California Department of Human Resources *Classification description (specification)* - www.calhr.ca.gov

ii. SYSTEMS SOFTWWARE SPECIALIST SERIES

Classes in this series are used to analyze, design, code, implement, maintain, and evaluate computer software; this includes, but is not limited to, operating systems, control systems, proprietary software packages, telecommunications software, and database management software. These classes are also used as technical advisors to act as consultants to other information technology personnel in solving system problems and achieving the best use of available hardware and software resources; to act as lead person or supervisor over other personnel; the classes are also used to coordinate and ensure effective operations of complex multiple hardware and software configurations; and to do other related work.

Computer software encompasses operating systems and utilities, telecommunications software, database management systems, special purpose vendor-supplied package software, special purpose control systems, and includes, but is limited to, both modified vendor-supplied systems and systems specifically developed by the user.

- Associate Systems Software Specialist
- Systems Software Specialist I (Technical)
- Systems Software Specialist II (Technical)
- Systems Software Specialist II (Supervisory)
- Systems Software Specialist III (Technical)
- Systems Software Specialist III (Supervisory)

Knowledge and Abilities

All Levels:

Knowledge of: Principles of public administration, organization, and management; information technology systems equipment, software, and practices; analytical techniques; technical report writing.

Ability to: Analyze information and situations, identify and solve problems, reason logically, and draw valid conclusions; develop effective solutions; apply creative thinking in the design of methods of processing information with information technology systems; monitor and resolve problems with information technology systems hardware, software, and processes; establish and maintain effective working relationships with others; communicate effectively.

2. PROPOSED CYBERSECURITY ROLES AND COMPETENCIES[4]

Eight roles have been identified to segment the many job titles within the State government information security workforce into manageable functional groups. Each of these roles represents a cluster of organizational positions/job titles that perform similar functions in the workplace with the appropriate information security competencies. The first four roles are executive or managerial in nature and have been included to illustrate the need for these roles, regardless of the cybersecurity classification structure.

Please note that the executive and managerial roles are included for illustrative purposes only, the focus of this whitepaper will remain on the represented classification series.

i. CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer (CISO) specializes in the information and physical security strategy within an organization supporting the strategic use and management of information, information systems and information technology. The CISO is charged with the development and subsequent enforcement of the organization's security policies and procedures, security awareness and education programs, business continuity and disaster recovery plans, and all security-related regulatory compliance issues.

ii. PRIVACY OFFICER

The Privacy Officer is responsible for developing and managing an organization's privacy compliance program. Privacy implementation is the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. The Privacy Officer establishes a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII) and ensures that PII is managed throughout the information life cycle from collection to disposal. Included is integration of the appropriate privacy security controls and technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

[4] A more thorough discussion of the proposed cybersecurity roles, competencies, knowledge, skills, and abilities can be found in the Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development.

iii. INFORMATION SECURITY OFFICER OR MANAGER

The Information Security Officer (ISO) or Information Security Manager (ISM) specializes in the information and physical security strategy within an organization. The ISO or ISM is charged with the development and subsequent enforcement of the organization's policies and procedures, security awareness program, business continuity and disaster recovery plans, and all industry and governmental compliance issues. The ISO or ISM:

- Manages an agency's information security program by overseeing and ensuring agency compliance with policies and procedures regarding the security of information assets.
- Must be of a sufficiently high-level job classification and/or position/job description that can execute the responsibilities of the office in an effective and independent manner.
- Establishes security policies and procedures.
- Understand the business process needs.
- Assesses internal and external risks and the respective business impact.
- Provide appropriate mitigation strategies.
- Stay current on State statutes, State/Federal laws and regulations.
- Provide oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems.
- Provides approval of proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data
- Determine aforementioned proposals meet all provisions of agency information security and risk management policies
- Approves the use of alternatives to support encryption for the protection of confidential, personal and sensitive information stored on portable electronic storage media and portable computing devices
- Approves any business use of peer-to-peer technologies.

iv. COMPLIANCE OFFICER (INFORMATION ASSURANCE)

The Compliance Officer is responsible for overseeing, evaluating and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Compliance Officer provides guidance and autonomous evaluation of the organization to management.

Information Assurance practitioners ensure, verify and validate the protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

v. CYBERSECURITY ENGINEER

The Cybersecurity Engineer applies cross-disciplinary IT and information security knowledge to build technology systems that remain dependable in the process of conducting business and in the face of malice, error and mischance.

vi. CYBERSECURITY PROFESSIONAL

The Cybersecurity Professional concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

The Cybersecurity Professional also includes the Cybersecurity Procurement Professional. The Cybersecurity Procurement Professional is responsible for purchasing and negotiating for products (e.g., software and hardware) and services (e.g., contractor support) in support of an organization's IT strategy. In the information security context, they must ensure that security requirements are specified within solicitation and contract documents (Sarbanes-Oxley, FISMA, etc.) and that only products and services meeting requirements are procured. Cybersecurity Procurement Professionals must be knowledgeable about their industry and their own organization, and must be able to effectively communicate with suppliers and negotiate terms of service.

vii. CYBERSECURITY OPERATIONS & MAINTENANCE PROFESSIONAL

The Cybersecurity Operations and Maintenance Professional ensures the security of information and information systems during the operations and maintenance phases of the system development lifecycle (SDLC).

viii. CYBERSECURITY SYSTEM ADMINISTRATION PROFESSIONAL

The Cybersecurity System Administration Professional supports the application of the principles, policies and procedures, and compliance with laws, regulations, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes the integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

C. FUNCTIONAL CATEGORIZATION BY PERSPECTIVE[5]: MANAGE (M), DESIGN (D), IMPLEMENT (I), EVALUATE (E)

Utilizing the roles developed in the IT Security Essential Body of Knowledge (EBK), each competency was categorized into one of the four functional perspectives of Manage, Design, Implement or Evaluate. The Functional Perspectives are defined as follows:

- **Manage (M)**[6]: Functions that encompass overseeing a program or technical aspect of a security program at a high-level and ensuring currency with changing risk and threat environments.
- **Design (D)**: Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.
- **Implement (I)**: Functions that encompass putting programs, processes, or policies into action with an organization.
- **Evaluate (E)**: Functions that encompass assessing the effectiveness of a program, policy, process or security service in achieving its objectives.

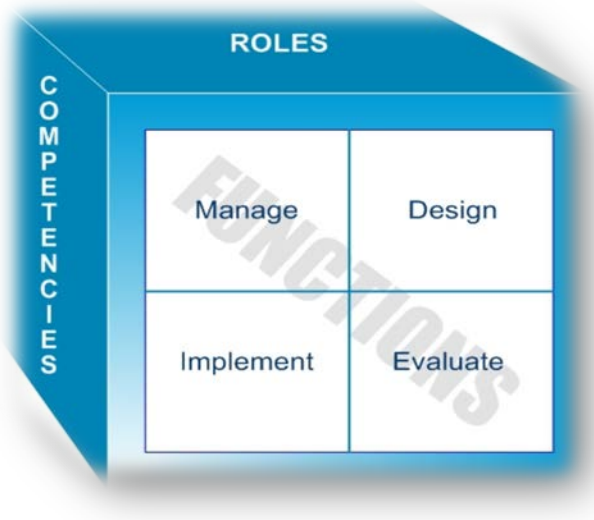


Figure 1 Mapping Diagram: Roles to Competencies to Functions

The next step was to map the roles to the appropriate sets of competencies, then identify the specific functional perspective to describe the work performed in each role. This effort is illustrated in the following sections.

---

[5] **Note:** These perspectives do **not** convey a lifecycle concept of task or program execution as is typical of a traditional system development lifecycle, but are used to sort functions of a similar nature.

[6] Manage (M) in this perspective refers to overseeing a program or technical aspect of a program, NOT managing people.

1. COMPETENCY CATEGORIZED BY FUNCTIONAL PERSPECTIVE: CURRENT CALIFORNIA IT ROLES

i. INFORMATION SYSTEMS ANALYST SERIES

Assistant Information Systems Analyst
Associate Information Systems Analyst (Specialist)
Associate Information Systems Analyst (Supervisor)
Staff Information Systems Analyst (Specialist)
Staff Information Systems Analyst (Supervisor)
Senior Information Systems Analyst (Specialist)
Senior Information Systems Analyst (Supervisor)

EBK COMPETENCIES:

- Data (Information) Security: Not listed in CalHR Specifications
- Digital Forensics: Not listed in CalHR Specifications
- Enterprise Architecture: Not listed in CalHR Specifications
- Enterprise Continuity (Disaster Recovery) : Not listed in CalHR Specifications
- Incident Management: Not listed in CalHR Specifications
- IT Security Training and Awareness: Not listed in CalHR Specifications
- IT Systems Operations and Maintenance: Not listed in CalHR Specifications
- Network and Telecommunications Security: Not listed in CalHR Specifications
- Physical and Personnel Security: Not listed in CalHR Specifications
- Policies, Standards and Compliance (Info Assurance): Not listed in CalHR Specs
- Privacy: Not listed in CalHR Specifications
- Procurement: Not listed in CalHR Specifications
- Security Risk Management: Not listed in CalHR Specifications
- Strategic Security Management: Not listed in CalHR Specifications
- System and Application Security: Not listed in CalHR Specifications

ii. SYSTEMS SOFTWARE SPECIALIST SERIES

Associate Systems Software Specialist
Systems Software Specialist I (Technical)

EBK COMPETENCIES:

- Data (Information) Security: Not listed in CalHR Specifications
- Digital Forensics: Not listed in CalHR Specifications
- Enterprise Architecture: Not listed in CalHR Specifications
- Enterprise Continuity (Disaster Recovery) : Not listed in CalHR Specifications
- Incident Management: Not listed in CalHR Specifications
- IT Security Training and Awareness: Not listed in CalHR Specifications
- IT Systems Operations and Maintenance: Not listed in CalHR Specifications
- Network and Telecommunications Security: Not listed in CalHR Specifications
- Physical and Personnel Security: Not listed in CalHR Specifications
- Policies, Standards and Compliance (Info Assurance): Not listed in CalHR Specs
- Privacy: Not listed in CalHR Specifications
- Procurement: Not listed in CalHR Specifications
- Security Risk Management: Not listed in CalHR Specifications
- Strategic Security Management: Not listed in CalHR Specifications
- System and Application Security: *Evaluate*

Systems Software Specialist II (Technical)
Systems Software Specialist II (Supervisory)

EBK COMPETENCIES:

- Data (Information) Security: Not listed in CalHR Specifications
- Digital Forensics: Not listed in CalHR Specifications
- Enterprise Architecture: Not listed in CalHR Specifications
- Enterprise Continuity (Disaster Recovery) : Not listed in CalHR Specifications
- Incident Management: Not listed in CalHR Specifications
- IT Security Training and Awareness: Not listed in CalHR Specifications
- IT Systems Operations and Maintenance: Not listed in CalHR Specifications
- Network and Telecommunications Security: Not listed in CalHR Specifications
- Physical and Personnel Security: Not listed in CalHR Specifications
- Policies, Standards and Compliance (Info Assurance): Not listed in CalHR Specs
- Privacy: Not listed in CalHR Specifications
- Procurement: Not listed in CalHR Specifications
- Security Risk Management: Not listed in CalHR Specifications
- Strategic Security Management: Not listed in CalHR Specifications
- System and Application Security: *Design, Evaluate*

Systems Software Specialist III (Technical)
Systems Software Specialist III (Supervisory)

EBK COMPETENCIES:

- Data (Information) Security: Not listed in CalHR Specifications
- Digital Forensics: Not listed in CalHR Specifications
- Enterprise Architecture: Not listed in CalHR Specifications
- Enterprise Continuity (Disaster Recovery) : Not listed in CalHR Specifications
- Incident Management: Not listed in CalHR Specifications
- IT Security Training and Awareness: Not listed in CalHR Specifications
- IT Systems Operations and Maintenance: Not listed in CalHR Specifications
- Network and Telecommunications Security: Not listed in CalHR Specifications
- Physical and Personnel Security: Not listed in CalHR Specifications
- Policies, Standards and Compliance (Info Assurance): Not listed in CalHR Specs
- Privacy: Not listed in CalHR Specifications
- Procurement: Not listed in CalHR Specifications
- Security Risk Management: Not listed in CalHR Specifications
- Strategic Security Management: Not listed in CalHR Specifications
- System and Application Security: *Design, Implement, Evaluate*

2. COMPETENCY CATEGORIZED BY FUNCTIONAL PERSPECTIVE: PROPOSED CYBERSECURITY ROLES

i. CHIEF INFORMATION SECURITY OFFICER

EBK COMPETENCIES:

- Data (Information) Security: *Manage, Evaluate*
- Digital Forensics: *Manage, Evaluate*
- Enterprise Architecture: *Evaluate*
- Enterprise Continuity (Disaster Recovery): *Manage*
- Incident Management: *Manage*
- Information Security Training and Awareness: *Manage*
- IT Systems Operations and Maintenance: N/A
- Network and Telecommunications Security: *Evaluate*
- Physical and Personnel Security: *Manage*
- Policies, Standards and Compliance (Information Assurance): *Manage, Evaluate*
- Privacy: *Manage, Design, Evaluate*
- Procurement: *Manage, Design, Evaluate*
- Security Risk Management: *Manage, Design, Implement, Evaluate*
- Strategic Security Management: *Manage, Design, Implement, Evaluate*
- System and Application Security: *Manage, Evaluate*

ii. PRIVACY OFFICER

EBK COMPETENCIES:

- Data (Information) Security: *Manage, Design, Evaluate*
- Digital Forensics: *Evaluate*
- Enterprise Architecture: N/A
- Enterprise Continuity (Disaster Recovery): *Evaluate*
- Incident Management: *Manage, Design, Implement, Evaluate*
- Information Security Training and Awareness: *Design, Evaluate*
- IT Systems Operations and Maintenance: N/A
- Network and Telecommunications Security: N/A
- Physical and Personnel Security: *Design, Implement, Evaluate*
- Policies, Standards and Compliance (Info Assurance): *Design, Implement, Evaluate*
- Privacy: *Manage, Design, Implement, Evaluate*
- Procurement: *Evaluate*
- Security Risk Management: Manage, *Design, Implement, Evaluate*
- Strategic Security Management: N/A
- System and Application Security: *Evaluate*

iii. INFORMATION SECURITY OFFICER OR MANAGER

EBK COMPETENCIES:

- Data (Information) Security: *Manage, Design, Evaluate*
- Digital Forensics: *Implement*
- Enterprise Architecture: N/A
- Enterprise Continuity (Disaster Recovery): *Evaluate*
- Incident Management: *Design, Implement, Evaluate*
- Information Security Training and Awareness: *Design, Implement, Evaluate*
- IT Systems Operations and Maintenance: N/A
- Network and Telecommunications Security: N/A
- Physical and Personnel Security: *Manage, Design, Evaluate*
- Policies, Standards, Compliance (Info Assurance): *Manage, Design, Implement, Evaluate*
- Privacy: *Implement*
- Procurement: N/A
- Security Risk Management: Design, Implement, Evaluate
- Strategic Security Management: *Implement*
- System and Application Security: *Evaluate*

iv. COMPLIANCE OFFICER (INFORMATION ASSURANCE)

EBK COMPETENCIES:

- Data (Information) Security: *Evaluate*
- Digital Forensics: *Evaluate*
- Enterprise Architecture: *Evaluate*
- Enterprise Continuity (Disaster Recovery): *Evaluate*
- Incident Management: *Evaluate*
- IT Security Training and Awareness: *Design, Evaluate*
- IT Systems Operations and Maintenance: *Evaluate*
- Network and Telecommunications Security: *Evaluate*
- Physical and Personnel Security: *Evaluate*
- Policies, Standards, Compliance (Info Assurance): *Manage, Design, Implement, Evaluate*
- Privacy: *Evaluate*
- Procurement: *Evaluate*
- Security Risk Management: Implement, *Evaluate*
- Strategic Security Management: *Evaluate*
- System and Application Security: *Evaluate*

v. CYBERSECURITY ENGINEER

EBK COMPETENCIES:

- Data (Information) Security: *Design, Implement, Evaluate*
- Digital Forensics: *Design, Evaluate*
- Enterprise Architecture: *Manage, Design, Implement, Evaluate*
- Enterprise Continuity (Disaster Recovery): *Design, Implement, Evaluate*
- Incident Management: *Design, Implement, Evaluate*
- IT Security Training and Awareness: *Design, Implement, Evaluate*
- IT Systems Operations and Maintenance: *Design, Implement, Evaluate*
- Network and Telecommunications Security: *Manage, Design, Implement*, *Evaluate*
- Physical and Personnel Security: *Implement, Evaluate*
- Policies, Standards and Compliance (Information Assurance): *Implement*
- Privacy: *Design, Evaluate*
- Procurement: *Design, Evaluate*
- Security Risk Management: Design, Implement, Evaluate
- Strategic Security Management: *Implement*
- System and Application Security: *Design, Implement, Evaluate*

vi. CYBERSECURITY PROFESSIONAL

EBK COMPETENCIES:

- Data (Information) Security: *Design, Implement*
- Digital Forensics: *Implement, Evaluate*
- Enterprise Architecture: *Evaluate*
- Enterprise Continuity (Disaster Recovery): *Design, Implement, Evaluate*
- Incident Management: *Design, Implement,, Evaluate*
- IT Security Training and Awareness: *Implement, Evaluate*
- IT Systems Operations and Maintenance: *Evaluate*
- Network and Telecommunications Security: *Evaluate*
- Physical and Personnel Security: *Design, Implement, Evaluate*
- Policies, Standards and Compliance (Information Assurance): *Implement, Evaluate*
- Privacy: *Design, Implement, Evaluate*
- Procurement: *Design, Implement, Evaluate*
- Security Risk Management: Design, Implement, Evaluate
- Strategic Security Management: *Implement, Evaluate*
- System and Application Security: *Design, Implement, Evaluate*

vii. CYBERSECURITY OPERATIONS & MAINTENANCE PROFESSIONAL

EBK COMPETENCIES:

- Data (Information) Security: *Implement, Evaluate*
- Digital Forensics: *Implement*
- Enterprise Architecture: *Implement*, *Evaluate*
- Enterprise Continuity (Disaster Recovery): *Design, Implement*
- Incident Management: *Design, Implement, Evaluate*
- IT Security Training and Awareness: *Implement, Evaluate*
- IT Systems Operations and Maintenance: *Manage, Design, Implement, Evaluate*
- Network and Telecommunications Security: *Manage, Design, Implement, Evaluate*
- Physical and Personnel Security: *Evaluate*
- Policies, Standards and Compliance (Information Assurance): *Implement, Evaluate*
- Privacy: *Implement, Evaluate*
- Procurement: *Evaluate*
- Security Risk Management: *Implement*
- Strategic Security Management: *Implement*
- System and Application Security: *Design, Implement, Evaluate*

viii. CYBERSECURITY SYSTEM ADMINISTRATION PROFESSIONAL

EBK COMPETENCIES:

- Data (Information) Security: *Design, Implement, Evaluate*
- Digital Forensics: *Implement*
- Enterprise Architecture: *Implement, Evaluate*
- Enterprise Continuity (Disaster Recovery): *Design, Implement, Evaluate*
- Incident Management: *Design, Implement, Evaluate*
- IT Security Training and Awareness: *Implement, Evaluate*
- IT Systems Operations and Maintenance: *Manage, Design, Implement, Evaluate*
- Network and Telecommunications Security: *Manage, Design, Implement, Evaluate*
- Physical and Personnel Security: *Design, Implement, Evaluate*
- Policies, Standards and Compliance (Information Assurance): *Implement, Evaluate*
- Privacy: Evaluate
- Procurement: *Evaluate*
- Security Risk Management: Design, Implement, Evaluate
- Strategic Security Management: *Implement*
- System and Application Security: *Design, Implement, Evaluate*

Current California IT Positions Mapped to the Competency and Functional Framework Essential Body of Knowledge (EBK)		CURRENT IT ROLES													
		Associate Information Systems Analyst		Staff Information Systems Analyst		Senior Information Systems Analyst		Associate Systems Software Specialist		Systems Software Specialist I		Systems Software Specialist II		Systems Software Specialist III	
INFORMATION SECURITY COMPETENCIES															
1	Data (Information) Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
2	Digital Forensics	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
3	Enterprise Architecture	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
4	Enterprise Continuity (Disaster Recovery)	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
5	Incident Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
6	Information Security Training and Awareness	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
7	IT Systems Operations and Maintenance	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
8	Network and Telecommunications Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
9	Physical and Personnel Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
10	Policies, Standards and Compliance (Info Assurance)	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
11	Privacy	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
12	Procurement	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
13	Security Risk Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
14	Strategic Security Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E
15	System and Application Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D
		I	E	I	E	I	E	I	E	I	E	I	E	I	E

Table 1: Current California IT Positions Competency & Functional Matrix

Proposed California Cybersecurity Positions Mapped to the Competency and Functional Framework Essential Body of Knowledge (EBK)			PROPOSED IT ROLES															
			Executive (Managerial)								Functional (Technical)							
			Chief Information Security Officer		Privacy Officer		Information Security Officer or Manager		Compliance Officer (Information Assurance)		Cybersecurity Engineer		Cybersecurity Prof.		Cybersecurity Operations & Maint. Prof.		Cybersecurity System Admin. Prof.	
INFORMATION SECURITY COMPETENCIES	1	Data (Information) Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	2	Digital Forensics	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	3	Enterprise Architecture	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	4	Enterprise Continuity (Disaster Recovery)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	5	Incident Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	6	Information Security Training and Awareness	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	7	IT Systems Operations and Maintenance	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	8	Network and Telecommunications Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	9	Physical and Personnel Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	10	Policies, Standards and Compliance (Info Assurance)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	11	Privacy	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	12	Procurement	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
	13	Security Risk Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	I	I	E
	14	Strategic Security Management	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	I	I	E
	15	System and Application Security	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
			I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E

Table 2: Proposed California IT Positions Competency & Functional Matrix

D. CYBERSECURITY CAREER PROGRESSION

1. SAMPLE CYBERSECURITY CAREER PROGRESSION

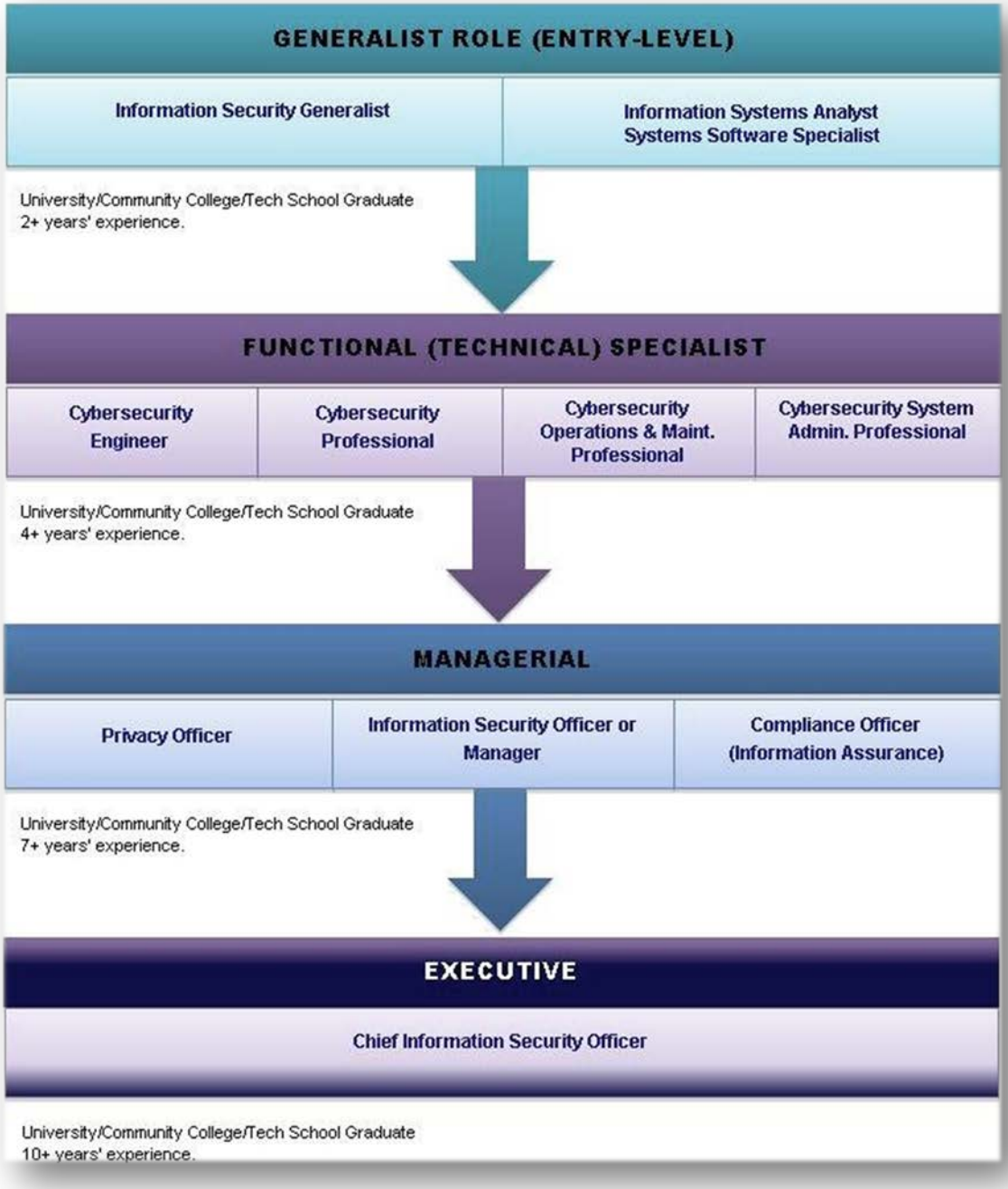


Figure 2: Sample Cybersecurity Career Progression

2. SAMPLE CYBERSECURITY CAREER LADDER

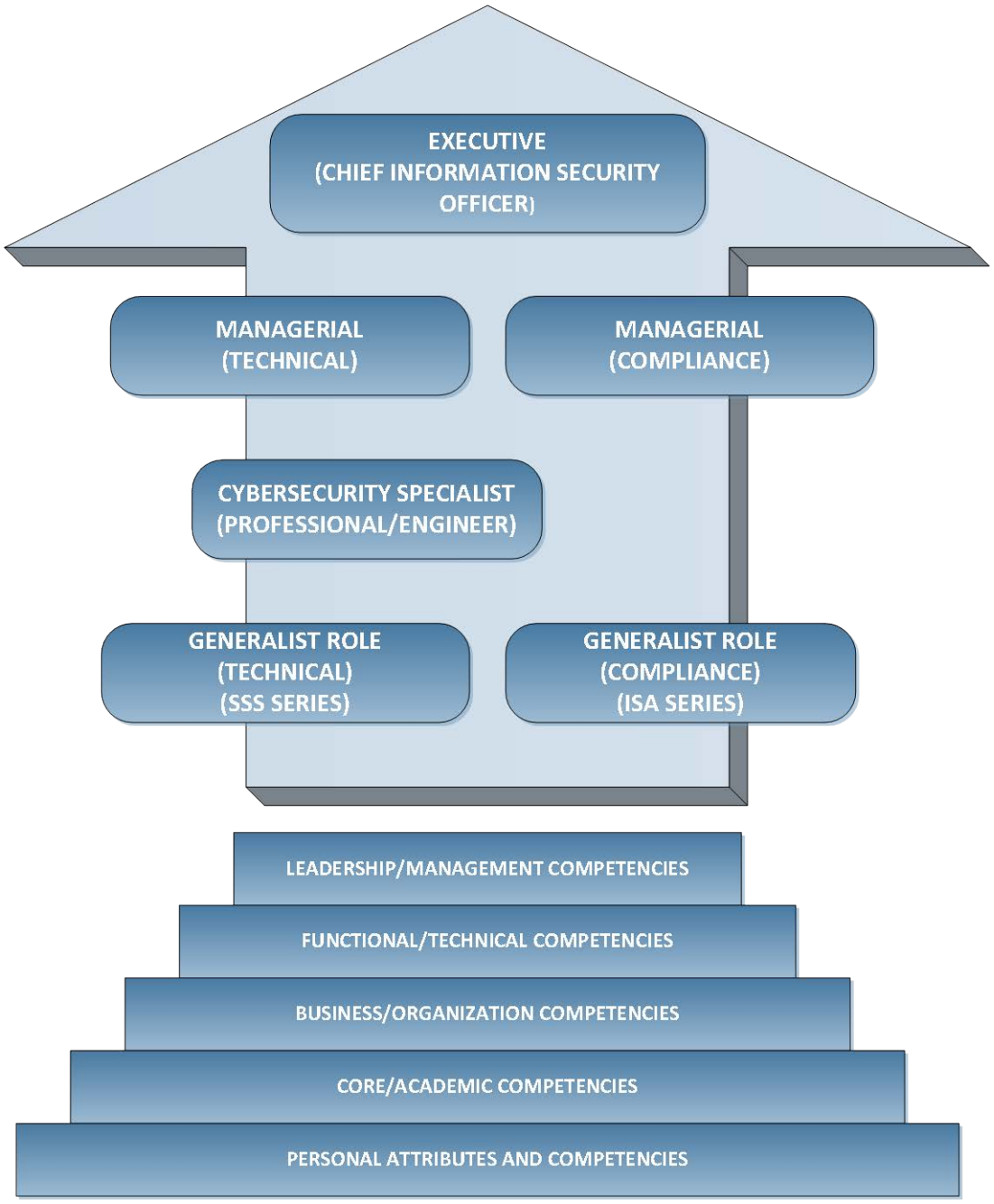


Figure 3: Sample Cybersecurity Career Ladder

VI. RECOMMENDATIONS

Despite double digit annual growth of the workforce in recent years, shortages remain. An effective workforce plan, in support of a sound cybersecurity strategy, requires a balance of well-rounded IT operators and sophisticated Cybersecurity Professionals who can successfully tackle the most complex challenges.

Based on our research, this workgroup makes the following recommendations:

1. Create a new Cybersecurity Professional classification - Adopt a new classification series of Cybersecurity Professionals in order to create a career ladder for highly skilled staff.

    a. A new classification series allows the State to be competitive in recruiting and retaining Cybersecurity Professionals.

    b. Endeavoring to create a highly skilled Cybersecurity Workforce will garner Union support for this classification series as increased recruitment and retention of Cybersecurity Professionals will reduce the State's dependence on outside vendors and consultants in this highly technical and specialized field.

2. Information Technology (IT) Capital Planning and Security Funding – All IT investments must demonstrate that costs for appropriate IT privacy and security controls and staffing are explicitly incorporated into the life cycle planning of all systems. Budget proposals should also include line items for vulnerability assessments and penetration testing.

3. Information Security training and awareness for all – All personnel who access confidential information are required to complete initial and annual information security and privacy training. Information security training and education needs to be integrated into the classification specifications for ALL State public servants and incorporated into duty statements throughout State service; more attention needs to be placed on role-based security training for information technology classifications.

VII. NEXT STEPS

- Discuss the recommendations of the "*State of California Cybersecurity Task Force, Workforce Development and Training: Objective 1*" with the California Department of Human Resources, Statewide Workforce Planning and Recruitment Unit.

- Establish a workgroup to develop a Workforce Plan.

- Develop Classification Descriptions (specifications) for the proposed Cybersecurity Professional series.

- Map out appropriate training based on Federal guidelines and industry best practices for IT security.

APPENDIX A: COMPETENCY AND FUNCTIONAL FRAMEWORK ESSENTIAL BODY OF KNOWLEDGE (EBK)

The fifteen (15) information security competencies defined below comprise *The State Government Information Security Model* competency areas.

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
1	**Data (Information) Security:** Refers to the application of the principles, policies and procedures necessary to ensure the confidentiality, integrity, availability and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.
2	**Digital Forensics:** Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed for our (4) phase: Prepare, Acquire, Analyze and Report.
3	**Enterprise Architecture:** Refers to the practice of applying security design principles to applications, and architecting enterprise-scale security solutions, infrastructure, processes and business activities.
4	**Enterprise Continuity (Disaster Recovery):** Refers to the application of the principles, policies and procedures to ensure than an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events.
5	**Incident Management:** Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization.
6	**Information Security Training and Awareness:** Refers to the principles, practices and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills and abilities.
7	**IT Systems Operations and Maintenance:** Refers to the ongoing application of principles, policies and procedures to maintain, monitor, control and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.
8	**Network and Telecommunications Security:** Refers to application of the principles, policies and procedures involved in ensuring the security of basic network and telecommunications services and data, and in maintaining the hardware layer on which it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.
9	**Physical and Personnel Security:** Refers to methods and controls use to: Physical Security - proactively protect an organization from natural or manmade threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Personnel Security - ensure than an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information and non-compliance.
10	**Policies, Standards and Compliance (Information Assurance):** Refers to the application of the principles, policies and procedures that enable an enterprise to meet applicable information security laws, standards and policies to satisfy statutory requirements, perform industry-wide best practices and achieve information security program goals.

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
11	**Privacy:** Refers to the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).
12	**Procurement:** Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.
13	**Security Risk Management:** Refers to the policies, processes, procedures and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment and to manage mitigation strategies that achieve the security needed at an affordable cost.
14	**Strategic Security Management:** Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of these analyses is to ensure that an organization's IT security principles, practices, and system design are in line with its mission statement.
15	**System and Application Security:** Refers to the principles, policies and procedures pertaining to integrating information security into an IT system or application during the SDLC prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation and software security standards compliance.

APPENDIX B: NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES FRAMEWORK SPECIALTY AREAS (FSA)

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
1	**All Source Intelligence:** Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
2	**Exploitation Analysis:** Analyzes collected information to identify vulnerabilities and potential for exploitation.
3	**Targets:** Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
4	**Threat Analysis:** Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
5	**Collection Operations:** Executes collection using appropriate strategies and within the priorities established through the collection management process.
6	**Cyber Operations:** Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities
7	**Cyber Operations Planning:** Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
8	**Digital Forensics:** Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations
9	**Investigation:** Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering
10	**Customer Service and Technical Support:** Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
11	**Data Administration:** Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data
12	**Knowledge Management:** Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
13	**Network Services:** Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems
National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	

14	**System Administration:** Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
15	**Systems Security Analysis:** Conducts the integration/testing, operations, and maintenance of systems security.
16	**Education and Training:** Conducts training of personnel within pertinent subject domain. Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques as appropriate.
17	**Information Systems Security Operations (Information Systems Security Officer):** Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).
18	**Legal Advice and Advocacy:** Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
19	**Security Program Management (Chief Information Security Officer):** Manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).
20	**Strategic Planning and Policy Development:** Applies knowledge of priorities to define an entity
21	**Computer Network Defense Analysis:** Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
22	**Computer Network Defense Infrastructure Support:** Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities
23	**Incident Response:** Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
24	**Vulnerability Assessment and Management:** Vulnerability Assessment and Management - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
25	**Information Assurance Compliance:** Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
26	**Software Assurance and Security Engineering:** Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
27	**Systems Development:** Works on the development phases of the systems development lifecycle.
28	**Systems Requirements Planning:** Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
29	**Systems Security Architecture:** Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
30	**Technology Research and Development:** Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
31	**Test and Evaluation:** Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

APPENDIX C:
A MAPPING of FRAMEWORK SPECIALTY AREAS (FSA) to ESSENTIAL BODY OF KNOWLEDGE (EBK)

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
1	**Data (Information) Security:** Refers to the application of the principles, policies and procedures necessary to ensure the confidentiality, integrity, availability and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.	10	**Customer Service and Technical Support**
		12	**Knowledge Management**
		21	**Computer Network Defense Analysis**
		30	**Technology Research and Development**
		31	**Test and Evaluation**
2	**Digital Forensics:** Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed for our (4) phase: Prepare, Acquire, Analyze and Report.	2	**Exploitation Analysis**
		4	**Threat Analysis**
		8	**Digital Forensics**
		9	**Investigation**
		21	**Computer Network Defense Analysis**
3	**Enterprise Architecture:** Refers to the practice of applying security design principles to applications, and architecting enterprise-scale security solutions, infrastructure, processes and business activities.	3	**Targets**
		7	**Cyber Operations Planning**
		20	**Strategic Planning and Policy Development**
		27	**Systems Development**
		28	**Systems Requirements Planning**
		29	**Systems Security Architecture**
4	**Enterprise Continuity (Disaster Recovery):** Refers to the application of the principles, policies and procedures to ensure than an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events.	2	**Exploitation Analysis**
		3	**Targets**
		5	**Collection Operations**
		28	**Systems Requirements Planning**

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
5	**Incident Management:** Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization.	1	**All Source Intelligence**
		2	**Exploitation Analysis**
		4	**Threat Analysis**
		5	**Collection Operations**
		6	**Cyber Operations**
		8	**Digital Forensics**
		9	**Investigation**
		21	**Computer Network Defense Analysis**
		23	**Incident Response**
6	**Information Security Training and Awareness:** Refers to the principles, practices and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills and abilities.	1	**All Source Intelligence**
		10	**Customer Service and Technical Support**
		16	**Education and Training**
7	**IT Systems Operations and Maintenance:** Refers to the ongoing application of principles, policies and procedures to maintain, monitor, control and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.	1	**All Source Intelligence**
		2	**Exploitation Analysis**
		3	**Targets**
		4	**Threat Analysis**
		5	**Collection Operations**
		6	**Cyber Operations**
		7	**Cyber Operations Planning**
		8	**Digital Forensics**
		12	**Knowledge Management**
		13	**Network Services**
		14	**System Administration**
		15	**Systems Security Analysis**
		24	**Vulnerability Assessment and Management**
		25	**Information Assurance Compliance**

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
8	**Network and Telecommunications Security:** Refers to application of the principles, policies and procedures involved in ensuring the security of basic network and telecommunications services and data, and in maintaining the hardware layer on which it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.	**1**	**All Source Intelligence**
		2	**Exploitation Analysis**
		3	**Targets**
		6	**Cyber Operations**
		7	**Cyber Operations Planning**
		13	**Network Services**
		21	**Computer Network Defense Analysis**
		22	**Computer Network Defense Infrastructure Support**
9	**Physical and Personnel Security:** Refers to methods and controls use to: Physical Security - proactively protect an organization from natural or manmade threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Personnel Security - ensure than an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information and non-compliance.	**1**	**All Source Intelligence**
		2	**Exploitation Analysis**
		21	**Computer Network Defense Analysis**
10	**Policies, Standards and Compliance (Information Assurance):** Refers to the application of the principles, policies and procedures that enable an enterprise to meet applicable information security laws, standards and policies to satisfy statutory requirements, perform industry-wide best practices and achieve information security program goals.	**16**	**Education and Training**
		18	**Legal Advice and Advocacy**
		19	**Security Program Management (Chief ISO)**
		20	**Strategic Planning and Policy Development**
		25	**Information Assurance Compliance**

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
11	**Privacy:** Refers to the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).	7	**Cyber Operations Planning**
		16	**Education and Training**
		18	**Legal Advice and Advocacy**
		19	**Security Program Management (Chief ISO)**
		25	**Information Assurance Compliance**
12	**Procurement:** Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.	7	**Cyber Operations Planning**
		17	**Information Systems Security Operations (Information Systems Security Officer)**
		25	**Information Assurance Compliance**
		28	**Systems Requirements Planning**
		30	**Technology Research and Development**

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
13	**Security Risk Management:** Refers to the policies, processes, procedures and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment and to manage mitigation strategies that achieve the security needed at an affordable cost.	**1**	**All Source Intelligence**
		2	**Exploitation Analysis**
		3	**Targets**
		4	**Threat Analysis**
		6	**Cyber Operations**
		8	**Digital Forensics**
		9	**Investigation**
		15	**Systems Security Analysis**
		22	**Computer Network Defense Infrastructure Support**
		24	**Vulnerability Assessment and Management**
14	**Strategic Security Management:** Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of these analyses is to ensure that an organization's IT security principles, practices, and system design are in line with its mission statement.	**19**	**Security Program Management (Chief Information Security Officer)**
		20	**Strategic Planning and Policy Development**
		25	**Information Assurance Compliance**
		29	**Systems Security Architecture**

California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)		National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)	
15	**System and Application Security:** Refers to the principles, policies and procedures pertaining to integrating information security into an IT system or application during the SDLC prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation and software security standards compliance.	1	**All Source Intelligence**
		2	**Exploitation Analysis**
		3	**Targets**
		4	**Threat Analysis**
		6	**Cyber Operations**
		7	**Cyber Operations Planning**
		12	**Knowledge Management**
		14	**System Administration**
		15	**Systems Security Analysis**
		16	**Education and Training**
		21	**Computer Network Defense Analysis**
		22	**Computer Network Defense Infrastructure Support**
		23	**Incident Response**
		24	**Vulnerability Assessment and Management**
		25	**Information Assurance Compliance**
		26	**Software Assurance and Security Engineering**
		27	**Systems Development**
		28	**Systems Requirements Planning**
		29	**Systems Security Architecture**
		30	**Technology Research and Development**
		31	**Test and Evaluation**

APPENDIX D:
A MAPPING of ESSENTIAL BODY OF KNOWLEDGE (EBK) to FRAMEWORK SPECIALTY AREAS (FSA)

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
1	**All Source Intelligence:** Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	5	**Incident Management**
		6	**Information Security Training and Awareness**
		7	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
		9	**Physical and Personnel Security**
		13	**Security Risk Management**
		15	**System and Application Security**
2	**Exploitation Analysis:** Analyzes collected information to identify vulnerabilities and potential for exploitation.	2	**Digital Forensics**
		4	**Enterprise Continuity (Disaster Recovery)**
		5	**Incident Management**
		7	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
		9	**Physical and Personnel Security**
		13	**Security Risk Management**
		15	**System and Application Security**
3	**Targets:** Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	3	**Enterprise Architecture**
		4	**Enterprise Continuity (Disaster Recovery)**
		7	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
		13	**Security Risk Management**
		15	**System and Application Security**

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
4	**Threat Analysis:** Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	2	**Digital Forensics**
		5	**Incident Management**
		7	**IT Systems Operations and Maintenance**
		13	**Security Risk Management**
		15	**System and Application Security**
5	**Collection Operations:** Executes collection using appropriate strategies and within the priorities established through the collection management process.	4	**Enterprise Continuity (Disaster Recovery)**
		5	**Incident Management**
		7	**IT Systems Operations and Maintenance**
6	**Cyber Operations:** Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities	5	**Incident Management**
		7	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
		13	**Security Risk Management**
		15	**System and Application Security**
7	**Cyber Operations Planning:** Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	3	**Enterprise Architecture**
		7	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
		11	**Privacy**
		12	**Procurement**
		15	**System and Application Security**
8	**Digital Forensics:** Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations	2	**Digital Forensics**
		5	**Incident Management**
		7	**IT Systems Operations and Maintenance**
		13	**Security Risk Management**
9	**Investigation:** Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.	2	**Digital Forensics**
		5	**Incident Management**
		13	**Security Risk Management**

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
10	**Customer Service and Technical Support:** Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).	**1**	**Data (Information) Security**
		6	**Information Security Training and Awareness**
11	**Data Administration:** Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.		
12	**Knowledge Management:** Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	**1**	**Data (Information) Security**
		7	**IT Systems Operations and Maintenance**
		15	**System and Application Security**
13	**Network Services:** Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.	**7**	**IT Systems Operations and Maintenance**
		8	**Network and Telecommunications Security**
14	**System Administration:** Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.	**7**	**IT Systems Operations and Maintenance**
		15	**System and Application Security**
15	**Systems Security Analysis:** Conducts the integration/testing, operations, and maintenance of systems security.	**7**	**IT Systems Operations and Maintenance**
		13	**Security Risk Management**
		15	**System and Application Security**
16	**Education and Training:** Conducts training of personnel within pertinent subject domain. Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques as appropriate.	**6**	**Information Security Training and Awareness**
		10	**Policies, Standards and Compliance (Information Assurance)**
		11	**Privacy**
		15	**System and Application Security**

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
17	**Information Systems Security Operations (Information Systems Security Officer):** Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).	12	**Procurement**
18	**Legal Advice and Advocacy:** Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.	10	**Policies, Standards and Compliance (Information Assurance)**
		11	**Privacy**
19	**Security Program Management (Chief Information Security Officer):** Manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).	10	**Policies, Standards and Compliance (Information Assurance)**
		11	**Privacy**
		14	**Strategic Security Management**
20	**Strategic Planning and Policy Development:** Applies knowledge of priorities to define an entity.	3	**Enterprise Architecture**
		10	**Policies, Standards and Compliance (Information Assurance)**
		14	**Strategic Security Management**
21	**Computer Network Defense Analysis:** Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.	1	**Data (Information) Security**
		2	**Digital Forensics**
		5	**Incident Management**
		8	**Network and Telecommunications Security**
		9	**Physical and Personnel Security**
		15	**System and Application Security**
22	**Computer Network Defense Infrastructure Support:** Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	8	**Network and Telecommunications Security**
		13	**Security Risk Management**
		15	**System and Application Security**

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
23	**Incident Response:** Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	5	**Incident Management**
		15	**System and Application Security**
24	**Vulnerability Assessment and Management:** Vulnerability Assessment and Management - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.	7	**IT Systems Operations and Maintenance**
		13	**Security Risk Assessment**
		15	**System and Application Security**
25	**Information Assurance Compliance:** Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	10	**Policies, Standards and Compliance (Information Assurance)**
		11	**Privacy**
		12	**Procurement**
		14	**Strategic Security Management**
		15	**System and Application Security**
26	**Software Assurance and Security Engineering:** Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	15	**System and Application Security**
27	**Systems Development:** Works on the development phases of the systems development lifecycle.	3	**Enterprise Architecture**
		15	**System and Application Security**
28	**Systems Requirements Planning:** Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.	3	**Enterprise Architecture**
		4	**Enterprise Continuity (Disaster Recovery)**
		12	**Procurement**
		15	**System and Application Security**

National Initiative for Cybersecurity Careers and Studies Framework Specialty Areas (FSA)		California IT Security Positions Competency and Functional Framework Essential Body of Knowledge (EBK)	
29	**Systems Security Architecture:** Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.	**3**	**Enterprise Architecture**
		14	**Strategic Security Management**
		15	**System and Application Security**
30	**Technology Research and Development:** Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.	**1**	**Data (Information) Security**
		12	**Procurement**
		15	**System and Application Security**
31	**Test and Evaluation:** Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.	**1**	**Data (Information) Security**
		15	**System and Application Security**

APPENDIX E: SAMPLE MINIMUM QUALIFICATIONS [7]

A minimum of five years of direct full-time security work experience in two or more of these 10 domains:

- **Access Control –** a collection of mechanisms that work together to create security architecture to protect the assets of the information system.
- **Telecommunications and Network Security –** discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
- **Information Security Governance and Risk Management** – the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
- **Cryptography** – the principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Security Architecture and Design** – contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
- **Operations Security** – used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
- **Business Continuity and Disaster Recovery Planning** – addresses the preservation of the business in the face of major disruptions to normal business operations.
- **Legal, Regulations, Investigations and Compliance** – addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
- **Physical (Environmental) Security** – addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information.

Note that if certain circumstances apply and with appropriate documentation, candidates are eligible to **waive one year of professional experience:**

- **One year waiver of the professional experience requirement based on a candidate's education**
  Candidates can substitute a maximum of one year of direct full-time security professional work experience described above if they have a four-year college degree OR Advanced Degree in information security from a U.S. National Center of Academic Excellence in information Security (CAEIAE) or regional equivalent.

[7] (ISC)[2] CISSP Professional Experience Requirement, https://www.isc2.org/cissp-professional-experience.aspx

OR

- **One-year waiver of the professional experience requirement for holding an additional credential on the approved list**
  Valid experience includes information systems security-related work performed as a practitioner, auditor, consultant, investigator or instructor, that requires Information Security knowledge and involves the direct application of that knowledge. The five years of experience must be the equivalent of actual fulltime Information Security work (not just Information Security responsibilities for a five year period); this requirement is cumulative, however, and may have been accrued over a much longer period of time.

A candidate shall be permitted a waiver of one year experience if:

- **Based on a candidate's education**
  Candidates can substitute a maximum of one year of direct full-time security professional work experience described above if they have a four-year college degree or regional equivalent or an advanced degree in information security from the U.S. National Center of Academic Excellence in Information Assurance Education (CAE/IAE).

OR

- **For holding an additional credential on the (ISC)² approved list below**
  Valid experience includes information systems security-related work performed as a practitioner, auditor, consultant, investigator, or instructor that requires information security knowledge and involves the direct application of that knowledge. The five years of experience must be the equivalent of actual full-time information security work (not just information security responsibilities for a five-year period); this requirement is cumulative, however, and may have been accrued over a much longer period of time.

A candidate shall be permitted a waiver of one year experience for holding an additional credential on the (ISC)² approved list below: (continued)
Approved Credentials for Experience Waiver:

- Certified Authorization Professional (CAP)
- Certified Business Continuity Professional
- Certified Computer Examiner (CCE)
- Certified Cyber Forensic Professional (CCFP)
- Certified Ethical Hacker v8
- Certified Forensic Computer Examiner (CFCE)
- Certified Fraud Examiner (CFE)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Internal Auditor (CIA)
- Certified Penetration Tester (GPEN)
- Certified Protection Professional (CPP) from ASIS
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Wireless Security Professional (CWSP)
- Cisco Certified Network Associate Security (CCNA Security)
- Cisco Certified Network Professional Security (CCNP Security)
- Cisco Cyber Security Specialist Program
- CIW – Security Analyst
- CIW Web Security Professional
- CIW Web Security Specialist
- CompTIA Advanced Security Practitioner (CASP)
- CompTIA Security+
- CyberSecurity Forensic Analyst (CSFA)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Forensics Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Global Industrial Cyber Security Professional (GICSP)
- GIAC Information Security Fundamentals (GISF)
- GIAC Information Security Professional (GISP)
- GIAC Mobile Device Security Analyst (GMOB)
- GIAC Penetration Tester (GPEN)
- GIAC Security Essentials Certification (GSEC)
- GIAC Security Leadership Certification (GSLC)
- GIAC Systems and Network Auditor (GSNA)
- Information Security Management Systems Lead Auditor (IRCA)
- Information Security Management Systems Principal Auditor (IRCA)
- Master Business Continuity Professional (MBCP)
- Microsoft Certified IT Professional (MCITP)
- Microsoft Certified Solutions Associate (MCSA)
- Microsoft Certified Systems Engineer (MCSE)
- Systems Security Certified Practitioner (SSCP)
- The International Association for Privacy Professionals (IAPP) Certification

APPENDIX F: SAMPLE CLASS SPECIFICATIONS

Class Specification: Los Angeles County

INFORMATION TECHNOLOGY SECURITY SPECIALIST
ITEM NUMBER: 2603
APPROVAL DATE: 10/15/2013

DEFINITION:
This expert-level class acts as lead technical consultant, systems architect, or project manager for a departmental information technology (IT) security program.

CLASSIFICATION STANDARDS:
Positions allocable to this class work under the general direction of a Departmental Information Security Officer II to provide consultative, systems architecture, and project-management expertise in the development, implementation, and monitoring of a departmental IT security program including related policies and procedures. Incumbents carry out highly-complex and -specialized assignments in one or more areas of IT security-related areas including application, network, physical/environmental, server, and workstation security; and security incident response, awareness training, identity and access management, and risk assessment.

These positions require advanced expertise in the denoted functional areas of information systems security, including applicable legislation regarding protection of IT resources; IT risk assessment strategies and methodologies; security issues related to protection of IT resources; information security best practices; security management and practices; computer threats, vulnerabilities and exploits; and Business Continuity Planning (BCP)/Disaster Recovery Planning (DRP). Incumbents must possess the ability to plan and lead highly-complex and mission-critical IT security projects for a large to very large County department. Also required is the ability to perform risk analyses; handle sensitive matters with discretion and maintain confidentiality; and develop and review technical documentation and narrative reports.

Information Technology Security Specialist is distinguished from Information Technology Security Analyst in that the latter performs routine to complex assignments for an IT security program under the general supervision of an IT supervisor or manager.

EXAMPLES OF DUTIES:
Leads or has primary responsibility for the development, implementation, and monitoring of departmental IT security policies, standards, procedures and guidelines, in accordance with County policies, standards, procedures and guidelines.

- Coordinates and participates in the analysis, design, and implementation of IT security solutions.
- Participates in and directs the development, testing, and verification of departmental computer disk images to standardize implementation of security controls.
- Assesses performance of applications across all components to identify potential vulnerabilities or threats; directs developers and infrastructure support staff in the planning and implementation of countermeasures.
- Ensures that network devices are tested, implemented, and maintained via upgrades, patches, and updates with appropriate security controls such as authentication and configuration.
- Documents network data flows and access controls.
- Conducts and directs risk assessments for identity and access controls.
- Analyzes security hardware and software to determine feasibility of use within the network infrastructure; conducts change control and technical review of proposed changes to IT resources.
- Analyzes system outages, alerts, and reports of abnormal system behavior due to suspected security-related events such as viruses, Trojan activity, and hacker intrusions.
- Monitors, analyzes and responds to security events using security-event management tools.

- Leads and participates in the technical analysis and correlation of security data from computing and network devices to identify potential threats and vulnerabilities or to determine the root cause of a security incident.
- Compiles and validates security-related statistical data for management reporting.
- Directs the development, implementation and evaluation of a departmental security awareness training program and related materials and the training of departmental staff at all levels on security protocols, policies, and procedures.
- Develops compliance strategies for IT security programs; leads the assessment of risks of non-compliance to management's policies, procedures, standards and guidelines and reports findings to appropriate management.
- Leads and participates in the development and implementation of Business Continuity Plans (BCP)/Disaster Recovery Plans (DRP).
- Maintains chain of custody of electronic and or physical evidence related to an IT security incident.
- Directs physical security control assessments and the monitoring and assessing of physical safeguards.
- May supervise IT staff in the performance of security-related assignments.
- May be required to participate in the Countywide Computer Emergency Response Team (CCERT), Departmental Computer Emergency Response Team (DCERT), and Security Engineering Teams (SET).
- May be required to represent the department in legal matters related to IT systems security.

MINIMUM REQUIREMENTS:

TRAINING AND EXPERIENCE:

OPTION 1: Three (3) years of experience in the implementation, management, and monitoring of an IT security program at the level of the Los Angeles County class of Departmental Information Security Officer I.

OPTION 2: Graduation from an accredited college or university with a bachelor's degree in Computer Science, Information Systems, or a closely-related discipline -AND- four (4) years of recent, full-time, highly responsible paid experience managing the security of multiple platforms, operating systems, software, and network protocols for a large IT organization.

OPTION 3: Five (5) years of highly responsible experience in the administration of a minimum of one (1) or more IT security functional areas at the level of Los Angeles County's class of Information Technology Security Analyst.

LICENSE:
A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

PHYSICAL CLASS:
2-Light

SPECIALTY REQUIREMENTS:
Specialized examinations may include one or more of the following:

Specialty / *Add

Application Security management (ASM): Experience in application development using standard IT systems development methodology and techniques for resolving business problems. Includes systems design, database management, development of online data entry and data inquiry capabilities, and defining techniques; communications, network analysis, design, planning and performance tuning.

Identity and Access Management (IAM): Experience assisting with defining, testing, and implementing IT user provisioning and identity management technologies. Includes developing IAM policies, standards, and procedures; identifying appropriate access control techniques; analyzing and selecting IAM solutions; and familiarity with security and system development life cycles (SDLC) processes.

Incident Response Management (IRM): Experience in an IT organization providing technical assistance in computer incident response for potential or actual information-security breaches or attacks. Includes detecting, analyzing, responding to, and reporting information security incidents; and familiarity with the chain-of-custody process.

Network Security Management (NSM): Experience in IT network planning, design, and analysis. Includes assisting in implementing security tools and controls such as intrusion detection/prevention systems, sniffers, and firewalls.

Physical / Environmental Security (PES): Experience assisting with managing physical and environmental IT security methodologies to prohibit unauthorized physical access and prevent damage to IT resources. Includes physical and environmental security planning, design, and analysis.

Policy and Compliance Management (PCM): Experience assisting with developing and implementing IT security policies and standards. Includes assisting in monitoring for compliance.

Risk Assessment Management (RAM): Experience performing IT security risk assessments. Includes assisting in developing and implementing business continuity and disaster recovery plans and in developing risk assessment reports of findings and recommendations for remediation.

Security Awareness Training (SAT): Experience assisting in developing, implementing, and evaluating IT security awareness training programs and related materials. Includes assisting in reporting of training compliance.

Server Security Management (SSM): Experience in IT server (e.g., email, web, application, and database) security management comprised of implementing upgrades, patches, and updates to operating systems, software applications, and security protection software. Includes configuring server environment to protect the integrity of the system, for example by limiting user rights, disabling unnecessary services, and establishing group policies where applicable.

Workstation Security Management (WSM): Experience managing the security of workstation (e.g., desktops, laptops and tablets) and portable devices (e.g., thumb drives and personal digital assistants). Includes implementing upgrades, patches, and updates to operating systems, software applications, and security protection software; establishing group policies and user rights; and disabling unnecessary services where applicable.

State Job Classification – South Carolina Dept. of Administration

IT Security Specialist/ Analyst I - (AM80)

General Nature of Work

Responsible for performing procedures and providing technical solutions that serve to provide appropriate access to and protect systems from intentional or inadvertent access or destruction.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for use at the mid-level.

Examples of Work

Implements and monitors enterprise information security and IT risk management for agency. Works with users to achieve security objectives and address identified risks. Recommends solutions. Translates security requirements into functional specifications. Assists with the analysis and development of security plans for various systems. Assists in developing and validating baseline security configurations for operating systems, applications, networking, and telecommunications equipment. Assists in developing technical documentation (designs, specifications, processes, and workflows) and communications. Carries out procedures to ensure that all systems, products, and services meet agency security standards. Assists units with information security risk assessments. Works with customers and management to identify, select, and implement technical control. Assists with information security training and awareness programs.

Knowledge, Skills and Abilities

Knowledge of security administration for various operating systems and software. Ability to write detailed technical documentation on security procedures. Basic analytical and problem solving skills. Basic knowledge and understanding of information risks concepts and principles as a means of relating business needs and security controls. Ability to communicate with audiences with varying levels of technical knowledge. Basic knowledge of project management.

Minimum Requirements

A bachelor's degree in information technology systems, computer science, or related field and experience in information technology systems or related area. Relevant experience may be substituted for bachelor's degree on a year-for-year basis.

Pay Band – 06 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$38,703.00	$55,155.00	$71,608.00

IT Security Specialist/ Analyst II - (AM81)

General Nature of Work

Responsible for assisting in the evaluation of IT environments and recommending security measures and practices that meet policies and standards and safeguard information assets.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for use at the experienced/ intermediate level, focusing on tasks of medium complexity.

Examples of Work

Works with users to achieve security objectives and address identified risks. Gathers, compiles, and synthesizes information for security processes or systems. Makes recommendations for development of new security systems/procedures or reuse/enhancement of existing security systems/procedures. Analyzes security needs to assess technical feasibility and solutions. Translates security requirements into functional specifications and manages changes. Involved in the full security systems life cycle; designing, coding, testing, implementing, maintaining and supporting software, quality assurance, testing, and deployment. Participates in the development of strategies and plans to achieve security requirements and address identified risks. Develops and validates baseline security configurations for operating systems, applications, networking, and telecommunications equipment. Develop technical documentation (designs, specifications, processes, workflows) and communications. Participates in creating and executing security procedures that ensure that all systems, products and services meet agency security standards, service level agreements and end-user requirements. Analyzes current security processes and procedures to create future configurations which lead to gains in security, efficiency, and cost savings. Consults with users and management with information security risk assessments. Work with users and management to identify, select and implement technical controls. Facilitates information security training and awareness programs.

Knowledge, Skills and Abilities

Knowledge of security administration for various operating systems and software. Ability to write detailed technical documentation on security policies and procedures. Moderate analytical and problem solving skills. Moderate knowledge and understanding of information risks concepts and principles as a means of relating business needs and security controls. Ability to communicate with audiences with varying levels of technical knowledge. Moderate knowledge of project management implementation.

Minimum Requirements

A bachelor's degree in information technology systems, computer science, or related field and experience in information technology systems or related area. Relevant experience may be substituted for bachelor's degree on a year-for-year basis.

Pay Band – 07 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$47,092.00	$67,108.00	$87,125.00

IT Security Specialist/ Analyst III - (AM82)

General Nature of Work

Responsible for evaluating IT environments and recommending security measures and practices that meet policies and standards and safeguard information assets.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for use at the advanced/senior level focusing on tasks of high complexity.

Examples of Work

Provides expertise for the design and development of security systems and procedures within a wide range of complexity levels. Establishes security standards for the agency. Recommends development tools and solutions to develop and enhance security systems and applications. Analyzes users needs to assess technical feasibility and solutions of security systems and processes. Translates security requirements into functional specifications and manages changes. May lead the full systems life cycle; designing, coding, testing, implementing, maintaining and supporting software, quality assurance, testing, and deployment. Develops and validates baseline security configurations for operating systems, applications, networking, and telecommunications equipment. Oversees staff in recreating security problems to resolve security concerns and identify complex problems. Creates and executes procedures that ensure all systems, products and services meet agency security standards, service level agreements, and end-user requirements. Analyzes current processes and procedures to create security plans which lead to gains in security, efficiency, and cost savings. Serves as a subject matter expert associated with highly technical security content, processes and procedures. Consults with users and management in identifying, selecting and implementing technical controls. Establishes and maintains information security training and awareness programs.

Knowledge, Skills and Abilities

Advanced knowledge of security administration for various operating systems and software. Ability to develop project plans for information security systems. Advanced technical knowledge of application and operating system hardening, vulnerability assessments, security audits, and firewalls. Advanced analytical and problem solving skills. Advanced knowledge and understanding of information risks concepts and principles as a means of relating business needs and security controls. Excellent documentation and presentation skills. Ability to explain information security concepts to audiences outside the field.

Minimum Requirements

A bachelor's degree in information technology systems, computer science, or related field and experience in information technology systems or related area. Relevant experience may be substituted for bachelor's degree on a year-for-year basis.

Pay Band – 08 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$57,299.00	$81,655.00	$106,012.00

Sr. IT Security Administrator - (AM85)

General Nature of Work

Responsible for the development and enforcement of security policies and strategy related to the security of agency information assets.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for use for positions that exercise enterprise-wide authority for compliance with information security policies consistent with applicable industry standards and governmental regulations.

Examples of Work

Develops, implements and monitors a strategic, comprehensive enterprise information security and IT risk management system. Manage the agency's security organization. Develops, maintains and publishes up-to-date security policies, standards and guidelines, and oversees training and dissemination of security policies and practices. Facilitates information security governance through implementation of a hierarchical governance program. Creates, communicates and implements a risk-based process for vendor risk management, including assessment and treatment for risks that may result from partners, consultants and other service providers. Identifies requirements for IT security products and services. Creates a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection. Works directly with customers and senior management to facilitate IT risk assessment and risk management processes, and works with stakeholders to identify acceptable levels of residual risk. Oversees the selection, development, deployment, monitoring, maintenance, and enhancement of the agency's security technology. Oversees performance of IT risk assessments, audits, security incident investigations and responses.

Knowledge, Skills and Abilities

Expert level knowledge of security administration for various operating systems and software. Ability to develop project plans for information security systems. Expert technical knowledge of application and operating system hardening, vulnerability assessments, security audits, and incident responses. Expert analytical and problem solving skills. Expert knowledge and understanding of information risks concepts and principles as a means of relating business needs and security controls. Expert level understanding of forensics investigations, intrusion detection systems and firewalls. Excellent documentation and presentation skills. Ability to explain information security concepts to audiences outside the field.

Minimum Requirements

A bachelor's degree in information technology systems, computer science, or related field and experience in information technology systems or related area. Relevant experience may be substituted for bachelor's degree on a year-for-year basis.

Pay Band – 09 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$69,717.00	$99,352.00	$128,987.00

Risk Management & Compliance Analyst I - (AF10)

General Nature of Work

Assists in professional work examining, evaluating, and/or monitoring conformity with laws, regulations, privacy, or other business standards. Participates in licensure and permit compliance activities.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for entry-level professional compliance activities in a state agency.

Examples of Work

Performs research and supports evaluation of the agency's compliance programs and associated policies, standards, procedures and controls. Supports the development of compliance documentation to guide employees in confirming that compliance standards are incorporated into the agency's processes, initiatives and development of information systems. Assists senior analysts in classifying information assets across the agency based on the data classification schema. Monitors the status and effectiveness of controls across departments, and provides reporting and escalation when needed. Assists in the investigation and documentation of complaints and reports results to management. Assists senior analysts in performing review of information systems and/or processes to identify privacy-related vulnerabilities. Participates in the response plan for violations of the agency's privacy and other compliance programs and associated policies, and provides communication to internal departments, including remediation steps. Reports violations of compliance or regulatory standards to duly authorized enforcement agencies as appropriate or required. Assists in deployment of compliance and privacy training awareness and communication programs to educate and update employees on requirements. Participates in the planning and development of information security and privacy audits. Performs investigations, accountability audits and other duties related to alleged violations of all applicable statutes, standards, rules, and regulations. Monitors the agency's compliance with established information security policies, standards, procedures and controls, by scheduling and assisting senior auditors to perform periodic compliance audits. Supports audits of the agency's information security and privacy policies, standards, procedures and controls to determine potential risks. Documents information security and privacy audit results and findings and prepares them for internal review. Identifies current information security and privacy controls and evaluates their operating effectiveness. Informs leadership regarding pending legal, regulatory or industry changes, trends, best practices and assesses the potential impact of these changes on agency processes. Consults legal staff as necessary to address difficult legal compliance issues.

Knowledge, Skills and Abilities

Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls. Ability to understand information privacy laws, policies, procedures and technology. Ability to communicate effectively with others orally and in writing. Knowledge of relevant laws and regulations. Ability to establish and maintain interpersonal relationships. Ability to use relevant information and individual judgment to determine whether events or processes comply with laws, regulations, or standards. Ability to analyze data and information in making decisions and solving problems.

Minimum Requirements

A high school diploma and relevant work experience. A bachelor's degree may be substituted for the required work experience.

Pay Band – 06 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$38,703.00	$55,155.00	$71,608.00

Risk Management & Compliance Analyst II - (AF20)

General Nature of Work

Performs professional work examining, evaluating, and/or monitoring conformity with laws, regulations, privacy or other business standards. Participates in licensure and permit compliance activities.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for journey-level professional compliance activities in a state agency. Some positions in this class may supervise administrative compliance related activities.

Examples of Work

Contributes to the implementation of compliance programs and associated policies, standards, procedures and controls within the organization. Works with others to define and incorporate controls into the organization's processes, initiatives and development of information systems. Identifies information assets and classifies them based on their level of sensitivity, value and criticality to the organization in line with the data classification schema. Works with others to provide mitigation for compliance risks. Investigates complaints and adopts the appropriate steps to respond to and address the complaints. Reports violations of compliance or regulatory standards to duly authorized enforcement agencies as appropriate or required. Works with managers to identify and investigate compliance incidents that violate the organization's compliance programs. Supports management in their role as a liaison for any complaints and/or investigations related to compliance. Supports the development of compliance training and communication programs to educate and update employees on requirements. Performs information security, privacy or other compliance audits. Works with senior auditors and management to develop the scope, objectives and auditing methodology for information security, privacy and other audits. Works with management to maintain and enhance existing information security and privacy audit programs to concur with regulatory changes. Identifies control deviations within the organization's technical infrastructure systems and key information security development initiatives. Works with auditors to document information security and privacy audit results and findings for internal review. Evaluates audit findings to confirm information security and privacy controls are implemented as designed, and that they remain operating effectively. Develops recommendations to remediate control deviancies and mitigate information security and privacy risks. Performs follow-up review on audit procedure issues noted in past audits to confirm they are not repeated in future audits. Keeps informed regarding pending legal, regulatory or industry changes, trends, and best practices and assesses the potential impact of these changes on organizational processes. Consults legal staff as necessary to address difficult legal compliance issues.

Knowledge, Skills and Abilities

Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls. Ability to understand information privacy laws, policies, procedures and technology. Ability to communicate effectively with others orally and in writing. Knowledge of relevant laws and regulations. Ability to establish and maintain interpersonal relationships. Ability to use relevant information and individual judgment to determine whether events or processes comply with laws, regulations, or standards. Ability to analyze data and information in making decisions and solving problems.

Minimum Requirements

A bachelor's degree and relevant experience

Pay Band – 07 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$47,092.00	$67,108.00	$87,125.00

Risk Management & Compliance Manager I - (AF30)

General Nature of Work

Manages and coordinates professional work examining, evaluating, and/or monitoring conformity with laws, regulations, information security, privacy or other business standards. Supervises others in compliance activities.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for journey-level management of professional risk management and compliance activities in a state agency. Participants in this class may manage risk management and compliance activities in a unit or department.

Examples of Work

Oversees and conducts risk management activities (e.g., risk assessment, gap analysis, business impact analysis) to identify current and future threats and to help the organization reach an acceptable level of risk. Plans, organizes and directs regulatory enforcement activities to ensure that all applicable statutes, rules, and regulations are met. Implements processes, standards and baseline thresholds for measurement, monitoring, reporting, mitigation and remediation of identified risks. Assists in the establishment and maintenance of the agency's information security program and associated strategies to support the business processes and overall goals of the organization. Enforces security requirements during the design, development, testing and delivery of information systems to confirm that organization assets are appropriately secure at all times against risks and threats. Establishes and maintains internal and external communication channels to support information security across the organization. Supports the development and review of the organization's governance, risk, and compliance (GRC) strategy that aligns the business, information technology and governance model. Supports the maintenance of the information security framework by updating controls in conjunction with regulatory requirements. Works with Information security and other management to monitor the effectiveness of the organization's GRC processes. Supports the organization's transition to a GRC platform for tracking risks due to non-compliance, information security and privacy control adoption and monitoring for implementation of security controls. Collaborates with management to leverage existing technology investments to support the GRC program Provides support to maintain collaboration among departments across the organization. Supports training deployment to raise GRC program awareness across the organization. Performs research in GRC technology, processes updates, and best practices, and advises management on adoption to improve GRC capabilities. Assists in the development of reports and dashboards to present the level of controls compliance and the current IT risk posture.

Knowledge, Skills and Abilities

Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls. Knowledge of governance, risk and compliance (GRC) program management. Understanding of risk assessment process, monitoring, and reporting. Ability to apply information security principles to business solutions. Ability to act as liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization. Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls. Knowledge in identifying and managing information security risks, threats, and incidents at an enterprise level.

Minimum Requirements

A bachelor's degree and relevant experience

Pay Band – 08 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$57,299.00	$81,655.00	$106,012.00

Risk Management & Compliance Manager II - (AF40)

General Nature of Work

Manages and coordinates professional work examining, evaluating, and/or monitoring conformity with laws, regulations, information security, privacy or other business standards. Supervises others in compliance activities.

Guidelines for Class Use/Distinguishing Characteristics

This class is intended for advanced-level management of professional risk management and compliance activities in a state agency. Manages activities of considerable complexity in a smaller state agency or directs activities in a larger state agency.

Examples of Work

Works with management to develop and implement a governance, risk, and compliance (GRC) strategy that aligns the business, information technology and governance domains. Plans, organizes and directs regulatory enforcement activities to ensure that all applicable statutes, rules, and regulations are met. Provides oversight for the development and implementation of information security processes, procedures and appropriate controls across business units taking into account the people, resources and technologies involved in the processes. Collaborates with agency executive management to define acceptable levels of risk and to establish risk mitigation and management plans at an enterprise level. Provides mentorship, guidance, and relevant technical training to other Information security staff and other departments. Assesses the maturity of existing discrete compliance and risk management programs to support scope definition of the GRC program. Assists in the vendor selection process and development of the agency's GRC platform. Formulates the tactical and strategic information security goals and associated key performance indicators to measure the effectiveness of the agency's information security program and its threat and vulnerability management capabilities. Monitors and suggests improvements to the GRC program. Understands the agency's response plan for risks and threats, and supports the remediation and response process by reporting necessary information and materials to the agency's management. Collaborates across the agency to facilitate proactive alignment between internal and external security requirements and processes and technology to administer GRC . Performs research in GRC technology, processes updates, and best practices, and advises management on adoption to improve GRC capabilities. Develops reports and dashboards to present the level of controls compliance and the current IT risk posture.

Knowledge, Skills and Abilities

Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls. Knowledge of governance, risk and compliance (GRC) program management. Understanding of risk assessment process, monitoring, and reporting. Ability to apply information security principles to business solutions. Ability to act as liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization. Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls. Knowledge in identifying and managing information security risks, threats, and incidents at an enterprise level.

Minimum Requirements

A bachelor's degree and relevant experience

Pay Band – 09 **Federal Category: E2**

Minimum Salary	Salary Mid Point	Maximum Salary
$69,717.00	$99,352.00	$128,987.00

Risk Management & Compliance Manager III - (AF50)

General Nature of Work

Directs and oversees professional work examining, evaluating, and/or monitoring conformity with laws, regulations, information security, privacy or other business standards. Directs compliance activities.

Guidelines for Class Use/Distinguishing Characteristics

The class is intended for directors of risk management and compliance activities statewide or for a large state agency.

Examples of Work

Collaborates with management to develop a compliance program that outlines the agency's compliance vision, mission and goals. Leads the development and maintenance of the agency's information security program and associated strategies with consideration for the business processes and overall goals of the organization. Facilitates collaboration between business functions (e.g., information technology, privacy, information security) to validate compliance with information security policies, standards, procedures, and controls and better understand risks within business processes and initiatives. Oversees the development and performance of vulnerability and risk assessments for business process, network, and applications. Initiates, facilitates, and promotes communications and training activities to reinforce information security awareness throughout the organization. Reviews and revises the privacy program on a periodic basis in light of changes in laws, regulations, or agency policy. Reports on a periodic basis the status of compliance programs to agency's stakeholders and/or management. Provides subject matter expertise regarding applicable state policies, standards, procedures and controls to confirm they are appropriately embedded in the agency's compliance practices. Leverages the data classification schema to establish a procedure to classify the agency's data to protect its confidentiality, integrity, and availability. Establishes controls to help maintain the privacy of the agency's data. Leads impact assessments to identify risks and potential impacts associated with processes, data and systems that are privacy-sensitive. Work with the agency's business units and departments to develop a response plan for privacy and other compliance incidents. May serve as a liaison to regulatory and accrediting bodies. Serves as the overall liaison for any complaints and/or investigations related to privacy and other compliance related issues.

Knowledge, Skills and Abilities

Knowledge of applicable internal and/or external regulatory policies, standards, procedures and controls. Knowledge of governance, risk and compliance (GRC) program management. Understanding of risk assessment process, monitoring, and reporting. Ability to apply information security principles to business solutions. Ability to act as liaison and effectively communicate information security topics (e.g., data constraints, information needs) to both technical and non-technical audiences at all levels of the organization. Knowledge of developing and managing an information security program, including its policies, standards, procedures, technologies, and controls. Knowledge in identifying and managing information security risks, threats, and incidents at an enterprise level.

Minimum Requirements

A bachelor's degree and relevant experience

Pay Band – 10 **Federal Category: E1**

Minimum Salary	Salary Mid Point	Maximum Salary
$84,828.00	$120,884.00	$156,941.00

APPENDIX G: COMPENSATION COMPARISON: CYBERSECURITY POSITIONS

<table>
<tr><th colspan="4">COMPENSATION
(Position Classification)</th></tr>
<tr><th>State of California[8]</th><th>LA County[9]</th><th>South Carolina Dept. of Admin.[10]</th><th>South Carolina Dept. of Admin.</th></tr>
<tr><td>$4,821.00 - $6,333.00
(Assoc. SSS Tech)</td><td></td><td>$3,225.25 - $5,967.33
(IT Security Specialist/Analyst I)</td><td>$3,225.25 - $5,967.33
(Risk Mgmt & Comp Analyst I)</td></tr>
<tr><td>$5,071.00 - $6,669.00
(Assoc. ISA Spec)</td><td></td><td rowspan="3">$3,924.33 - $7,260.42
(IT Security Specialist/Analyst II)</td><td rowspan="3">$3,924.33 - $7,260.42
(Risk Mgmt & Comp Analyst II)</td></tr>
<tr><td>$5,294.00 - $6,962.00
(SSS I Tech)</td><td></td></tr>
<tr><td>$5,295.00 - $6,963.00
(Staff ISA Spec)</td><td></td></tr>
<tr><td>$5,814.00 - $7,642.00
(SSS II Tech)</td><td rowspan="2">$6,244.55 – 8,189.64
(IT Security Analyst)</td><td rowspan="3">$4774.92 - $8,834.33
(IT Security Specialist/Analyst III)</td><td rowspan="3"></td></tr>
<tr><td>$5,824.00 -$7,655.00
(Sr. ISA Spec)</td></tr>
<tr><td>$6,388.00 - $ 8,396.00
(SSS III Tech)</td><td>$7,383.82 – 9,683.73
(IT Security Specialist)</td></tr>
<tr><td>$5,560.00 - $7,311.00
(DPM I)</td><td rowspan="3">$9,572.03
(Range Maximum[11]/Control)
(Department ISO I)</td><td rowspan="4">$5,809.75 - $10,748.92
(Sr. IT Security Administrator)</td><td rowspan="2">$4,774.92 - $8,834.33
(Risk Mgmt & Compliance Mgr I)</td></tr>
<tr><td>$6,115.00 - $8,038.00
(DPM II)</td></tr>
<tr><td>$7,260.00 - $8,656.00
(DPM III)</td><td>$5,809.75 - $10,748.92
(Risk Mgmt & Compliance Mgr II)</td></tr>
<tr><td>$7,982.00 - $9,518.00
(DPM IV)</td><td>$8,628.72 - $13,060.26
(Department ISO II)</td><td>$7,069.00 - $13,078.42
(Risk Mgmt & Compliance Mgr III)</td></tr>
</table>

[8] Source: http://www.calhr.ca.gov/Pay%20Scales%20Library/PS_Sec_15.pdf Updated 7/21/2015
[9] Source: cao.lacounty.gov/pdf/alpha.pdf
Los Angeles County Class and Salary Listing, Effective date April 1, 2015
[10] Source: http://www.jobs.sc.gov/OHR/OHR-browse-class.phtm
[11] A maximum rate that is equal to the fifth step of the standardized salary schedule that ends the range.

APPENDIX H: HISTORICAL INFORMATION SECURITY ANALYST SALARIES[12]

Information Security Analyst Salary Range

As cyber security attacks continue to escalate in frequency, scope and sophistication, businesses and government agencies alike are making it a top priority to hire and retain talented IT security personnel. As a testament to their organizational value, information security analysts' salary is among the highest - and fastest growing - in the IT industry.

Here is a dynamic look at Information Security Analyst salaries, including trends from the leading salary surveys and workforce studies. Use our IT salary calculator, job search and education tools to maximize your own information security salary, and explore the IT security specialist career path for a deep dive into this red-hot field.

[12] http://www.itcareerfinder.com/brain-food/it-salaries/information-security-analyst-salary-range.html

Historical Information Security Analyst Salaries

Starting salary ranges for information security analysts and related job roles from 2013 through 2015:

Job Title	2013 Salary	2014 Salary	2015 Salary	2-Year Change
Info Security Analyst	$95,000 - $129,750	$100,500 - $137,250	$106,250 - $149,000	**+ 12%**
Systems Security Administrator	$89,500 - $123,750	$95,250 - $131,500	$100,000 - $140,250	**+ 11.2%**
Network Security Engineer	$93,500 - $123,250	$99,750 - $131,250	$105,000 - $141,500	**+ 12.1%**
Info. Systems Security Manager	$108,000 - $149,750	$115,250 - $160,000	$122,250 - $171,250	**+ 12.2%**
Chief Security Officer (CSO)	$119,750 - $179,250	$126,750 - $189,750	$134,250 - $204,750	**+ 11.8%**

APPENDIX I:
BILLS FOR CYBER SECURITY TASK FORCE CONSIDERATION
(As of April 28, 2015)

1. California Bills

- AB 195 (Chau (D)) Unauthorized Access to Computer Systems
- AB 670 (Irwin (D)) Security Assessment
- AB 739 (Irwin (D)) Civil Law: Liability: Cyber Security: Threat
- AB 1172 (Chau (D)) California Cyber Security

2. Federal Bills

- HR 1560 (Nunes (R)) Cybersecurity Threat Information Sharing
- HR 1704 (Langevin (D)) Nation Data Breach Notification Standard
- HR 1731 (McCaul (R)) National Cybersecurity Protection Advancement Act
- HR 1770 (Blackburn (R)) Notice of Personal Information Security Breach
- S 178 (Cornyn (R)) Justice for Victims of Trafficking
- S 456 (Carper (D)) Mechanisms for Enabling Cybersecurity Threat Indicator
- S 754 (Burr (R)) Cybersecurity Threats

APPENDIX J: REFERENCES

- Council on CyberSecurity: Cybersecurity Workforce Handbook, A Practical Guide to Managing your Workforce, October 2014 http://www.counciloncybersecurity.org/workforce/workforce-management
- Homeland Security Advisory Council Task Force on CyberSkills Final Report September, 2012 https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf
- Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development, Office of Cybersecurity and Communications National Cyber Security Division, September 2008
- $(ISC)^2$ CISSP Professional Experience Requirement https://www.isc2.org/cissp-professional-experience.aspx
- Job Market Intelligence: Report on the Growth of Cybersecurity Jobs, 2014 Burning Glass Technologies http://www.burning-glass.com/media/4187/Burning%20Glass%20Report%20on%20Cybersecurity%20Jobs.pdf
- National Initiative for Cybersecurity Careers and Studies (NICCS™) http://niccs.us-cert.gov/
- National Initiative for Cybersecurity Education (NICE) Framework http://niccs.us-cert.gov/research/national-cybersecurity-workforce-framework
- NASCIO State IT Workforce: Facing Reality with Innovation, 2015 President's Initiative http://www.nascio.org/publications/documents/NASCIO_StateITWorkforceSurvey2015_WEB.pdf
- NIST Tech Beat: November 8, 2011: NICE Issues Cybersecurity Workforce Framework for Public Comment http://www.nist.gov/itl/cyberwork- 110811.cfm
- Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making, Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council
- State Government Information Security Workforce Development Model, A Best Practice Model and Framework, June 2010 http://msisac.cisecurity.org/awareness/documents/state-government-is-workforce-development-model-june-2010-final.docx
- State of Cybersecurity: Implications for 2015; 2015 ISACA/RSA Conference http://www.isaca.org/CYBER/Pages/state-of-cybersecurity-implications-for-2015.aspx

ACKNOWLEDGEMENTS:

Gary Dias
CISSP
Author, Workforce Development and Training, Objective 1
Co-Chair, Cybersecurity Objective 1 Task Force
California Department of Health Care Services

Christie Borchin
Co-chair, Statewide Cybersecurity Task Force
California Department of Technology

Dolly Roco
Co-author, Workforce Development and Training, Objective 1
California Department of Health Care Services

Kenneth Ma
Researcher, Workforce Development and Training, Objective 1
California Department of Health Care Services

Kevin Fuller
GSEC, GCIA, GSNA, GCIH, GAWN, GPEN, GXPN, GWAPT
Researcher, Workforce Development and Training, Objective 1
California Department of Health Care Services

SPECIAL THANKS TO THE FOLLOWING INDIVIDUALS FOR THEIR SUPPORT OF OBJECTIVE 1:

Carlos Quant
Co-Chair, Cybersecurity Objective 1 Task Force
Labor and Workforce Development Agency

Carla Simmons
California Office of Emergency Services

Chris Chambers
Department of Justice

Ken Foster
California Military Department

Mary DiPietro
California Department of Technology

Mary Morshed
California Department of Technology

Melissa Russell
California Department of Human Resources

Michele Robinson
CA State Chief Information Security Officer
California Department of Technology

Patrick McGuire
California Department of Technology

Robert Pittman
Los Angeles County

Robert Schmidt
California Department of Food and Agriculture

Victoria Craig
California Department of Transportation

Thys Bohr
California Department of Veterans Affairs