CEA ACTION PROPOSAL

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date

2019-03-04

2. Department

Department of Motor Vehicles (DMV)

3. Organizational Placement (Division/Branch/Office Name)

Information Systems Division (ISD)

4. CEA Position Title

Chief Information Security Officer (CISO)

5. Summary of proposed position description and how it relates to the program's mission or purpose. (*2-3 sentences)*

DMV requests establishment of a Career Executive Assignment (CEA) position to serve as the CISO and head of the Security Operations Center (SOC) for the DMV. Under the general direction of the Deputy Director, ISD/Chief Information Officer (CIO), the CISO will be responsible for developing, implementing, administering, and evaluating policies and procedures to ensure the security of DMV's information assets.

6. Reports to: (*Class Title/Level*)

Career Executive Assignment, Level C

7. Relationship with Department Director (*Select one)*

☑ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.

☐ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(*Explain*):

8. Organizational Level *(Select one)*

☐ 1st ☐ 2nd ☑ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

Under the general direction of the Deputy Director, ISD/CIO, the CEA serves as CISO and head of the SOC for DMV. The incumbent is responsible for managing issues affecting information security, operation recovery, and network security. The CEA recommends, develops, and administers policies that comply with risk management industry standards to identify and assess risk associated with DMV's information security assets. The CEA performs the following duties:

Oversees DMV's information security program to support business operations and align with DMV's information security mission, goals, and objectives. Ensures DMV and external partners are in compliance with all applicable legal, statutory, and regulatory requirements. Establishes action plans that include DMV's goals, strategic objectives, and performance measures. Hires, trains, develops, and manages DMV Information Security Office (ISO) personnel.

Ensures the protection of DMV's data and information processing assets by managing vulnerabilities within the information processing infrastructure, managing threats and incidents impacting DMV's information resources, assuring the appropriate use of DMV's information resources, and educating and informing DMV employees of their responsibility to protect customer information security. Develops, implements, and maintains risk analyses including assessments to identify potential vulnerabilities that could threaten the security of DMV's information assets.

Oversees DMV's SOC and provides strategic direction for security monitoring functions. Ensures monitoring, analysis, and necessary actions are taken to ensure DMV's perimeter defense systems are secure from external and internal threats. Ensures information systems within the DMV network infrastructure are monitored for active exploits of known or unknown vulnerabilities. Hires, trains, develops, and manages SOC personnel. Activates incident response appropriate to detected events. Communicates with DMV management, the State Information Security Officer, and law enforcement agencies when incidents involve active or detected threats and exploits to DMV networks and systems.

Collaborates with stakeholders to develop and implement policies for information security management. Develops policies that provide operations guidance to ensure the security of: network equipment and software (servers, routers, etc.), communications and media, and physical information assets. Reviews and ensures compliance with certification and reporting requirements for DMV to its external stakeholders.

Identifies security and risk implications for new technologies. Ensures security improvement actions are evaluated, validated, and implemented.

Represents DMV regarding the security program with the California Department of Finance, California Department of Technology, California State Transportation Agency, and California Governor's Office of Emergency Services.

Ensures configuration management control changes to system software, firmware, hardware, and documentation align with policies, standards, and acceptable risk levels throughout the life of DMV systems. Verifies security measures through audits, reviews, projects, and meetings. Ensures an inventory of security-relevant hardware and software is maintained. Ensures documentation detailing DMV hardware, firmware, and software configuration and all security features is maintained.

Researches and evaluates current and new information security technologies and trends. Performs other related duties as required.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

☑ Program is directly related to department's primary mission and is critical to achieving the department's goals.

□ Program is indirectly related to department's primary mission.

□ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: The information security program is critical to DMV's achievement of its mission to proudly serve the public by licensing drivers, registering vehicles, securing identities, and regulating the motor vehicle industry. To meet its mission, DMV must ensure the data and personal information of its customers are secure and any threats to the security of the information are detected and prevented. Any data breaches would severely impact the trust of DMV's customers and the public. A robust information security program is not only critical to DMV's mission, but is also an essential component to DMV's vision to be a trusted leader in delivering innovative DMV services.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

There are three factors driving the need to establish a CEA to serve as DMV's CISO and head of SOC: increased mobile and online technology, increased scrutiny of DMV's technology and security practices from the State Legislature, and a trend for consolidating security policy and security monitoring into one functional area based on best practices.

Increased Mobile and Online Technology:
The use of tablets was recently implemented in most DMV field offices to streamline the customer intake process. Additionally, vehicle registration, driver license renewals, and address changes are all now available via online applications. The proliferation of mobile technology and increased availability of online applications has dramatically increased the vulnerability of DMV's systems to unauthorized access, corruption, disclosure, and destruction of DMV's information and information systems.

The responsibility of the CISO is to ensure the security, availability, and confidentiality of DMV's information systems. The scope of responsibility has grown dramatically in the past several years as more transactions have migrated from paper-based or in-house processing to online real-time transactions. The domain of the CISO today covers 190 field offices serving 27 million licensed drivers, auto clubs, business partner sites, and headquarters. With the increased demand for cybersecurity comes greater responsibility and a need for greater expertise to protect DMV's information assets.

Increased Scrutiny over DMV's Security and Technology:
DMV has been in the news for several months due to increased customer wait times in field offices, which in turn brought increased scrutiny from the State Legislature and other government officials. In the October 4, 2018, hearing before the Senate Transportation and Housing Committee, one of the various causes for the lengthy wait times discussed was DMV's antiquated Vehicle Registration System. The lack of modern technology to support faster transactions and the associated security raised concerns with some of the committee members. The mobile technology recently implemented in field offices to help streamline intake for REAL ID applicants was also discussed. This raised additional concerns about security and questions about DMV's ability to prevent hacking of mobile technology in field offices. The CISO is instrumental in setting policy to properly manage, evaluate, and respond to risks involving DMV's protected data and must serve as an expert advisor to the DMV Directorate on related matters.

Best Practice to Consolidate Security Policy and Security Monitoring Under the CISO:
Cybersecurity is one of the highest priorities for DMV as it serves nearly every California resident. Customers expect their data to be secure, and DMV cannot afford to breach this trust. The ISO is overseen by the CISO and is responsible for security policies, standards, and procedures to protect the confidentiality, integrity, and availability of DMV's information assets. The ISO is critical to ensuring DMV defends against internal and external threats to its data and information assets. The SOC is an around-the-clock centralized facility that monitors DMV's information assets, systems, and infrastructure, and performs analysis, correlation, investigation, reporting, and remediation on internal and external threats based on security incidents, events, and hunting campaigns. The goal of SOC is to actively manage security threats, vulnerabilities, events, and incidents to ensure the availability of critical systems and increase DMV's overall security posture. Although the SOC supports and closely aligns to the mission of the ISO, the offices are currently in two separate functional areas.

Moving the SOC under the direction of the CISO, alongside the ISO, will allow the department to better manage its resources and monitor DMV's information assets. This aligns with the Department of Technology's recommendation to combine the ISO and SOC, following the model of several other State departments, including the California Department of Transportation, the California Department of Technology, and the California Franchise Tax Board. This increased level of responsibility and scope, in addition to the factors discussed above, requires the establishment of a CEA to serve as CISO.

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

The CEA will be the principal policy maker for the following:

1. Security policies and criteria for protecting and using DMV's information assets, including, but not limited to: preventing unauthorized access, corruption, disclosure, or destruction of DMV's information or information systems to ensure the security, availability, and confidentiality of information assets. In protecting DMV's assets, the CISO protects confidential data for the vast majority of California residents, including voter registration that is transmitted to the California Secretary of State, as well as financial data impacting business partners and third party vendors.

2. Policies that provide operational guidance in securing network equipment and software, communications and media, and physical security systems related to data transmittal and storage. These policies will ensure that connectivity between DMV headquarters, field offices, and business partners is guarded against intrusions.

3. Policies for the SOC to monitor and ensure DMV's perimeter defense systems are secure from internal and external threats. This includes policies related to activating incident response and communicating active or detected threats and exploits to DMV networks and systems. The decisions made in this area will be essential to managing security threats, reducing their impact to the DMV and its customers, and ensuring systems critical to DMV's operations are available to provide ongoing customer service.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

The CISO will have broad decision-making authority in the development, revision, recommendation, and implementation of policies and procedures related to the full scope of the security and monitoring of DMV's information assets. The CISO will be required to identify resolutions to problems by developing timely and effective strategies to improve the programs of the ISO and SOC. The CISO will be responsible for managing, administering, monitoring, and coordinating the programs of the ISO and SOC in accordance with applicable laws, rules, and regulations, as outlined below:

The ISO is responsible for the implementation and management of the following enterprise-wide programs: the Information Security Program, which consists of policies, standards, and procedures to protect the confidentiality, integrity, and availability of DMV’s information assets and to ensure DMV is in compliance with governing authorities; the Risk Management Program, which consists of ongoing system categorizations, data classifications, and risk assessments, and developing mitigation strategies to reduce the probability and impact of risks; the Incident Response Program, which consists of the intake, processing, and reporting of information security incidents, and overseeing departmental incident response communications; and the Information Security Awareness and Training Program, which consists of continuous efforts to provide information security expertise as well as awareness, guidance, and education to DMV information assets users on information and cybersecurity issues.

The SOC is responsible for continuously monitoring DMV’s information assets, systems, and infrastructure and performing analysis, correlation, investigation, reporting, and remediation of internal and external threats based on security incidents, events, and hunting campaigns. The SOC’s core functions include around-the-clock monitoring, cyber threat intelligence analysis, forensic and malware analysis, threat hunting, incident response, and client services support.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The CEA will be responsible for revising existing and/or developing and implementing new policy as new state and federal legislation and regulations impacting the ISO and SOC programs are enacted. The CEA will be responsible for interpreting existing policy by serving as a key advisor and resource to the DMV Directorate regarding information security and monitoring matters and managing, administering, and monitoring the ISO and SOC programs in accordance with applicable laws and rules.