STATE OF CALIFORNIA – DEPARTMENT OF FINANCIAL PROTECTION AND INNOVATION

POSITION DUTY STATEMENT

DFPI-HRO 203 (Rev. 08-21)

NAME [Name of candidate hired]	**EFFECTIVE DATE** [Date position filled]
CLASSIFICATION TITLE Information Technology Manager I	**POSITION NUMBER** 410-113-1405-100
WORKING TITLE Chief Information Security Officer (CISO)	**DIVISION/OFFICE/UNIT/SECTION** Executive/ITSD/Information Security Unit (ISU)
BARGAINING UNIT M01	**GEOGRAPHIC LOCATION** Sacramento

General Statement: Under the general direction of Chief Information Officer, the Information Technology Manager I serves as the department's Chief Information Security Officer (CISO)and is responsible for the development, implementation, and maintenance of department policies and procedures ensuring IT security oversight for the department's information/cyber security program, including technology, data, and information assets. Duties include, but are not limited to, the following:

A. Specific Assignments:

Strategic planning, personnel, infrastructure, inside and outside threats, Internal Affairs, requirements, policy enforcement, emergency planning, security awareness, security operations, and other resources. Maximum security for continued access to external systems required to meet the department's mission, goals, and objectives.

Information Security Engineering/Information Technology Project Management

Manage the development, implementation, and maintenance of Access Control systems and policies; manage the development, implementation, and maintenance of Asset Management and Protection; coordinate physical and environmental security with the department's Facilities Management Office (FMO); coordinate Risk Assessments; Manage and coordinate security assessments; maintain business continuity processes and procedures; develop, implement, and maintain incident response unit, processes, and training; develop, implement, and maintain processes for media protection and system and communication protection; develop, implement, and maintain processes and procedures for configuration management; oversee, monitor, and maintain privacy policies and procedures; Oversee communications and system operations.

Information Security Engineering/Client Services

Oversee audit and assessment efforts; serve as point of contact for acquisitions, development, and maintenance; oversee security training program for meetings and; serve as Chair on the IT Security Change Advisory Board (CAB); attend regular State Information Security Officer meetings; establish and maintain security status report

consistent with state guidelines; evaluate and approve all change requests and security exceptions; lead ISU meetings and participate in IT manager meetings, and attend security training and seminars.

B. Supervision Received

The CISO reports directly to and receives the majority of assignments from the CIO; however, direction and assignments may also come from the California Department of Technology, and the Agency Information Officer.

C. Supervision Exercised

General Direction

D. Administrative Responsibility

Responsible for the day-to-day operations of the Information Security Unit (ISU); lead the information security team to actively monitor the DFPI's security environment for suspicious activity and install security measures to prevent breaches; research new threats and collaborate with the DFPI Network Operations to upgrade software as necessary; provides oversight and direction to staff regarding business goals, priorities, security monitoring and response processes and procedures and other highly critical or sensitive IT security issues; develops, manages, and maintains the data necessary to report metrics on operations; directs all activities related to IT security oversight, security intelligence, and Cybersecurity Protection and Response programs; develops, implements, and maintains an IT security strategic plan and ensures alignment with the goals of the Department's and IT's Strategic Plans.

E. Personal Contacts

In addition to managing staff within the ISU, the CISO represents DFPI when communicating with internal and external stakeholders including program division chiefs, state control agencies, the state data center, state and federal auditors, other information security officers, California Highway Patrol, and various department and state level committees.

G. Functional Requirements

The incumbent generally works 40 hours per week in an office setting and/or telework capacity, with artificial light and temperature control. The use of a personal computer, telephone, copier, and fax machine is essential to the duties of this position. The

position requires bending and stooping to retrieve files, sitting and standing consistent with office work, and light lifting of no more than 25 lbs.

H. Other Information

Exercises good judgment in decision-making, exercises creativity and flexibility in problem identification and resolution, and manages time and resources effectively. Works well with others, under changing priorities, and work irregular hours when workload dictates. Regular attendance and punctuality are essential. Possesses good written and verbal communication skills. The incumbent may be required to travel by various methods of transportation, both locally and out-of-town, for the administration of security purposes.

CONFLICT OF INTEREST

This position is subject to Title 10, § 250.30 of the California Code of Regulations, the Department of Financial Protection and Innovation's Conflict of Interest Regulations, the incumbent is required to submit a Statements of Economic Interests (Form 700) within 30 days of assuming office, annually by April 1st and within 30 days of leaving office.

FINGERPRINTING

Title 11, section 703 (d) of the California Code of Regulations requires criminal record checks of all personnel who have access to Criminal Offender Record Information (CORI). Pursuant to this requirement, applicants for this position will be required to submit fingerprints to the Department of Justice and be cleared before hiring. In accordance with DFPI's (CORI) procedures, clearance shall be maintained while employed in a CORI-designated position. Additionally, the position routinely works with sensitive and confidential issues and/or materials and is expected to maintain the privacy and confidentiality of documents and topics pertaining to individuals or to sensitive program matters at all times.

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Health & Safety analyst.)

_____

Employee Signature Date

_____

Employee's Printed Name, Classification

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

_____

Supervisor Signature Date

_____

Supervisor's Printed Name, Classification