

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Manager I	Cybersecurity Risk Manager
NAME OF INCUMBENT:	POSITION NUMBER:
	280-390-1405-013
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Privacy and Integrated Risk Management Office	
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	Information Technology Manager II
BRANCH:	REVISION DATE:
Information Technology Branch	1/8/2024
Duties Based on: <input checked="" type="checkbox"/> FT <input type="checkbox"/> PT– Fraction _____ <input type="checkbox"/> INT <input type="checkbox"/> Temporary – _____ hours	
2. REQUIREMENTS OF POSITION	
Check all that apply: <input checked="" type="checkbox"/> Conflict of Interest Filing (Form 700) Required <input type="checkbox"/> Call Center/Counter Environment <input type="checkbox"/> May be Required to Work in Multiple Locations <input checked="" type="checkbox"/> Requires Fingerprinting & Background Check <input type="checkbox"/> Requires DMV Pull Notice <input type="checkbox"/> Bilingual Fluency (<i>specify below in Description</i>) <input type="checkbox"/> Travel May be Required <input type="checkbox"/> Other (<i>specify below in Description</i>)	
Description of Position Requirements: (e.g., qualified Veteran, Class C driver's license, bilingual, frequent travel, graveyard/swing shift, etc.)	
3. DUTIES AND RESPONSIBILITIES OF POSITION	
Summary Statement: (Briefly describe the position's organizational setting and major functions)	
Information Technology Domains (Select all domains applicable to the incumbent's duties/tasks.) <input type="checkbox"/> Business Technology Management <input checked="" type="checkbox"/> IT Project Management <input type="checkbox"/> Client Services <input checked="" type="checkbox"/> Information Security Engineering <input type="checkbox"/> Software Engineering <input type="checkbox"/> System Engineering	
<p>Under general direction of the Privacy and Integrated Risk Management Office Manager II, the Information Technology Manager I (ITM I) will manage the daily operations of the Security Risk and Integrated Risk Management (IRM) Unit within the Cybersecurity Division (CSD) and will serve as the Unit Manager overseeing the EDD Cybersecurity Risk Management Program. The CSD provides advice, consultation, and oversight to various EDD lines of business to ensure reasonable and appropriate protection and use of the EDD's information assets. The ITM I is responsible for all aspects of the EDD Cybersecurity Risk Management Program within the Information Technology Branch.</p>	

The incumbent will work closely with staff and customers from other Information Technology Branch (ITB) divisions and other Employment Development Department (EDD) divisions and branches in support of the CSD Risk Management Program.

The Cybersecurity Risk Manager must possess technical, analytical, communication, and interpersonal skills appropriate to the IT management level. The incumbent must be detail-oriented with excellent follow-up abilities. The Cybersecurity Risk Manager must demonstrate tact and good judgment and be able to communicate effectively to develop and maintain effective and cooperative working relationships. The incumbent must be able to adapt easily to changing priorities and maintain consistent, predictable attendance in the performance of the assigned specific functions.

The incumbent contributes to the growth of the ITB into a customer-focused, service organization by following the Branch’s cultural principles and by providing constructive feedback to others within the Branch regarding the application of these principles.

Percentage of Duties	Essential Functions
30%	<p>Conducts, tracks and monitors security risk management activities, identifies critical systems and vulnerabilities within the EDD by:</p> <ul style="list-style-type: none"> • Directing asset management and classification activities. • Overseeing targeted risk assessment[s], managing risk, remediation priorities and recommendations in consultation with system owners. • Overseeing EDD CSD system security plan development and providing security consulting services to assist lines of business in identifying and mitigating vulnerabilities within their respective information technology environments. • Managing EDD’s information security incident reporting activities. • Establishing partnerships with EDD stakeholders including State, federal, and local entities responsible for Information Technology and cybersecurity to share information on potential risks and cyber incidents impacting the EDD. • Reporting on impending security risks and vulnerabilities and providing immediate steps for corrective action. • Leading EDD Cal-CSIRS Incident Response Reporting Team and participating in the investigations of alleged EDD information security violations. • Establishes service levels and develops performance metrics.
30%	<p>Establishes critical enterprise Information Security policies, standards, and procedures to ensure critical EDD assets are protected by:</p> <ul style="list-style-type: none"> • Developing IT security policies, standards, and procedures. • Disseminating information to EDD Information Technology Branch Executives, IT managers on EDD risk posture, critical IT security vulnerabilities, flaws, and remediation. • Overseeing the establishment of EDD risk management control documents to address hazards, threats and risks. • Establishing EDD roles and responsibilities for preventing, detecting, and correcting cybersecurity risks. • Providing technical guidance and leadership to various lines of business and CSD Senior Management Team.

25%	<p>Directs the oversight of EDD IT cybersecurity risk management practices by:</p> <ul style="list-style-type: none"> • Reviewing and approving CSD IT security and capital plans, enterprise IT related policies, standards and procedures. • Tracking of incident reports and remediation activities. • Monitoring security and privacy-based legislation and industry best practices. • Reviewing and revising EDD cybersecurity practices and procedures.
10%	<p>Performs day-to-day management activities:</p> <ul style="list-style-type: none"> • Develops action plans to accomplish CSD goals and objectives in accordance with organizational mission and strategic goal, supports and advocates for management's philosophy, policies, and procedures. • Evaluates staff on completion of their responsibilities; develops and updates duty statements as needed, establishes performance expectations, completes individual development plans annually and probationary reports on a timely basis, and other performance management activities including adherence to the State's progressive discipline policy involving taking corrective or disciplinary action as necessary. • Makes informed and defensible administrative and personnel management decisions in accordance with department and state policies, personnel-related laws, rules established by the EDD Human Resources Services Division administrative processes and procedures, and collective bargaining agreements. • Ensures staff comply with all EDD policies, office standard operating procedures, and protocols. • Encourages unit team building, facilitates cross training and promotes continuous improvement of processes. Implements motivation techniques, promotes training, and creates a positive climate for change. • Fosters methods of creative decision-making and problem solving and provides continuous feedback to managers.
Percentage of Duties	Marginal Functions
5%	Performs other duties as assigned.
4. WORK ENVIRONMENT <i>(Choose all that apply)</i>	
Standing: Occasionally - activity occurs < 33%	Sitting: Frequently - activity occurs 33% to 66%
Walking: Occasionally - activity occurs < 33%	Temperature: Temperature Controlled Office Environment
Lighting: Artificial Lighting	Pushing/Pulling: Occasionally - activity occurs < 33%
Lifting: Occasionally - activity occurs < 33%	Bending/Stooping: Occasionally - activity occurs < 33%
Other: <i>Click here to enter text.</i>	
Type of Environment:	
<input type="checkbox"/> High Rise <input checked="" type="checkbox"/> Cubicle <input type="checkbox"/> Warehouse <input type="checkbox"/> Outdoors <input type="checkbox"/> Other:	
Interaction with Customers:	
<input type="checkbox"/> Required to work in the lobby <input type="checkbox"/> Required to work at a public counter <input type="checkbox"/> Required to assist customers on the phone <input type="checkbox"/> Required to assist customers in person <input type="checkbox"/> Other:	

5. SUPERVISION EXERCISED: (List total per each classification of staff)		
Directly – 3 IT Specialist II; 3 IT Specialist I		
6. SIGNATURES		
Employee's Statement: <i>I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of the Position Statement.</i>		
Employee's Name:		
Employee's Signature:		Date:
Supervisor's Statement: <i>I have reviewed the duties and responsibilities of this position and have provided a copy of the Position Statement to the employee.</i>		
Supervisor's Name:		
Supervisor's Signature:		Date:
7. HRSD USE ONLY		
Personnel Management Group (PMG) Approval		
<input checked="" type="checkbox"/> Duties meet class specification and allocation guidelines.	PMG Analyst Initials	Date Approved
<input type="checkbox"/> Exceptional allocation, STD-625 on file.	dmg	1/31/2024
Reasonable Accommodation Unit use ONLY <i>(completed after appointment, if needed)</i> <i>If a Reasonable Accommodation is necessary, please complete a Request for Reasonable Accommodation (DE 8421) form and submit to Human Resource Services Division (HRSD), Reasonable Accommodation Coordinator.</i> List any Reasonable Accommodations made:		

Supervisor: After signatures are obtained, make 2 copies:

- Send a copy to HRSD (via your Attendance Clerk) to file in the employee's Official Personnel File (OPF)
- Provide a copy to the employee
- File original in the supervisor's drop file