

DUTY STATEMENT

GS 907T (REV. 03/05)

SHADED AREA TO REFLECT RECLASS POSITION NUMBER ONLY**INSTRUCTIONS:** Refer to the Essential Functions Duty Statement Manual for instructions on how to complete the Duty Statement.

RPA-

10286-ETS

EFFECTIVE DATE:

DGS OFFICE OR CLIENT AGENCY Enterprise Technology Solutions	POSITION NUMBER (Agency - Unit - Class - Serial) - - -
UNIT NAME AND CITY LOCATED Information Security Office – West Sacramento	CLASS TITLE Staff Information Systems Analyst (Specialist)
WORKING DAYS AND WORKING HOURS Monday through Friday 8 a.m. to 5 p.m.	SPECIFIC LOCATION ASSIGNED TO 707 3rd St. West Sacramento 95605
PROPOSED INCUMBENT (If known)	CURRENT POSITION NUMBER (Agency - Unit - Class - Serial) 306-072-1312-002

YOU ARE A VALUED MEMBER OF THE DEPARTMENT'S TEAM. YOU ARE EXPECTED TO WORK COOPERATIVELY WITH TEAM MEMBERS AND OTHERS TO ENABLE THE DEPARTMENT TO PROVIDE THE HIGHEST LEVEL OF SERVICE POSSIBLE. YOUR CREATIVITY AND PRODUCTIVITY ARE ENCOURAGED. YOUR EFFORTS TO TREAT OTHERS FAIRLY, HONESTLY AND WITH RESPECT ARE IMPORTANT TO EVERYONE WHO WORKS WITH YOU.

BRIEFLY (1 or 2 sentences) DESCRIBE THE POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS

Under the general supervision of the Information Security Officer (ISO) and as part of the ISO team, the incumbent provides oversight and guides DGS compliance with federal, state and other pertinent regulations, mandates and standards regarding protection of information assets.

% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. <i>(Use additional sheet if necessary)</i>
------------------------------------	---

35%	<p>All work will be accomplished in accordance with State laws, policies and procedures utilizing DGS Information Technology Standards, IT manufactures' specifications, California Government Code (GC), Public Contract Code (PCC), California Code of Regulations (CCR), State Information Management Manual (SIMM), State Administrative Manual (SAM), Governor's Executive Orders (EO), Management Memos (MM), Budget Letters (BL), Administrative Orders (AO), and State IT Governance Guidelines.</p> <p>The Department of General Services' (DGS) Core Values and Employee Expectations are key to the success of the Department's Mission. That mission is to "Deliver results by providing timely, cost-effective services and products that support our customers." DGS employees are to adhere to the Core Values and Employee Expectations, and to perform their duties in a way that exhibits and promotes those values and expectations.</p> <p>ESSENTIALS FUNCTIONS</p> <p>In order to provide quality Information Security Services in accordance with the laws, policies and guidelines:</p> <ul style="list-style-type: none"> • Develops a sustainable Information Security Risk Management program for departmental implementation to maintain an acceptable level of risk mitigation and protection of information assets. • Conducts complex information security gap analysis, summarize findings and make recommendations for an initial departmental information security and privacy baseline and progress in compliance with Federal and State requirements and application of industry best practices. • Supports a partnership with Division Programs and Enterprise Technology Solutions (ETS) in order to facilitate assessment of DGS' business and technology environment and information security program implementation. • Understands DGS' complex and diverse business environment, which has inter-departmental and state-level impact; and a complex information technology environment including large mainframe applications, databases, converged networks, virtual systems and remote access to ensure information security and privacy compliance with control agency mandates.
-----	---

SUPERVISOR'S STATEMENT: I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE

SUPERVISOR'S NAME (Print)

SUPERVISOR'S SIGNATURE

DATE

EMPLOYEE'S STATEMENT: I HAVE DISCUSSED WITH MY SUPERVISOR THE DUTIES OF THE POSITION AND HAVE RECEIVED A COPY OF THE DUTY STATEMENT

The statements contained in this duty statement reflect general details as necessary to describe the principal functions of this job. It should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise balance the workload.

EMPLOYEE'S NAME (Print)

EMPLOYEE'S SIGNATURE

DATE

DUTY STATEMENT

GS 907T (REV. 03/05)

RPA- 10286-ETS

% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. <i>(Use additional sheet if necessary)</i>
25%	<ul style="list-style-type: none"> • Promotes the integration of the Risk Management Program within DGS' operational functions and information technology in the initial development or life cycle of projects, processes, or systems to ensure appropriate risk assessment and mitigation by developing and publishing processes and procedures. <p>In order to ensure that Information Security project priorities are met in accordance with the laws, policies and guidelines:</p> <ul style="list-style-type: none"> • Serves as the project leader for the system analysis, documentation and development of complex Security projects through all phases of lifecycle: facilitation, assisting, planning, initiation, executing, controlling, and close-out activities. • Ensures information security and privacy projects and accountability across the organization. • Ensures project management methodology within the unit and provides support and guidance to project teams. • Ensures proactive communication with customers and management to keep them abreast of project status through meetings, email and status reports.
25%	<p>In order to ensure DGS policies align with Federal and State laws, codes and policies:</p> <ul style="list-style-type: none"> • Develops and maintains Information Security and Privacy policies, standards, guidelines and procedures to ensure compliance. • Reviews Federal and State requirements, industry standards and best practices for interpretation and applicability to the DGS business and technology environment provide recommendations to management for implementation. • Analyzes and comprehends business functions, technical resources and related applicable legal requirements to ensure policy consistency, relevancy, comprehensiveness of information security and privacy policies. • Assess and capture deficiencies in existing information security and privacy policy for improvement or clarification. • Establishes policy that facilitates translation into business and technical standards and procedures. • Align information security policies and practices for compliance with the Information Practices Act, California Public Records Act, Privacy, Health Information Portability and Accountability Act (HIPAA), and other pertinent Federal and State requirements aimed to protect DGS information assets from logical or physical interruption or destruction by integrating an educational and awareness campaign to inform DGS staff. • Research, analyze, and create written policy and related documents in a clear and concise manner.
10%	<p>In order to provide customer service and support in accordance with the laws, policies and guidelines:</p> <ul style="list-style-type: none"> • Works with ETS Customer Relationship Managers, provides security consultation to ETS customers, supported agencies, departments and outside entities in support of Memorandums of Understanding and service level agreements by providing information security and privacy analysis and recommendations. • Increases customer's knowledge and understanding of policies to ensure appropriate development and implementation of standards, guidelines and procedures applicable to all operational environments by disseminating information security and privacy requirements. • Communicates and conducts presentations to provide information sharing to staff and management. • Advocates information security in the initial development or life cycle of projects, processes, or systems to ensure appropriate risk assessment and mitigation by implementing appropriate standards, processes, and procedures.
5%	<p>MARGINAL FUNCTIONS</p> <p>In order to ensure the security and availability of information assets:</p> <ul style="list-style-type: none"> • Maintains abreast of appropriate Federal and State laws or legislation proposals, security and privacy controls and existing and emerging technology, methodologies and industry best practices to ensure departmental compliance with new and changing requirements. • Maintains up-to-date awareness on all types of threats facing DGS systems to provide analysis and recommendations for the protection of DGS information assets. • Provides support to the DGS contingency plan program to ensure appropriate policy development to uphold the availability of DGS' assets and system disaster recovery.

DUTY STATEMENT

GS 907T (REV. 03/05)

RPA- 10286-ETS

% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. <i>(Use additional sheet if necessary)</i>
	<p>KNOWLEDGE AND ABILITIES</p> <p>Knowledge of: Principles of public administration, organization, and management; information technology systems equipment, software, and practices; analytical techniques; complex technical report writing.</p> <p>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.</p> <p>DESIRABLE QUALIFICATIONS</p> <ul style="list-style-type: none"> • Knowledge of Federal and State Laws, Government Codes, regulations and guidelines pertaining to Information Security and Privacy. . Such HIPAA, IRS 1075, California Public Records Act • Knowledge of security and control frameworks, such as FIPS, NIST, ISO 17799\27001, CobiT, COSO and MOF. • Must have knowledge of information security and information technology. • Knowledge of network, PC, and platform operating systems. • Knowledge of current systems software/ hardware, protocols and standards. <p>SPECIAL PERSONAL CHARACTERISTICS:</p> <ul style="list-style-type: none"> • Ability to act independently, be open-minded and flexible to other ideas and solutions, and be tactful. • Ability to identify, define and articulate issues and risks and track, facilitate and monitor their resolution. • Ability to learn new technologies quickly and thoroughly. • Ability to resolve technical problems quickly and tactfully. • Ability to handle multiple projects simultaneously. • Ability to work effectively under tight time constraints, client demands, and the pressure of multiple deadlines. • Communicate by speaking and writing in a clear and concise manner <p>INTERPERSONAL SKILLS:</p> <ul style="list-style-type: none"> • Ability to communicate security related concepts to a broad range of technical and non-technical staff. • Ability to act tactfully in difficult situations; negotiate and resolve issues without confrontation. • Ability to be creative, highly motivated, handle rapidly changing priorities, and demonstrate leadership ability. • Ability to take and follow direction from supervisors. <p>WORK ENVIRONMENT, PHYSICAL OR MENTAL ABILITIES REQUIRED TO PERFORM DUTIES:</p> <ul style="list-style-type: none"> • Wear appropriate attire for a professional office environment. • Communicate effectively with various clients. • Frequent daily use of a personal computer, related software applications, and various peripherals. • Read, understand, and apply knowledge acquired from various security related documents and resources. • Work occasional overtime. • Light physical demands such as exert up to 20 lbs. of force occasionally, and/or up to 10 lbs. of force frequently, and/or a negligible amount of force constantly to move objects. Physical demands are in excess of those of sedentary work. • Effectively work under stress and deadlines.