POSITION DESCRIPTION *(Please Read Instructions on the Back)*

1. Agency Position No: 5148-0

2. Reason for Submission: ☐ Redescription ☒ New ☐ Reestablishment ☐ Other
Explanation *(Show any positions replaced)*

3. Service: ☐ Hdqtrs ☒ Field

4. Employing Office Location: Palo Alto, CA

5. Duty Station: Palo Alto

6. OPM Certification:

7. Fair Labor Standards Act: ☒ Exempt ☐ Nonexempt

8. Financial Statements Required: ☐ Executive Personnel ☐ Employment and Financial

9. Subject to IA Action: ☐ Yes ☒ No

10. Position Status: ☒ Competitive ☐ Excepted *(Specify in Remarks)* ☐ SES (Gen.) ☐ SES (CR)

11. ☐ Supv. ☐ Mgr. ☒ Neither

12. Sensitivity: ☒ 1-Non-Sensitiv ☐ 3-Critical ☐ 2-Noncriti ☐ 4-Special

13. Competitive Level Code: X01

14. Agency Use: Bus Code: 8888

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational	Gra	Initial	Date
a. U.S. Office of Personnel Management						
b. Department, Agency or Establishment						
c. Second Level Review						
d. First Level Review	Security Specialist (Auto Info Sys)	GS	080	12	CP	05/12/08
e. Recommended by Supervisor or Initiating Office						

16. Organization Title of Position *(If different from the official title)*

17. Name of Employee *(if vacant, specify)*

18. Department, Agency, or Establishment: VA Palo Alto Health Care System

a. First Subdivision: Office of the Director

b. Second Subdivision:

c. Third Subdivision:

d. Fourth Subdivision:

e. Fifth Subdivision:

19. Employee Review — This is an accurate description of the major duties and responsibilities of my position.
Signature of Employee *(optional)*

20. **Supervisory Certification.** *I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purpose. relating to appointment and payment of public funds, and that false o misleading statements may constitute violations of such statues or thei implementing regulations.*

a. Type Name and Title of Immediate Supervisor
Signature | Date

b. Typed Name and Title of Higher-Level Supervisor or Manager *(optional)*
Elizabeth Joyce Freeman, Director
Signature | Date 5/12/08

21. **Classification/Job Grading Certification.** *I certify that this position has been classified/graded as required by Title 5, U.S. Code in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.*
Typed Name and Title of Official Taking Action
Carol Phillips, Classification Specialist
Signature | Date 05/12/08

22. Position Classification Standards Used in Classifying/Grading Position.
GS-080, dtd 12/87 & GS-2210, dtd 05/01.

Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be corrected by the agency or the U.S. Office of Personnel Management (OPM). Information on classification/job grading appeals, and complaints on exemption from FLSA is available from the personnel office or OPM.

23. Position Review	Initials	Date	Initials	Date	Initials	Date	Initial	Date	Initial	Date
a. Employee *(optional)*										
b. Supervisor										
c. Classifier										

24. Remarks

25. Description of Major Duties and Responsibilities *(See Attached)*

POSITION DESCRIPTION

Security Specialist (Auto Info Sys), GS-080-12

Introduction:

This position is located in the Office of the Director, Information Security Office (ISO) at the VA Palo Alto Health Care System (HCS). The ISO office mission is to plan, develop, and administer system and information ownership; information and data classification guidelines; standards and procedures. Develops, establishes and maintains standards, procedures and guidelines to promote the security and uninterrupted operation of computer-base applications systems at VA Palo Alto HCS. Identifies and addresses exposures to accidental or intentional destruction, disclosure, modification or interruption of information that may cause serious financial and/or information lost to the VA Palo Also HCS. Is responsible for the protection Facility assets and information which is processed or stored by the VA Palo Alto HCS' computerized systems.

Major Duties:

The incumbent is responsible for implementation of local AIS (Automated Information System) security procedures that assure compliance with the requirements of safeguarding personal and other sensitive data. Identifies and reports suspected or actual AIS security breaches affecting physical environment and equipment, software, ensures user log off of systems, the use of no-fips compliant devices are not used, misuse of data storage, stored data or computer output and other physical and logical security problems that occur. Reviews and evaluates the impact of proposed Health Care System (HCS) changes in AIS security. Reviews daily the sensitive records to find potential violators, starts investigations of suspected violations, handles the Facility computer forensics investigations for criminal activity or abuse. Conducts Internet monitoring and generates Internet usage reports for investigations. Ensures the proper sanitization of hard drives and other storage media. Functions as an internal consulting resource to Stanford Research on information security issues. Functions as a technical advisor/computer technician on the integration of legacy proprietary research devices onto the VA computerized network.

Trains and assists services to facilitate the development of testing of service level contingency plans. Provides Information Security and Information Technology training to OI&T community. Includes development of formal training plans for classroom training, and provides one-on-one training as well. Maintains lists of all local staff designated as remote authorized users of the host system. Notifies ISO office of the transfer or termination of any employee who has system access privileges; ensures that all computer devices under that employee are either returned to the dispensing official or are otherwise identified.

Performs surveys of PC workstations to ensure appropriateness of the software loaded on the PC, assists with alternate coordination duties and responsibilities for desktop support,

server, network support VISTA/PIMS (Patient Information Management System) and IT project management for the installation of new equipment. Reviews application and data analysis, and AMIS Reports coordination for the HCS. Protects assets from damage, destruction, alteration and misappropriation, including fire, safety and planning for contingencies. The incumbent is a member of IMC, ADPAC, IT Audit Subcommittee, R&D Environmental Rounds Teams, and the Info Sec & Privacy Unannounced Assessments Team.

Factors:

1) Knowledge Required by the Position

Knowledge of methods for evaluating, implementing and disseminating IT security tools and procedures sufficient to develop, implement and coordinate activities designed to ensure, protect and restore IT systems, services and capabilities. Knowledge of network operations and protocols to provide advice and guidance in implementing IT security policies and procedures in the development and operations of network systems. Ability to communicate a clear, logical and concise explanation of information both orally and in writing. Knowledge of Research daily operations and protocols of a research environment.

2) Supervisory Controls

The supervisor outlines broad objectives and available resources. The incumbent sets his/her own timeframes and scope of the assignments, including possible approaches. The incumbent independently plans and carries out projects and analyses, interprets policies, procedures and regulations. Resolves conflicts as they arise. Technical judgments are almost always un-reviewed by the supervisor. The incumbent has the authority to analyze and make technical decisions that may lead to security program changes and operational decisions. Keeps the supervisor informed the of broad direction of future program planning.

3) Guidelines

A wide variety of reference materials and manuals are available but are not directly applicable or has gaps in significant areas. Precedents are available outlining the preferred approach to more general problems or issues. The employee uses judgment in adapting guides and precedents for application to the assigned project or gathers considerable information to supplement gaps or lack of specificity to particular problems.

4) Complexity

Assignments consist of a variety of duties that involve many different and unrelated processes and methods pertinent to the IT field. Deciding what needs to be done involves evaluating unusual circumstances complicated by incomplete or conflicting data that must be analyzed to determine the applicability of established methods or the

consideration of difference approaches. Judgment and originality are use in interpreting data, planning the work and perfecting the methods and techniques being used.

5) Scope and Effect

The work involves a variety of problems, questions or situations that are dealt with in accordance with established criteria. The work affects the operating of IT systems security and the quality and reliability of services.

6) Personal Contacts

Contacts are with HCS management and staff, consultants, computer personnel of other VA's or VACO. Contacts are often made in an unstructured setting. Contacts may include officials several managerial levels above the employee when such contacts occur on an ad hoc or other irregular basis.

7) Purpose of Contacts

The purpose of contacts is to persuade program managers and other decision making officials with differing goals and interests to follow a recommended course of action consistent with established, or changing, security policies and objectives. Contacts may be made to discuss and resolve derogatory or potentially derogatory information that may affect the ability of employees to continue to use computers at the health care system. At this level the incumbent must ensure health care system management and staff are fully in compliance with security laws and policies.

8) Physical Demands

The work is primarily sedentary. Duties may require lifting and carrying computer equipment such as monitors and printers.

9) Work Environment

The work area is adequately lighted, heated and ventilated. The environment involves everyday risks or discomforts that require normal safety precautions.