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

1. Agency Position No.
DOII007

2. Reason for Submission
□ Redescription ☒ New
□ Reestablishment □ Other
Explanation *(Show any positions replaced)*
New DOI Standard PD

3. Service
□ Hdqtrs □ Field

4. Employing Office Location

5. Duty Station

6. OPM Certification No.

7. Fair Labor Standards Act
☒ Exempt □ Nonexempt

8. Financial Statements Required
□ Executive Personnel Financial Disclosure □ Employment and Financial Interest

9. Subject to IA Action
☒ Yes □ No

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

11. Position Is
☒ Supervisory
□ Managerial
□ Neither

12. Sensitivity
□ 1–Non-Sensitive □ 3–Critical
□ 2–Noncritical Sensitive □ 4–Special Sensitive

13. Competitive Level Code

14. Agency Use

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational Code	Grade	Initials	Date
a. Office of Personnel Management						
b. Department, Agency or Establishment	Supervisory IT Cybersecurity Specialist	GS	2210	15	rl	04/11/2019
c. Second Level Review						
d. First Level Review						
e. Recommended by Supervisor or Initiating Office						

16. Organizational Title of Position *(if different from official title)*

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

18. Department, Agency, or Establishment
Department of the Interior

a. First Subdivision

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 purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.*

a. Typed Name and Title of Immediate Supervisor

Signature

Date

b. Typed Name and Title of Higher-Level Supervisor or Manager *(optional)*

Signature

Date

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
Renae Lockwood,
Classification Program Manager

Signature
RENAE LOCKWOOD
Digitally signed by RENAE LOCKWOOD
Date: 2019.04.10 13:26:32 -04'00'

Date
04/10/2019

22. Position Classification Standards Used in Classifying/Grading Position
Administrative Work in the Information Issued: May 2001 Technology Group, 2200 Revised: 8/03, 9/08, 5/11, October 2018, General Schedule Supervisory Guide HRCD-5 June 1998

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

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

24. Remarks

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

Instructions for Completing Optional Form 8
POSITION DESCRIPTION

In order to comply with the requirements of FPM Chapter 295, subchapter 3, and other provisions of the FPM, agencies must complete the items marked by an asterisk. Agencies may determine what other items are to be used.

*1. Enter position number used by the agency for control purposes. *See FPM Chapter 312, Subchapter 3.*

*2. Check one.

- "Redescription" means the duties and/or responsibilities of an existing position are being changed.
- "New" means the position has not previously existed.
- "Reestablishment" means the position previously existed, but had been cancelled.
- "Other" covers such things as change in title or occupational series without a change in duties or responsibilities.
- **The "Explanation" section should be used to show the reason if "Other" is checked, as well as any position(s) replaced by position number, title, pay plan, occupational code, and grade.**

3. Check one.

*4. Enter geographical location by city and State (or if position is in a foreign country, by city and country).

*5. Enter geographical location if different from that of #4.

6. To be completed by OPM when certifying positions. (See Item 15 for date of OPM certification.) For SES and GS-16/18 positions and equivalent, show the position number used on OPM Form 1390 (e.g., DAES0012).

*7. Check one to show whether the incumbent is exempt or nonexempt from the minimum wage and overtime provisions of the Fair Labor Standards Act. See FPM Chapter 551.

8. Check box if statement is required. See FPM Chapter 734 for the Executive Personnel Financial Disclosure Report, SF 278. See FPM Chapter 735, Subchapter 4, for the Employment and Financial Interests Statement.

9. Check one to show whether Identical Additional positions are permitted. See FPM Chapter 312, Subchapter 4. Agencies may show the number of such positions authorized and/or established after the "Yes" block.

10. Check one. See FPM Chapter 212 for information on the competitive service and FPM Chapter 213 for the excepted service. For a position in the excepted service, enter authority for the exception, e.g., "Schedule A-213.3102(d)" for Attorney positions excepted under Schedule A of the Civil Service Regulations. SES (Gen) stands for a General position in the Senior Executive Service, and SES (CR) stands for a Career Reserved position.

11. Check one.

- A "Supervisory" position is one that meets the requirements for a supervisory title as set forth in current OPM classification and job-grading guidance. Agencies may designate first-level supervisory positions by placing "1" or "1st" after "Supervisory."
- A "Managerial" position is one that meets the requirements for such a designation as set forth in current OPM classification guidance.

12. Check one to show whether the position is non-sensitive, noncritical sensitive, critical sensitive, or special sensitive for security purposes. If this is an ADP position, write the letter "C" beside the sensitivity.

13. Enter competitive level code for use in reduction-in-force actions. See FPM Chapter 351.

14. Agencies may use this block for any additional coding requirement.

*15. Enter classification/job grading action.

- For "Official Title of Position," see the applicable classification or job grading standard. For positions not covered by a published standard, see the General Introduction to "Position Classification Standards," Section III, for GS positions, or FPM Supplement 512-1, "Job Grading System for Trades and Labor Occupations," Part 1, Section III.
- For "Pay Plan code, see FPM Supplement 292-1, "Personnel Data Standards," Book III.
- For "Occupational Code," see the applicable standard; or, where no standard has been published, see the "Handbook of Occupational Groups and Series of Classes" for GS positions, or FPM Supplement 512-1, Part 3, for trades and labor positions. **For all positions in scientific and engineering occupations, enter the two-digit functional classification code in parentheses immediately following the occupational code, e.g., "GS-1310(14)."** The codes are listed and discussed in the General Introduction to "Position Classification Standards," Section VI.

16. Enter the organizational, functional, or working title if it differs from the official title.

17. Enter the name of the incumbent. If there is no incumbent, enter "vacancy."

*18. Enter the organizational location of the position, starting with the name of the department or agency and working down from there.

19. If the position is occupied, have the incumbent read the attached description of duties and responsibilities. The employee's signature is optional.

*20. This statement normally should be certified by the immediate supervisor of the position. At its option, an agency may also have a higher-level supervisor or manager certify the statement.

*21. This statement should be certified by the agency official who makes the classification/job grading decision. Depending on agency regulations, this official may be a personnel office representative, or a manager or supervisor delegated classification/job grading authority.

22. Enter the position classification/job grading standard(s) used and the date of issuance, e.g., "Mail and File, GS-305, May 1977."

23. Agencies are encouraged to review periodically each established position to determine whether the position is still necessary and, if so, whether the position description is adequate and classification/job grading is proper. See FPM Letter 536-1 (to be incorporated into FPM Chapter 536). This section may be used as part of the review process. The employee's initials are optional. The initials by the supervisor and classifier represent recertifications of the statements in items #20 and #21 respectively.

24. This section may be used by the agency for additional coding requirements or for any appropriate remarks.

*25. Type the description on plain bond paper and attach to the form. The agency position number should be shown on the attachment. See appropriate instructions for format of the description and for any requirements for evaluation documentation, e. g., "Instructions for the Factor Evaluation System," in the General Introduction to "Position Classification Standards," Section VII.

Supervisory IT Cybersecurity Specialist

GS-2210-15

INTRODUCTION

The Department of the Interior (Department) manages 451 million acres of the nation's public lands (about one-sixth of the land in the U.S.) and more than 2,500 operating sites, all requiring protection of information and Information Technology (IT) assets. This is a standardized position description for positions located in the various Bureaus and Bureau Offices (Bureau/Office) of the Department.

IT Security Program Services include: providing information technology (IT) security leadership and policy implementation across DOI; offering a centralized resource for cybersecurity information, awareness, planning, reporting, and compliance; providing IT security development and implementation plans; providing IT security operations and implementation requirements to the DOI IT Infrastructure Network and Application Systems; implementing the Federal Information Security Management Act (FISMA), Information System Security, and Privacy and training requirements; ensuring that end users adhere to security policy and guidelines as well as complete mandatory security training in a timely manner; and conducting IT security testing and Assessment and Authorization to meet DOI operations requirements.

This is a National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework (Framework). The incumbent performs Cybersecurity roles and responsibilities outlined in the NICE Framework. The NICE Framework provides Work Role Descriptions associated with Work Roles and Cybersecurity Codes.

MAJOR DUTIES 75%

Ensures confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information system security program policies, procedures, and tools within and across the enterprise. Advises on all assigned information security support programs and initiatives aimed at identifying and safeguarding systems against new vulnerabilities or that involve information security. Promotes the awareness of security issues ensuring sound security principles and appropriate project and resource integration are documented and justified. Ensures project duplications are avoided and project goals and objectives are in harmony with one another, as well as the cybersecurity program's strategic and mission direction.

Provides leadership and managerial direction to subordinate staff responsible for providing information security management and the rigorous application of cybersecurity/information assurance policies, principles, and practices in the delivery of planning and management services to all components of the enterprise. Provides policy guidance to staff through the discussion of overall specific problems, which may be precedent setting, extremely complex, and/or very unusual. Develops and maintains information security guidelines, policies, plans and procedures ensuring effective conduct of assigned missions, functions, and operations of the bureau/office.

Reviews IT security programs to assess overall compliance with cybersecurity plans and policies, as well as their alignment with business requirements. Modifies cybersecurity policies and processes to respond to changes in business requirements and processes and/or changes in policy or regulatory requirements. Evaluates the impact of new cybersecurity guidance on current programs and recommend changes to existing policies and processes to ensure compliance and responsiveness.

Leads efforts to develop, implement, and manage long and short-term IT security plans in compliance with the bureau's security and IT strategic plan to ensure information security programs and procedures are aligned with the Department's IT security program. Provides expert input to the development and implementation of the bureau's mission, goals, and objectives as an authority on safeguarding systems and information. Updates and coordinates changes to these plans as events occur, e.g., changing regulations, cutting edge systems and/or technology, new risks or vulnerabilities, and ensures that these plans are coordinated and understood by stakeholders throughout the bureau/office.

Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology security goals, and reduce overall organizational risk. Oversee expenses and budgetary obligations of the bureau/office, understanding and guiding costs, expenses, and contractor oversight and input if warranted, in support of fiscal year budgetary planning and operations.

Participates in formal and informal management planning, policy and decision- making sessions regarding legislative changes, technological improvements, and changes in Federal and non-Federal policies and standards are followed during development, implementation and maintenance of security programs. Reviews recommendations proposed by management and technical specialists for compatibility with stated mission goals and objectives. Monitors relationships with internal and external customers on a continuing basis concerning cybersecurity development initiatives. Assesses potential problem areas and personally intervenes to restore or *improve the level of confidence and cooperation required to efficiently meet mission objectives.*

Performs other duties as assigned.

Supervisory/Managerial Responsibilities 25%

Through a staff of subordinate supervisors manages the planning, direction, and execution of all organizational operations; and provides administrative and technical oversight to subordinate staff. Determines goals and objectives that need additional emphasis; determines the best approach or solution for resolving budget shortages; and plans for long range staffing needs, to include whether to contract out work. Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support IT security goals, and reduce overall organizational risk. Plan work to be accomplished and establishes priorities and deadlines through subordinate supervisors and/or team leaders for employees based upon workload and abilities. Provides advice and counsel to staff, interviews and selects candidates for positions within the bureau/office, makes promotions and reassignments, hears and resolves complaints from employees, initiates disciplinary action if required; and ensures specialized training is provided to enhance individual and collective operational effectiveness of personnel commensurate with their responsibilities. Ensures reasonable equity among subordinates concerning performance standards, rating techniques, and assessment of subordinates. Initiates and makes recommendations pertaining to employee awards; approves/disapproves leave, and hears and promotes acceptance and adherence to the provisions of the Equal Employment Opportunity Program. Exercises significant responsibilities in engagement with security leadership, and other bureau/offices within the Department.

GENERAL SCHEDULE SUPERVISORY GUIDE FACTORS

Factor 1 — Program Scope and Effect (FL 1-4/775 PTS)

Directs a program responsible for aspects of information systems security to ensure confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information system security program policies, procedures, and tools within and across the enterprise. As a recognized expert in the field of information security, provides authoritative guidance to senior Department officials across the enterprise regarding information security support programs and initiatives aimed at identifying and safeguarding systems against new vulnerabilities or that involve information security. The work performed and supervised by the employee is critical to carrying out the Department's mission and affects all national programs administered by the bureau/office through initiating and administering actions that meet several DOI strategic objectives.

Factor 2 - Organizational Setting (FL 2-2/250 PTS)

The employee is accountable to a position that is one reporting level before the first SES equivalent position.

Factor 3 — Supervisory/Managerial Authority Exercised (FL 3-3b/775 PTS)

As a second-level supervisor, manages the planning, direction, and execution of the bureau/office operations; and provides technical and administrative supervision to a staff, including Federal government employees and contractors through subordinate supervisors and/or team leaders. Exercises the following supervisory authorities and responsibilities: 1) Uses subordinate supervisors and/or team leaders to direct, coordinate, and oversee the work and provide similar oversight of contractors; 2) Exercises significant responsibilities in dealing with officials of other Department organizations, other Federal agencies, state and local government agencies, commissions, and non-government organizations; 3) Assures reasonable equity of performance standards and rating techniques and assures comparable equity in the assessment of the adequacy of contractor capabilities or contractor completed work; 4) Makes decisions on work problems presented by subordinate supervisors, team leaders or contractors; 5) Evaluates subordinate supervisors and serves as the reviewing official on evaluations as appropriate; 6) Makes, approves or recommends selections for subordinate positions; 7) Hears and resolves group grievances or serious employee complaints; 8) Determines whether contractor- performed work meets standards of adequacy necessary for authorization of payment; 9) Recommends awards or bonuses for personnel and changes in position classification; and 10) Finds and implements ways to promote team building and/or improve business practices.

Factor 4 - Personal Contacts

Subfactor 4A — Nature of Contacts (FL 4A-3/75 PTS)

Contacts, which are related to enterprise-wide information security and privacy program, involves interaction with senior level managers and IT professionals throughout the Department as well as program managers, consultants, contractors, and/or vendors. The settings for these contacts can be both formal, e.g., when serving on departmental or interagency working groups, and informal. Many of the contacts also require significant preparation prior to the meeting due to the technical complexity of the issues at hand.

Subfactor 4B - Purpose of Contacts (FL 4B-3/100 PTS)

The purpose of the contacts is to inform, influence, motivate, or persuade and gain support for key IT Cybersecurity initiatives; determine, justify and negotiate priorities with management and stakeholders; discuss specific operational matters, IT projects, and their related technical or administrative issues; and represent the bureau/office in a variety of settings. In many cases, the employee must explain complex technical concepts and operations to lay individuals. At other times, due to the cost and impact of decisions, the employee must negotiate/resolve conflicts and *problems, and influence program managers to use recommended technical solutions that address* cybersecurity program needs. Contacts usually involve active participation in meetings and briefings.

Factor 5 - Difficulty of Typical Work Directed (FL 5-8/1030 PTS)

The highest grade-level of nonsupervisory work managed is GS-13.

Factor 6 - Other Conditions (FL 6-5b/1225 PTS)

Directs, controls, and supervises program work, that through subordinate supervisors and/or team leaders requires exceptional and extensive coordination and integration of a number of very important and complex program segments of personnel security management work comparable in difficulty at the GS-13 grade level, involving extreme urgency to help protect DOI against potential IT threats and vulnerabilities; and to ensure compliance with Federal mandates and legislation, including the Federal Information Security Management Act and the President's Management Agenda. The Department's cybersecurity program plays an important role in protecting the bureau/office's ability to provide mission-critical operations. Projects managed include conducting studies to identify improvements in the way IT security capabilities are applied to key business functions for the agency; and to develop plans and strategies to modify the IT security infrastructure to support short and long range agency goals and objectives. The work requires extensive coordination and integration of activities with senior management throughout the IT enterprise and requires extensive analysis prior to providing effective cybersecurity solutions. The issues addressed are rapidly evolving and the incumbent must consider probable areas of future change in system designs and technology in order to meet later requirements and programmatic strategies that deal with shifting priorities, resources, and funds. The employee provides authoritative advice to senior-level management and makes recommendations involving the adoption of new technologies to improve the efficiency of program operations.

TOTAL POINTS: 4283

POINT RANGE: 4055-up

FINAL DETERMINATION: GS-15