

POSITION DESCRIPTION (Please Read Instructions on the Back)1. Agency Position No.
DOI010

2. Reason for Submission

☐ Redescription ☒ New
☐ Reestablishment ☐ OtherExplanation (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	IT Cybersecurity Specialist	GS	2210	13	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

c. Third Subdivision

a. First Subdivision

d. Fourth Subdivision

b. Second 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

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

Signature

Date

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.

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

Typed Name and Title of Official Taking Action

Rena Lockwood,
Classification Program Manager**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.

Signature

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

Date

04/10/2019

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.

IT Cybersecurity Specialist

GS-2210-13

INTRODUCTION

The Department of the Interior (DOI) 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 DOI.

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

Serves as the principal bureau/service contact or Office of the Chief Information Officer (OCIO) contact for coordination, implementation, and/or enforcement of assigned information cybersecurity policies and portfolios. Implements higher-level security requirements; integrates security programs across disciplines; defines the scope and level of detail for security plans and policies; assesses new systems design methodologies to improve software quality; leads or performs implementation activities; institutes measures to ensure awareness and compliance; identifies the need for changes based on new security technologies or threats; reviews and evaluates security incident response policies; develops long-range plans for IT security systems; reviews new systems, networks, and software designs for potential security risks; and resolves integration issues related to the implementation of new systems with the existing infrastructure.

Initiates, develops, implements, and evaluates security programs, including the implementation of security programs designed to anticipate, assess, and minimize system vulnerabilities such as intrusion detection or access authentication programs. Leads and coordinates the implementation of security programs across platforms and establishes vulnerability reporting criteria; enforces proper backup procedures for all system and network information; and enforces legal controls

that provide protection from unauthorized access, alteration, loss, disclosure, and blocking of information.

Drafts and/or develops operational policies, procedures, and criteria for interfacing with program systems resources, and coordinates with other OCIO, OIS, and OpDiv staff on the development of information security systems and application policies, guidelines, standards, requirements, and procedures. Recommends ways to protect the bureau/office's information and information systems.

Develops and provides compliance oversight for implementation of systems cybersecurity policies, guidelines and procedures related to web-based applications, network, and systems designs. This includes initial design, system lifecycle change review, and configuration management.

Provides expert advice, counsel, and instruction to employees and supervisors on cybersecurity issues, and establishes and maintains strong relationships with internal and external groups working with legal, internal audits, physical security, and other information security matters as assigned.

Reviews and evaluates cybersecurity incident response policies; identifies the need for changes based on new security technologies or threats; tests and implements new policies; and institutes measures to ensure awareness and compliance. Advises and provides technical oversight and assistance to staff in carrying out security development, implementation, operations, and maintenance requirements when staff members install or update software, networks, and applications.

Performs other similar duties as assigned.

FACTORS

Factor 1 - Knowledge Required by the Position (FL 1-8/1550 Points)

Mastery of, and skill in applying, advanced IT security and cybersecurity principles, concepts, methods, standards, and practices sufficient to provide expert technical advice, guidance, and recommendations to management and other technical specialists on critical IT cybersecurity issues; apply new developments to previously unsolvable problems; and make decisions or recommendations that significantly influence important agency IT policies or programs.

Mastery of, and skill in applying, total infrastructure protection environment; and Federal information systems security protocols sufficient to integrate information systems cybersecurity with other security disciplines; and ensure coordination and/or collaboration on security activities throughout the bureau/service and with DOI.

Mastery of, and skill in applying IT systems security principles, concepts, and methods; and the infrastructure protection environment sufficient to develop long-range plans for IT security systems that anticipate, identify, evaluate, mitigate, and minimize risks associated with IT systems vulnerabilities.

Mastery of, and skill in applying information systems security principles and concepts, the enterprise IT architecture, new IT security developments, and project management principles and methods sufficient to lead the implementation of security programs designed to anticipate, assess, and minimize system vulnerabilities and to coordinate the implementation of security programs across platforms and establishes vulnerability reporting criteria.

Knowledge of Federal InfoSec directives, policies, procedures, guidelines, and standards in order to respond to the Office of the Inspector General under the Information Technology Management Reform Act of 1996.

Mastery of, and skill in applying information systems security concepts and methods, multiple IT disciplines, enterprise IT architecture, and project management principles and methods sufficient to perform the following for assigned portfolios: review, evaluate and draft/develop security policies; identify need for and develop changes based on new security technologies or threats; test and implement new policies; and institute measures to ensure awareness and compliance throughout the bureau/service and/or DOI.

Knowledge of file system management, secure data transfer, backup system management, and performance monitoring and management.

Knowledge of server level security concepts and methods to ensure the development and implementation of security policies and plans that ensure a robust level of protection is provided for applications and databases.

Ability to communicate, orally and in writing, complex technical requirements to non-technical personnel and prepare and present briefings to senior management officials on complex and controversial issues.

Factor 2 - Supervisory Controls (FL 2-4/450 Points)

The supervisor outlines overall objectives and available resources. The employee and supervisor, in consultation, discuss timeframes, scope of the assignment including possible stages, and possible approaches. The employee determines the most appropriate principles, practices, and methods to apply in all phases of assignments, including the approach to be taken, degree of intensity, and depth of research in management advisories. Frequently interprets regulations on his/her own initiative, applies new methods to resolve complex and/or intricate, controversial, or unprecedented issues and problems, and resolves most of the conflicts that arise; and keeps the supervisor informed of progress and of potentially controversial matters. The supervisor reviews completed work for soundness of overall approach, effectiveness in meeting requirements or producing expected results, the feasibility of recommendations, and adherence to requirements. The supervisor does not usually review methods used.

Factor 3 - Guidelines (FL 3-4/450 Points)

The employee uses guidelines and precedents that are very general regarding agency policy statements and objectives. Guidelines specific to assignments are often scarce, inapplicable, or have gaps in specificity that require considerable interpretation and/or adaptation for application

to issues and problems. The employee uses judgment, initiative, and resourcefulness in deviating from established methods to modify, adapt, and/or refine broader guidelines to resolve specific complex and/or intricate issues and problems; treat specific issues or problems; research trends and patterns; develop new methods and criteria; and/or propose new policies and practices.

Factor 4 - Complexity (FL 4-5/325 Points)

Work consists of establishing, implementing, and interpreting the requirements for agency compliance with higher level policy directives and Executive orders governing infrastructure protection. The employee performs the following duties: coordinates the review and evaluation of the agency infrastructure protection program, including policies, guidelines, tools, methods, and technologies; identifies current and potential problem areas; updates or establishes new requirements; and makes recommendations for a fully compliant infrastructure protection program to be implemented throughout the agency. The employee exercises considerable judgment in: monitoring agency compliance with infrastructure protection requirements across IT programs; and adjusting program guidelines in response to changing technologies.

Factor 5 - Scope and Effect (FL 5-4/225 Points)

Work involves developing, implementing, and administering an information cybersecurity program within an assigned portfolio for a bureau/service or for the OCIO, consisting of standards, procedures, and guidance designed to protect information available on a major wide area network from unauthorized access. The work involves establishing criteria, formulating projects, assessing program effectiveness and investigating and analyzing a variety of unusual conditions, problems, or issues. Work ensures protection of the bureau/office's IT assets through the administration of effective IT cybersecurity programs. The work impacts the effectiveness of the Department's cybersecurity program.

Factor 6 - Personal Contacts (FL 6-3/60 Points)

Contacts are with individuals or groups from outside the agency, including consultants, contractors, and/or vendors in moderately unstructured settings. Contacts are related to technological information and developments applicable to assigned IT security projects. Contacts may also include agency officials who are several managerial levels removed from the employee when such contacts occur on an ad hoc basis. The employee must recognize or learn the role and authority of each party during the course of the meeting.

Factor 7 - Purpose of Contacts (FL 7-C/120 Points)

The purpose of contacts is to influence and persuade employees and managers to accept and implement findings, advice, guidance, and recommendations in the technology specialty area(s) of the position. The employee may encounter resistance as a result of issues such as organizational conflict, competing objectives, or resource problems. The employee must be skillful in approaching contacts to obtain the desired effect (e.g., gaining compliance with established policies and regulations by persuasion or negotiation).

Factor 8 - Physical Demands (FL 8-1/5 Points)

The work is primarily sedentary. Some work may involve travel to and attendance at meetings and conferences away from the work site. Some employees may carry light items such as papers, books, or small parts, or drive a motor vehicle. The work does not require any special physical effort.

Factor 9 - Work Environment (FL 9-1/5 Points)

The work area is adequately lighted, heated, and ventilated. The work environment involves everyday risks or discomforts that require normal safety precautions. Some employees may occasionally be exposed to uncomfortable conditions in such places as research facilities.

TOTAL POINTS - 3190

GS-13 POINT RANGE=3155-3600

FINAL DETERMINATION: GS-13