

POSITION DESCRIPTION (Please Read Instructions on the Back)1. Agency Position No.
DOI1013

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	09	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.

Typed Name and Title of Official Taking Action

Renae Lockwood,
Classification Program Manager

Signature

RENAE
LOCKWOODDigitally 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

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.

IT Cybersecurity Specialist

GS-2210-09

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

Provides support and assistance for assignments and projects relative to information systems and/or cybersecurity matters. Assists higher-graded specialists in ensuring the confidentiality, integrity, and availability of systems, networks, and data through the development, implementation, maintenance, and enhancement of information systems security policies, procedures, and tools.

Participates in the implementation of security programs designed to anticipate, assess, and minimize system vulnerabilities such as intrusion detection or access authentication programs. Ensures compliance with legal controls that provide protection from unauthorized access, alteration, loss, disclosure, and blocking of information.

Performs routine and recurring implementation activities; implements measures to ensure awareness and compliance; and identifies or recommends the need for changes based on new security technologies or threats.

Participates in implementation of systems security policies, guidelines and procedures related to web-based applications, network, and systems designs. This includes initial design, system

lifecycle change review, and configuration management. Participates in identifying and writing specifications to meet IT security requirements.

Assists employees and supervisors on security issues; participates in testing and implementation of new security technologies; and institutes measures to ensure awareness and compliance.

Assists staff in carrying out security development, implementation, operations, and maintenance requirements.

Participates in creating and maintaining system security plans, contingency plans, risk assessments, and certification statements; and participates in periodic systems security evaluations, audits, and reviews.

Identifies and resolves problems in response to customer reported issues, and researches, evaluates, and provides feedback on problematic trends and patterns. Assists higher-graded specialists in providing customer training.

Implements security measures to ensure controlled access and maintains data integrity and confidentiality.

Performs other similar duties as assigned.

FACTORS

Factor 1 - Knowledge Required by the Position (FL 1-6/950 Points)

Knowledge of, and skill in applying, IT security and cybersecurity principles, methods, and practices in information security; technical documentation methods and procedures; systems security methods and procedures; and analytical methods sufficient to identify and resolve issues and problems; prepare and update manuals, instructions, and operating procedures; provide information and assistance to customers; and ensure the application of appropriate security measures to the assignment.

Knowledge of, and skill in applying IT security principles and methods associated with applying risk factors; technical documentation methods; and performance management methods sufficient to conduct integrated analysis of audit logs; implement corrective and preventive actions and support cybersecurity applications; and provide input in drafting information systems security documentation (e.g., systems security plans, risk assessments, disaster recovery plans, business continuity plans, and user security guides and policies).

Knowledge of, and skill in applying IT security principles and methods; and IT security regulations and policies sufficient to participate in identifying and writing specifications to meet IT security requirements.

Ability to communicate orally and in writing to provide guidance to customers and to prepare and present reports.

Factor 2 - Supervisory Controls (FL 2-3/275 Points)

The supervisor outlines or discusses possible problem areas and defines objectives, plans, priorities, and deadlines. Assignments have clear precedents requiring successive steps in planning and execution. The employee independently plans and carries out the assignments in conformance with accepted policies and practices; adheres to instructions, policies, and guidelines in exercising judgment to resolve commonly encountered work problems and deviations; and brings controversial information or findings to the supervisor's attention for direction. The supervisor provides assistance on controversial or unusual situations that do not have clear precedents; reviews completed work for conformity with policy, the effectiveness of the employees approach to the problem, technical soundness, and adherence to deadlines; and does not usually review in detail the methods used to complete the assignment.

Factor 3 - Guidelines (FL 3-3/275 Points)

The employee uses a wide variety of reference materials and manuals; however, they are not always directly applicable to issues and problems or have gaps in specificity. Precedents are available outlining the preferred approach to more general problems or issues. The employee uses judgment in researching, choosing, interpreting, modifying, and applying available guidelines for adaptation to specific problems or issues.

Factor 4 — Complexity (FL 4-3/150 Points)

Work consists of various duties that involve applying a series of different and unrelated processes and methods. The employee decides what needs to be done based on analyses of information security issues related to the assignment; and selects appropriate courses of action from many acceptable alternatives. The employee identifies and analyzes important factors and conditions in order to recognize and apply an understanding of interrelationships among different IT security functions and activities.

Factor 5 - Scope and Effect (FL 5-3/150 Points)

Work involves a variety of common information security problems, questions, or situations that are dealt with in accordance with established criteria. Work affects the design, testing, implementation, operation, or support of security systems or the quality and reliability of services.

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

Contacts are with individuals or groups from outside the agency, including consultants, contractors, or vendors, in moderately unstructured settings. Contacts are related to technological information and developments applicable to assigned IT and/or 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. Must recognize or learn the role and authority of each party during the course of the meeting.

Factor 7 - Purpose of Contacts (FL 7-B/50 Points)

The purpose of contacts is to plan, coordinate, or advise on developments and issues in the technology specialty area(s) of the position, and/or to resolve issues or operating problems by influencing or persuading people who are working toward mutual goals and have basically cooperative attitudes. Contacts typically involve identifying options for resolving problems.

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: 1920

POINT RANGE: 1855-2100

FINAL DETERMINATION: GS-09