



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

APR 23 2019

Memorandum

To: Bureau Chief Information Officer
Bureau Chief Human Capital Officers
Human Resources Directors/Officers

From: William E. Vajda
Chief Information Officer
Office of the Chief Information Officer

Raymond A. Limon
Deputy Assistant Secretary - Human Capital and Diversity
Chief Human Capital Officer

Subject: Standardized Position Descriptions for IT Cybersecurity Specialists

The Department of the Interior's Office of the Chief Information Officer (OCIO) and the Office of Human Capital (OHC) identified inconsistencies within position descriptions across the information technology workforce (2210s) within the Department. The OHC, OCIO and the Information Management and Technology Leadership Team (IMTLT) collaborated to establish standardized position descriptions (SPDs) for cybersecurity work.

IT management teams, representing the bureau IT workforce, developed and built a consensus for the major job duties and factor levels for DOI cybersecurity work, consistent with the U.S. Office of Personnel Management's job family standard (2018); the Federal Information Security Modernization Act of 2014 (FISMA); Clinger-Cohen Act (CCA) of 1996; Privacy Act of 1974; Presidential Decision Directive 63; OMB Circular A-130, Appendix III), Federal Information Technology Acquisition Reform Act (FITARA).

The attached Personnel Bulletin disseminates and provides guidance on implementing the newly established standard position descriptions.

Questions concerning these SPDs should be directed to the respective Bureau/equivalent Human Resources Office. Bureau headquarters staff can contact Renae Lockwood at renae_lockwood@ios.doi.gov

Attachments



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

PERSONNEL BULLETIN NO: 19-03

SUBJECT: Standardized Position Descriptions for IT Cybersecurity Specialists

1. Purpose. This personnel bulletin establishes Department of the Interior standard position descriptions (SPDs) for supervisory and non-supervisory IT Cybersecurity Specialists.

2. Background. These positions are required for the protection of information and information systems and for providing a framework to manage and measure IT Cybersecurity Program performance, promote increased awareness throughout the Department, and to reduce potential breaches of sensitive information and the compromise of information systems. These positions will assist the Associate Chief Information Security Officers (ACISO) and Chief Information Security Officer (CISO) in the development and/or implementation of IT cybersecurity policy and ongoing assessment for compliance with Department, Federal, and National Institute of Standards and Technology (NIST) policies, directives, guidelines, and best practices. These positions will also help ensure that information systems maintain confidentiality, integrity and availability, and prevent and defend against unauthorized access to systems, networks, and data. (Federal Information Security Modernization Act of 2014 (FISMA); Clinger-Cohen Act (CCA) of 1996; Privacy Act of 1974; Presidential Decision Directive 63; OMB Circular A-130, Appendix III), Federal Information Technology Acquisition Reform Act (FITARA)).

The Department of the Interior (DOI)'s Office of Human Capital (OHC), Office of the Chief Information Officer (OCIO) and the Information Management and Technology Leadership Team (IMTLT) collaborated to establish these SPDs. These SPDs were vetted with the Bureaus.

3. Policy. Effective immediately, Bureaus will implement the use of these new DOI SPDS for new appointments. Additionally, Bureaus will carefully review existing positions with the assigned parentheticals *infosec and/or security* and manage the integration of these SPDs for current employees, within their assigned career ladder positions, to ensure minimal impact. DOI standard PDs DOI005 and DOI006 are exempt from this PB. Bureaus must replace legacy PDs with the new DOI standardized PDs, where applicable, and process the necessary reassignment actions as soon as possible, but not later than 60 days from the date of this Personnel Bulletin (PB). The official SPDs with SPD numbers covered by this PB are:

DOI007	Supervisory IT Cybersecurity Specialist	GS-2210-15
DOI008	Supervisory IT Cybersecurity Specialist	GS-2210-14
DOI009	IT Cybersecurity Specialist	GS-2210-14
DOI010	IT Cybersecurity Specialist	GS-2210-13
DOI011	IT Cybersecurity Specialist	GS-2210-12

DOII012	IT Cybersecurity Specialist	GS-2210-11
DOII013	IT Cybersecurity Specialist	GS-2210-9

4. Hiring Controls. In accordance with Personnel Bulletin 16-05, the Bureau/Office Associate Chief Information Officers (ACIO) will provide approval of all recruitment actions in collaboration with the OCIO.

5. Official Titles. The U.S. Office of Personnel Management's prescribed official titles are located in Block 15b on the PD cover sheet (OF-8). This title **must be** entered into the Federal Personnel and Payroll System (FPPS) and be reflected on the incumbent's SF-50, *Notification of Personnel Action*. Variations to official titles are not authorized.

Organizational Titles. In addition to the official title, bureaus/offices have the option to assign an organizational title. Organizational titles do not replace, but complement, official position titles.

6. Standard PD Numbering System. Bureaus **must use** the DOI standardized PD numbering system when using these SPDs for newly established positions and when replacing existing SPDs. The use of a bureau-level numbering system in lieu of a DOI SPD number is not authorized. The DOI SPD number **must be** entered into FPPS, in accordance with Bureau procedures, so it prints on the incumbent's SF-50 (Notification of Personnel Action). The SPD number is recorded in Block 1 of the OF-8 attached for each DOI SPD. In order to conform to the position number data field length in FPPS, the SPD numbers assigned are seven digits in length.

7. PD Cover Page. The servicing human resources office (SHRO) will complete the PD cover page with organizational titles, Position Risk/Sensitivity Level, cybersecurity codes, etc.

8. Management's Responsibility for PD Accuracy and Position Management. Use of Standardized PDs in no way detracts from management's authority and responsibility to ensure that officially assigned and performed duties and responsibilities accurately match PDs of record for all covered employees. Likewise, using SPDs also does not diminish management's responsibility to adhere to basic position management principles. Management officials are urged to contact their respective SHRO for classification and position management advice and guidance.

9. Exception to the Rules. Bureaus may make minor edits to these SPDs to reflect bureau/office specific requirements (e.g. terminology). Major edits must be avoided. Bureau Human Resources Offices and Associate Chief Information Officers must fully coordinate major edits to these SPDs with the Department's Chief Information Security Officer and the Office of Human Capital.

Questions concerning SPDs should be directed to the respective Bureau/equivalent Human Resources Office. Bureau headquarters staff can contact Renae Lockwood at renae_lockwood@ios.doi.gov.



Raymond A. Limon
Deputy Assistant Secretary – Human Capital
and Diversity
Chief Human Capital Officer

Attachments