UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

Wednesday, January 4, 2017

MEMORANDUM FOR: HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: BETH F. COBERT, ACTING DIRECTOR

Subject: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions

I am pleased to share guidance that explains how agencies will institute the updated procedures for assigning codes to Federal cybersecurity positions. This guidance supports the U.S. Office of Personnel Management's (OPM) role with implementing the Federal Cybersecurity Workforce Assessment Act. Additionally, coding and identifying our cybersecurity workforce is important foundational work to better managing these critical positions.

Background

In 2013, OPM began efforts under the "Special Cybersecurity Workforce Project" to collect and analyze data on the Federal cybersecurity workforce to identify and address the skills needed by this important group. This effort included identifying and coding Federal positions with cybersecurity functions, thus allowing the Federal Government to pinpoint these crucial functions and positions.

Since 2013, Federal agencies have assigned Government-wide Cybersecurity Data Standard Codes to their positions with cybersecurity functions. The codes align to an early version of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Framework) and recognize nine categories and 31 specialty areas of cybersecurity functions. The NICE Framework brings standardization across the public, private, and academic sectors to define cybersecurity work and the common set of tasks and knowledge, skills, and abilities (KSAs) required to perform cybersecurity work. This standardization is an important part of educating, recruiting, training, developing, and retaining a highly-qualified workforce.

New Cybersecurity Coding Requirement

The Federal Cybersecurity Workforce Assessment Act of 2015 (Act) requires OPM to establish procedures to implement the NICE coding structure and to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

The NICE coding structure, captured in the Federal Cybersecurity Coding Structure, has recently been updated to include "work roles" and associated codes, and broadened to include not only cybersecurity functions, but also information technology and cyber-related functions. OPM has

revised the *Government-wide Cybersecurity Data Standard Codes*, contained in the Guide to Data Standards, to align with the new Federal Cybersecurity Coding Structure. We expect the Federal Cybersecurity Coding Structure to be mirrored in the upcoming revised NICE Framework.

It is important for agencies to participate in the process to standardize the cybersecurity workforce terminology and concepts promoted by NICE across the public, academic, and industry sectors. The coding of Federal positions with information technology, cybersecurity, and cyber-related functions, and aligning to the Federal Cybersecurity Coding Structure and NICE Framework, are beneficial for several reasons, including the following:

- Enhancing Recruitment of Needed Skills. Applying the codes and categorizing Federal cybersecurity positions to align with the NICE Framework make our work requirements and skill needs match the skills being developed through academic curricula and industry work experiences, as these also correspond with the NICE Framework.
- Hiring Needed Skills. The coding allows us to consistently describe the tasks, functions, and work roles of Federal cybersecurity positions, and leverage the affiliated KSAs in job opportunity announcements, applicant assessments, and staff development.
- Identifying Critical Needs. Using the codes provides a common framework for identifying critical needs and provides a standardized method to compare current workforce skills and work roles to those needed in the future.
- Training and Development. When we code and categorize Federal cybersecurity positions in relation to the NICE Framework, we can take advantage of the library of cybersecurity training courses aligned to the codes and work roles.

In accordance with the Act, within three months from the date of this memorandum all Federal agencies must establish procedures for identifying and coding their encumbered and vacant civilian positions with information technology, cybersecurity, and cyber-related functions. The Act cites a deadline of one year after the agency procedures are established for the agencies to complete this coding. Agencies should use this guidance as a resource in establishing their coding procedures.

Instructions for Assigning Revised Codes

OPM collaborated with stakeholder groups to develop the following instructions for agencies to assign the revised Cybersecurity Data Standard Codes.

- Agencies must use the Federal Cybersecurity Coding Structure to find the Cybersecurity Data Standard Codes to assign to encumbered and vacant positions. The codes represent the various work roles found in information technology, cybersecurity, and cyber-related functions.
    - The Cybersecurity Data Standard Codes in the Federal Cybersecurity Coding Structure are also described in *OPM's Guide to Data Standards*.
- Chief Information Officer (CIO) staff, managers, and human resources (HR) and classification staff must partner to identify encumbered and vacant positions with information technology, cybersecurity, and cyber-related functions and assign the revised Cybersecurity Data Standard Codes. CIO staff will have perspectives on where

cybersecurity work is being accomplished across the agency, how to interpret the work roles described in the Cybersecurity Data Standard Codes, and what expectations the agency has regarding information technology, cybersecurity, and cyber-related functions, skills, requirements, etc. Managers will play a key role in knowing what positions are performing functions that will be coded. HR and classification staff will develop and implement, with assistance from the partners described above, the overall process for identifying positions and assigning the Cybersecurity Data Standard Codes, in accordance with these instructions.

- Agencies must review all encumbered positions and authorized and funded vacant positions performing information technology, cybersecurity, and cyber-related functions and annotate the reviewed position descriptions (PDs) with the appropriate revised Cybersecurity Data Standard Code(s). The new Cybersecurity Data Standard Codes are three digits, in comparison to the 2-digit original codes. Positions that perform information technology, cybersecurity, and cyber-related functions will extend beyond the GS-2210 Information Technology occupational series.
- Agencies must send the coded PD information for encumbered positions to the Enterprise Human Resources Integration (EHRI) data warehouse, so that OPM receives the data. In the next two years, agencies will be required to report their vacant positions (by Cybersecurity Data Standard Codes) once OPM begins tracking cybersecurity vacancies across the Government. Such tracking will provide insight into the Federal Government's cybersecurity recruitment and skill needs, and progress in closing cybersecurity skill gaps.
- Agencies must assign Cybersecurity Data Standard Code "000" to positions that do not perform information technology, cybersecurity, and cyber-related functions, and Cybersecurity Data Standard Codes within the range of "100" to "999" to positions with substantial information technology, cybersecurity, and cyber-related functions. The coded cybersecurity functions (i.e., covering information technology, cybersecurity, and cyber-related functions) are described in the Federal Cybersecurity Coding Structure and the codes are defined in *OPM's Guide to Data Standards*.
- In some cases, a position may perform substantial work in more than one information technology, cybersecurity, and cyber-related function. Agency classification staff should assist managers, as needed, with determining when multiple, substantial functions exist in a position. Agencies may code up to three substantial functions per position; therefore, they should assign the Cybersecurity Data Standard Codes in the order in which the most critical function of the job is listed first, the next critical function of the job is listed next, and so on.
- Agencies must conduct a thorough review to identify and properly code all positions with information technology, cybersecurity, and cyber-related functions. The resulting coding data is intended to help agencies, and the Federal Government, identify and address the recruitment, training, development, and skills needed for this critical workforce; therefore, ensuring that accurate codes are assigned to positions is paramount as the data will be used to inform decisions made that will affect the workforce.

- During the process of identification and coding, agencies may need to update PDs to ensure information technology, cybersecurity, and cyber-related functions are accurately described. The PushButtonPD™, a no-cost resource, along with OPM classification guidance, can help managers and classification staff develop or update PDs for positions with information technology, cybersecurity, and cyber-related functions. In the near future, agencies will be able to use OPM's forthcoming Interpretive Guidance for Cybersecurity Positions as cybersecurity coding and classification decisions are made. Agency questions regarding classification may be sent to Fedclass@opm.gov.

Resources

Please refer to the Federal Cybersecurity Workforce Assessment Act MAX page for periodic updates and helpful resources for applying the revised Cybersecurity Data Standard Codes and carrying out other requirements of the Act. You may address questions to Jodi Guss (Jodi.Guss@opm.gov).

cc: Chief Human Capital Officers, Human Resource Directors, Chief Information Officers, and HR Line of Business