


APR 04 2017

  
Approved for Release

4/4/17  
Date

Kevin E. Mahoney  
Director for Human Resources Management and  
Chief Human Capital Officer

**DEPARTMENT OF COMMERCE  
OFFICE OF HUMAN RESOURCES MANAGEMENT  
HUMAN RESOURCES (HR) BULLETIN #215, FY17**

**SUBJECT:** Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions at the Department of Commerce

**EFFECTIVE DATE:** Upon release of this HR Bulletin

**EXPIRATION DATE:** Effective until superseded or revoked

**SUPERCEDES:** HR Bulletin #201, FY15, "Additional Implementation of the 2013 Federal Cybersecurity Initiative at the Department of Commerce," dated March 13, 2015.

**REVISIONS:** The National Initiative for Cybersecurity Education (NICE) coding structure has been updated to include "work roles" and associated codes, and has been broadened to include not only cybersecurity functions, but also information technology (IT) and cyber-related functions. The updated codes now have three digits, in comparison with the original two-digit codes, and up to three codes may be assigned per position.

**PURPOSE:** This bulletin provides the implementation plan for the Department of Commerce (Department) in order to adhere to the procedures established by Office of Personnel Management (OPM), which uphold the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015 (Act). The Department must ensure it is up-to-date in utilizing the new cybersecurity coding structure to include IT and cyber-related functions, and must use the new three-digit codes for all positions by April 4, 2018.

**BACKGROUND:** Beginning in 2013, under the Special Cybersecurity Workforce Project, Federal agencies have been tasked to identify and code positions that perform cybersecurity work within the IT Management Series (2210 series). Agencies were later tasked with identifying and coding all positions with appropriate cybersecurity codes. The initial coding aligned with an early version of the NICE Cybersecurity Workforce Framework, and recognized 9 categories and 31 specialty areas of cybersecurity functions. The intention was to provide standardization across the public, private, and academic sectors to define cybersecurity work, as well as the common set of tasks and the knowledge, skills, and abilities (KSAs) required to perform cybersecurity work. The Department met the objectives of the initial Special Cybersecurity Workforce Project.

The Act requires OPM to establish procedures to implement the latest NICE coding structure to identify all Federal civilian positions that require the performance of IT, cybersecurity, or other cyber-related functions. OPM has revised the Government-wide Cybersecurity Data Standard Codes to align with the new coding structure.

**COVERAGE:** Applies to all Servicing Human Resources Offices (SHROs) in the Department.

**POLICY:** In order to complete the requirements of the Act, as defined in OPM's "Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions," the Department must review all encumbered, authorized, and funded vacant positions that are performing IT, cybersecurity, and cyber-related functions, and must annotate the reviewed position descriptions (PDs) with the appropriate revised Cybersecurity Data Standard Code(s).

The SHROs, in conjunction with their Chief Information Officer (CIO) community counterparts, are required to work with managers/supervisors in their serviced areas to identify IT, cybersecurity, and/or other cyber-related functions being performed within all occupational series. Each SHRO and CIO must have a designated point of contact to co-manage the initiative.

The Federal Cybersecurity Coding Structure must be used to find the Cybersecurity Data Standard Codes to assign to encumbered and vacant positions. The codes represent the various work roles found in IT, 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."

Department policy establishes that IT, cybersecurity, or cyber-related duties must be performed 25 percent of the time or more in order for a cybersecurity code to be assigned. Coding for these positions will be according to their "category," "specialty area," and "work role." Federal IT, cybersecurity, and cyber-related positions may include more than one, and up to three, substantial functions per position. If more than one code is selected, they should be assigned in the order in which the most critical function of the job is listed first, and so on.

### **Categories, Specialty Areas, and Work Roles**

The Federal Cybersecurity Coding Structure comprises 7 categories, which include 33 specialty areas and 52 work roles. Categories provide the overarching organizational structure of the NICE Framework, and contain groupings of cybersecurity work, which are called specialty areas. Work roles are the most detailed groupings of IT, cybersecurity, or cyber-related work. These roles include lists of KSAs that a person must have to perform a set of functions or tasks.

More information on the Federal Cybersecurity Coding Structure can be found at: [http://csrc.nist.gov/nice/framework/opm\\_codes/OPM.pdf](http://csrc.nist.gov/nice/framework/opm_codes/OPM.pdf).

The most up-to-date Guide to Data Standards in the Cybersecurity Category/Specialty Area can be found at: <https://ehr.nbc.gov/datastandards/referenceData/2273/current?category=&q=Cyber>.

## **Coding**

The result of coding positions performing IT, cybersecurity, or cyber-related duties is intended to help 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 impact the workforce.

Positions performing IT, cybersecurity, or cyber-related duties 25 percent of the time or more must be identified by category, specialty area, and work role(s), and coded using the Cybersecurity Data Standard Codes. A cybersecurity identifier field resides within the Position Management section in HR Connect. As these changes are made, they will update in our service provider's system, the National Finance Center (NFC), and will be sent to OPM's Enterprise Human Resources Integration (EHRI) system.

**Note:** Positions that perform IT, cybersecurity, or cyber-related duties will extend beyond the IT Management Series (2210 series). The Department must assign Cybersecurity Standard Data Code "000" to positions not performing IT, cybersecurity, or cyber-related duties.

In addition, for new positions, the Classification and Performance Management Record (form CD-516) will be updated to include a cybersecurity field that requires the corresponding three-digit code, an update to the current two-digit field, to be recorded under Section C, Individual Position.

## **Process**

**SHROs:** The SHROs and CIO counterparts should work with managers/supervisors to identify cybersecurity positions using the Cybersecurity Data Standard Codes. The SHROs and CIO counterparts need to determine timelines with managers, within the broad Department timeframes, to identify these positions and meet the OPM requirements.

### **SHRO Responsibilities:**

- Work with CIO counterparts.
- Communicate with all supervisors/managers and explain the Cybersecurity Data Standard Codes.
- The SHROs give worksheet (provided) to managers to validate the category, specialty area, and work role(s).
- The manager submits the worksheet to his/her SHRO.
- The SHRO codes the category, specialty area, and work role(s) in the Position Management section of HR Connect.
- Ensure that the updated CD-516 is being used when applicable.

### **Managers/Supervisors:**

- Review the PDs for accuracy, and update IT, cybersecurity, and cyber-related duties as applicable.
- Determine the IT, cybersecurity, and cyber-related duties being performed 25 percent of the time or more.
- Assign a category, special area, and work role code(s) to cybersecurity duties being performed at least 25 percent of the time.

- Provide the cybersecurity worksheet to the SHRO.
- Use the most up-to-date CD-516 when applicable.

### **Government-wide Time Line**

- December 9, 2017 – All service providers, such as the NFC, must start using the three-digit coding system.
- April 4, 2018 – All positions must be reviewed and coded appropriately.

### **Department Timeline**

- May 19, 2017 – SHROs and CIO counterparts review bulletin and discuss responsibilities.
- July 14, 2017 – SHROs meet with all managers/supervisors to discuss new requirements.
- December 9, 2017 – Managers/supervisors provide the SHROs with the completed Worksheet for Managers.
- December 11, 2017 – Coding may begin using HR Connect and the NFC.
- February 2, 2018 – 50 percent of all positions must be reviewed and coded appropriately.
- March 28, 2018 – 100 percent of all positions must be reviewed and coded appropriately.
- Ongoing – All new positions, and any position changes, must continue to be reviewed and coded appropriately.

### **Reporting Requirements**

The SHROs must provide an updated Cybersecurity Progress Template to report the percentage of positions coded by the designated date above to the Program Manager.

**REFERENCES:** OPM’s “Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions,”

<https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity>. “Federal Cybersecurity Coding Structure,”

[http://csrc.nist.gov/nice/framework/opm\\_codes/OPM.pdf](http://csrc.nist.gov/nice/framework/opm_codes/OPM.pdf). Data Standards: Cybersecurity Category/Specialty Area,

<https://ehr.nbc.gov/datastandards/referenceData/2273/current?category=&q=Cyber>.

**OFFICE OF POLICY AND PROGRAMS:** Valerie Smith, Director, [VSmith@doc.gov](mailto:VSmith@doc.gov), (202) 482-0272

**PROGRAM MANAGER:** Mary O’Connor, [MOConnor@doc.gov](mailto:MOConnor@doc.gov), (202) 482-2080

### SHRO and CIO Points of Contact

<b>Bureau</b>	<b>SHRO Contact</b>	<b>CIO Contact</b>
BEA	Catherine Hayes	Randy (Frederick) Carlson, Lisa Smith
BIS	Jamica McCoy	Ida Mix, Rob Richardson
Census	Catherine Hayes	Tim Ruland, Jeff Jackson
EDA	Jamica McCoy	Sandranette Moses
ESA	Catherine Hayes	June Kim
ITA	Jamica McCoy	Joe Ramsey, Marques Young
MBDA	Jamica McCoy	June Kim
NIST	Sandy Nail	Robert Glenn, Carolyn Schmidt
NOAA	Angela Taylor	Robert Brunner
NTIS	Sandy Nail	Shine Kang, Heather Lynch
NTIA	Jamica McCoy	Alan Willard, Mike Miller
USPTO	Sandy Robinson	John Pardun
OIG	Tonia Patterson	Toan Pham
OS	Jamica McCoy	June Kim
FirstNet	Benita Park	June Kim