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

3/13/15
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #201, FY15

SUBJECT: Additional Implementation of the 2013 Federal Cybersecurity Initiative at the Department of Commerce

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until superseded or revoked

SUPERCEDES: HR Bulletin #185, FY14, "Implementation of the 2013 Federal Cybersecurity Initiative at the Department of Commerce," dated December 18, 2013

REVISIONS: This bulletin implements the newest requirement from the Office of Personnel Management (OPM) on the 2013 Federal Cybersecurity Initiative. Initially, the Department of Commerce (Department) was tasked to identify and code positions that perform cybersecurity work within the IT Management Series (2210 series). The Department has now been tasked with identifying and coding all Department positions by the end of Calendar Year (CY) 2015. Also, form CD-516, Classification and Performance Management Record, has been updated to include a cybersecurity field.

PURPOSE: The bulletin provides background, guidance, and key additional information on implementing the revised objectives of the Federal cybersecurity initiative within the Department for all positions.

BACKGROUND: On July 8, 2013, OPM released guidance (on the presidential initiative) for all Federal agencies on identifying and coding cybersecurity positions, which will help in reducing skills gaps, aid in recruiting cybersecurity IT (information technology) professionals, and augment training and future development in the Department.

There is little consistency throughout the Federal Government and the Nation on how cybersecurity work is defined or described. Significant variations exist in occupations, job titles, position descriptions, and in job series listed by OPM. The absence of common language to describe cybersecurity work (and its requirements) hinders the Government's ability to establish a baseline of capabilities, identify skills gaps, ensure an adequate pipeline of future talent, and continually develop a highly qualified cybersecurity workforce. Establishing and using a common lexicon, taxonomy, and other data standards for cybersecurity requirements are vital.

The National Cybersecurity Workforce Framework has established a common taxonomy and lexicon to describe cybersecurity work and workers, irrespective of where or for whom the work is performed. The Framework is intended to be applied in the public, private, and academic sectors. The National Initiative for Cybersecurity Education (NICE) Framework has developed a structure of 31 specialty areas organized into 7 categories, with related specialty areas together. (The specialty areas within a category are more similar to one another than to specialty areas in other categories. Within each specialty area typical tasks, knowledge, skills, and abilities are grouped.)

In FY 2014, the Department was tasked to identify cybersecurity work performed within the 2210 series; in order to further implement the presidential initiative, OPM has tasked the Department to identify cybersecurity work being performed within all occupational series by the end of CY 2015.

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

POLICY: SHROs are required to work with managers/supervisors in their serviced areas to identify cybersecurity work being performed within all occupational series, not only in the IT Management Series (2210 series).

Each SHRO must have a designated point of contact (POC) to manage the initiative. The NICE Framework will be used to identify positions by the established categories and specialty areas as well as by the knowledge, skills and abilities (KSAs), competencies, and tasks.

Department policy seeks to identify cybersecurity duties that are being performed 25 percent of the time or more. These duties are to be identified as "cybersecurity," and should be coded according to their Category/Specialty Area.

- For positions that have multiple cybersecurity duties, the Category/Specialty Area of the duty encompassing the greatest percentage of time should be used for coding purposes.
- For positions where cybersecurity duties are split equally, the manager should identify which Category/Specialty Area is paramount, or more important to the position.
- If there are multiple relevant Specialty Areas in a Category and no single Specialty Area dominates, use the code for the Category in which those Specialty Areas fall.

Categories and Specialty Areas

The NICE Framework comprises 7 categories, which include 31 specialty areas. It adopts an organizing structure based on extensive job analyses, which groups together work and workers that share common major functions, regardless of job titles or other occupational terms. Specialty areas in the same category are generally more similar to one another than to those in other categories. Categories and corresponding specialty areas are listed below.

Categories/Specialty Areas:

Analyze – Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- Threat Analysis
- Exploitation Analysis
- Targets
- All Sources Intelligence

Collect and Operate – Specialty areas responsible for denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Investigate – Specialty areas responsible for investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

- Investigation
- Digital Forensics

Operate and Maintain – Specialty areas responsible for providing support, administration, and maintenance necessary for effective and efficient IT system performance and security.

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management

Oversight and Development – Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development
- Information Systems Security Operations (ISSO)
- Security Program Management [Chief Information Security Officer (CISO)]

Protect and Defend – Specialty areas responsible for identification, analysis, and mitigation of threats to internal IT systems or networks.

- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Analysis
- Computer Network Defense (CND) Infrastructure Support

Securely Provision – Specialty areas responsible for conceptualizing, designing, and building secure IT systems (i.e., responsible for some aspects of systems development).

- Systems Requirements Planning
- Systems Development
- Software Assurance and Security Engineering
- Systems Security Architecture
- Test and Evaluation
- Technology Research and Development
- Information Assurance (IA) Compliance

More information on the seven categories, as well as sample job titles by corresponding specialty area and corresponding KSAs, can be found at: http://niccs.us-cert.gov/training/tc/framework/categories.

Additional material on specialty areas can be found at: http://niccs.us-cert.gov/training/tc/framework/specialty-areas.

Coding

Positions performing cybersecurity duties 25 percent of the time or more will be identified by category/specialty area and will be coded using OPM's "Guide to Data Standards," page A-107, see attached. There is a cybersecurity identifier field that resides in the Individual Position (IP) record in the Position Management System (PMSO). The cybersecurity *value* is recorded in the Status Report of OPM's Enterprise Human Resources Integration (EHRI) system and is a snapshot of the IP at the time OPM generates a report from EHRI. **Only one code (2 digits) is permitted so it is important that the most appropriate code is used.**

Positions not performing cybersecurity duties will be coded as "00." In order to code these positions more efficiently, SHROs may submit a list of positions (using the enclosed worksheet for non-cybersecurity positions) to the Department's Cybersecurity Program Manager with the following information 15 days prior to the end of the quarter: the master position number, the individual position number, agency, Personnel Office Indicator (POI), and grade. A Front-End System Interface (FESI) file will be created and submitted to the National Finance Center (NFC) for processing.

Additionally, for new positions, form CD-516, Classification and Performance Management Record, has been updated to include a cybersecurity field that requires the corresponding 2-digit code be recorded under Section C, Individual Positon.

OPM's "Guide to Data Standards" can also be found at: http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf.

Process

SHROs: SHROs should work with managers/supervisors to identify cybersecurity positions using the NICE Framework. SHROs need to determine timelines with managers, within the broad Department timeframes, to identify these positions and meet the OPM requirements. Before each quarterly deadline, SHROs are to return a completed Cybersecurity Progress Template to the Department in order to report to OPM in a timely manner.

SHRO Responsibilities:

- Communicate with all supervisors/managers and explain the NICE Framework and the initiative.
- SHROs provide attached worksheet to the managers to validate the Category and Specialty Area by signing the worksheet.
- Manager submits the worksheet to his/her SHRO.

- SHRO codes the Category and Specialty Area in PMSO.

Managers/Supervisors: Steps of Review Process

- Review position description for accuracy, and update cybersecurity duties as applicable.
- Determine the cybersecurity duties being performed 25 percent of the time or more.
- Review the cybersecurity category definitions and corresponding sample job titles, and KSAs, using the NICE Framework.
- Assign a category to cybersecurity duties being performed at least 25 percent of the time.
- Review the specialty area definition within the assigned category(ies) using the NICE Framework.
- Assign a specialty area to each assigned category.
- Determine the final cybersecurity code for the position based on the duty that is being performed the greatest percentage of time, the duty that is most important, or the Category itself if multiple Specialty Area duties are being performed.
- Provide the cybersecurity worksheet to the SHRO.

Government-wide Time Line

- December 31, 2015 – All current and new positions must be reviewed and coded appropriately.

Department Timeline

- March 31, 2015 – SHROs meet with all managers/supervisors as needed.
- June 30, 2015 – 50 percent of all positions must be reviewed and coded appropriately.
- September 30, 2015 – 75 percent of all positions must be reviewed and coded appropriately.
- December 31, 2015 – 100 percent of all positions must be reviewed and coded appropriately.

Reporting Requirements

SHROs must provide a written report (see attached) to the Department's Cybersecurity Program Manager beginning with the June 30, 2015 date, within 5 working days from each designated date above.

REFERENCES: NICE Framework: http://csrc.nist.gov/nice/framework/, http://niccs.us-cert.gov/training/tc/framework, http://niccs.us-cert.gov/training/tc/framework/categories, http://niccs.us-cert.gov/training/tc/framework/specialty-areas. OPM's "Guide to Data Standards": http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf.

Office of Policy and Benefits: OPBservices@doc.gov

Worksheet for Non-Cybersecurity Positions

Master Position Number	Individual Position Number	Agency	POI	Grade

SHROs Report to Department

SHRO	Positions	Number of Positions Coded by 6/30	Percentage of Positions Coded by 6/30	Number of Positions Coded by 9/30	Percentage of Positions Coded by 9/30	Number of Positions Coded by 12/31	Percentage of Positions Coded by 12/31
Census	14220	0	0%	0	0%	0	0%
DOCHROC	2648	0	0%	0	0%	0	0%
NIST	3271	0	0%	0	0%	0	0%
NOAA	11528	0	0%	0	0%	0	0%
OIG	154	0	0%	0	0%	0	0%
USPTO	12670	0	0%	0	0%	0	0%
Total	44491	0	0%	0	0%	0	0%

*Data as of 3/9/15