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

12/18/13
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #185, FY14

SUBJECT: 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EXPIRATION DATE: Effective until superseded or revoked

SUPERSEDES: None

PURPOSE: This bulletin provides background and guidance on the process of implementing the Federal cybersecurity initiative within the Department of Commerce (Department).

BACKGROUND: On July 8, 2013, the Office of Personnel Management (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 in 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 used 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. In addition, the National Initiative for Cybersecurity Education (NICE) Framework has developed a structure that consists 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.)

COVERAGE: This HR Bulletin applies to all Servicing Human Resources Offices (SHROs) within the Department.

POLICY: SHROs are required to work with managers/supervisors in their serviced areas to identify cybersecurity work being performed within the IT Management Series (2210 series), as well as in other occupational series that could perform cybersecurity duties. 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 within a Category and no single Specialty Area predominates, the code for the Category in which those Specialty Areas fall should be used.

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 to ensure 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 identified by category/specialty area will be coded using OPM's "Guide to Data Standards," page A-107, see attached. There is a new 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.**

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 supervisors/managers of all 2210 positions 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.
- 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

- March 31, 2014: 60 percent of all 2210 positions must be reviewed and coded appropriately*
- September 30, 2014: 90 percent of all 2210 positions must be reviewed and coded appropriately*

*These codes are to be applied to other positions in occupation series where cybersecurity work is assigned.

Department Timeline

- December 31, 2013: SHROs meet with all managers/supervisors
- January 31, 2014: 10 percent of all 2210 positions must be reviewed and coded appropriately
- March 31, 2014: 60 percent of all 2210 positions must be reviewed and coded appropriately
- June 30, 2014: 75 percent of all 2210 positions must be reviewed and coded appropriately
- September 30, 2014: 90 percent of all 2210 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 January 31, 2014 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 PROGRAMS: Valerie Smith, Director, VSmith@doc.gov, (202) 482-0272

PROGRAM MANAGER: Mary O'Connor, MOConnor@doc.gov, (202) 482-2080