U.S. Nuclear Regulatory Commission

Procedures for Identifying and Coding Civilian Positions with Information Technology (IT), Cybersecurity, and Cyber-Related Functions

Background:

As the threats to cybersecurity and the protections to be implemented grow and evolve, a cybersecurity workforce must be prepared to adapt, develop, implement, maintain, measure, and understand all aspects of cybersecurity. A skilled cybersecurity workforce is needed to meet unique critical infrastructure, enterprise, and operational technology systems and networks.

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology, is coordinating with several different entities, including the Federal government, to ensure that our cybersecurity workforce is prepared to protect our nation from existing and emerging cybersecurity challenges. The initiative's intention is that all IT, cybersecurity and cyber-related work is identifiable within the NICE Cybersecurity Workforce Framework and that work being performed by these positions is indicated by selecting one or more work roles relevant to that position and the mission or business processes being supported by that position from the NICE Cybersecurity Workforce Framework. The initiative is not limited to positions in the 2210 occupational series. This effort includes any position that has IT, cyber security, and cyber-related functions in series 0099-2299.

Beginning in 2013, Federal agencies were delegated the task of assigning Government-wide Cybersecurity Data Standard Codes to positions with IT and cybersecurity functions. These codes align to an early version of the NICE Cybersecurity Workforce 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 required to perform this work. This standardization is an important part of educating, recruiting, developing, and retaining a highly-qualified workforce.

In order to comply with this initiative, agencies must conduct a thorough review of all related positions and code them accordingly. Procedural guidance has been provided below to assist in the identification and coding of these positions agency-wide as required. Please contact the servicing Human Resources (HR) Specialist for the Office of the Chief Information Officer (OCIO) for more information and/or assistance.

Identifying IT, Cyber, and Cyber-Related Positions:

1. Human Capital Analysis Branch (HCAB) will, upon request, prepare a report of all IT, cyber-security and cyber-related positions and submit to the servicing HR Specialist for OCIO.
2. Each office will assign a designated office contact for this effort. The servicing HR specialist for OCIO will review the report from HCAB and discuss the positions with the designated program office contacts to verify report information.
3. If positions need to be added, replaced, or updated, the designated office contact and HR Specialist will work together to update the report.
4. Positions that are not in the 2210 occupational series that include duties related to any of the 31 specialty areas will be added to this report and coded accordingly.

5. The HR specialist will maintain an updated designated program office contact list and ensure that the HCAB report remains up to date.
6. The designated program office contacts will work with the HR Specialist to maintain this report annually and as requested by the HR Specialist.

Coding IT, Cyber, and Cyber-Related Positions:

New and Vacant Positions:

1. All positions that include IT, cyber-security, and cyber-related functions must be officially classified and coded. This includes positions that are not in the 2210 occupational series that encompass duties related to any of the 31 specialty areas.
2. All Position Descriptions (PD) must be officially classified before any vacant position is filled.
3. The supervisor of the position is required to prepare the PD and submit it to the Office of the Chief Human Capital Officer (OCHCO) at the time the request to fill the position is submitted. If the position is not classified or does not include a completed 772A, it must be submitted for classification.
4. The supervisor must provide a Microsoft Word version of the PD to the HR Specialist.
5. The HR Specialist will code the position description with the correct NICE Codes and submit it to the current supervisor for review.
6. The current supervisor will review the codes assigned by the HR Specialist to ensure that the codes are correct. If the codes need to be modified the supervisor will inform the HR Specialist so that the PD can be revised with the correct codes.
7. The HR Specialist will work with the current supervisor and classifier to ensure that the PD is officially classified.
8. The HR specialist will ensure that the 9-digit NICE code is added to the classified PD in the comments field of the 772A and add the code to the designated FPPS field.
9. Once the PD is classified, the supervisor will receive a copy of the PD and sign the PD cover sheet (772A) verifying that the PD is up to date and that the NICE coding is accurate.
10. The HR Specialist will add the PD to the OCHCO PD library.
11. The HR Specialist will submit the classified and coded PD to the Enterprise Human Resources Integration data warehouse so that the Office of Personnel Management receives the data.

Encumbered Positions:

1. Office managers must identify the skills and duties/responsibilities of each position and document this information in the PD.
2. All positions must be classified and coded.
3. All positions must be reviewed at least once every 5 years.
4. Significant updates require classification review.
5. The hiring manager and the HR Specialist will work together to ensure proper coding and classification.

Cybersecurity Coding Guidance

Each cybersecurity position can have up to three codes. Cyber Security codes should be transmitted as a 9 digit number. The codes can be thought of as three, 3-digit codes combined into one 9-digit number. The code for no value is 000. Codes should be

assigned in descending order according to the order of the level of criticality of the work roles for the respective position. For example, a position whose primary function is Risk Management and a secondary function of Data administration would list the code for Risk Management first and the code for Data Administration second (611421000). Risk Management code is listed first because that is the code for the primary (most critical) function of the position.

As an example, consider three hypothetical codes.
code 123 - cyber security test code 1
code 456 - cyber security test code 2
code 789 - cyber security test code 3

The new cyber security data field can be presented in the following ways.

No relevant cyber security codes would be presented as:
cyber security code = 000000000.

One relevant cyber security code would be presented as:
If the specialty area is Risk Management (code for Risk Management is 611) the cyber security code would be 611000000.

Two relevant cyber security codes would be presented as:
If the specialty area is Risk Management (code for Risk Management is 611) and Software Development (code for Software Development is 621) the cyber security code would be 611621000.

Three relevant cyber security codes would be presented as*:*
If the specialty area is Risk Management (code for Risk Management is 611), Software Development (code for Software Development is 621), and Data Administration (code for Data Administration is 421) the cyber security code would be 621611421.

0's should never precede a valid code; empty codes (000) should always follow valid codes. For example, cyber security code 000000123 would be incorrect, while 123000000 is the correct way to display the code.

HELPFUL RESOURCES:

The following links are provided to assist supervisors and OCHCO with ensuring that PDs and positions are coded accurately.

Link I: Federal Cybersecurity Coding Structure:
https://www.nist.gov/sites/default/files/documents/2017/05/15/opm_cybersecuritycodingstructure.pdf

Link II: Government-wide Cybersecurity Data Standard Codes
https://dw.opm.gov/datastandards/referenceData/2273/current?index=C

Link III: Resource for PD updates and classification
https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool