



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, DC 20240

**APR 05 2017**

## Memorandum

To: Bureau Human Resources Offices

From: Raymond A. Limon *RL*  
Director, Office of Human Resources

Subject: Revised National Initiative for Cybersecurity Education (NICE) coding structure.

In collaboration with the Department of Homeland Security, the U.S. Office of Personnel Management (OPM) updated the Government-wide Cybersecurity Data Standard Codes, contained within the Guide to Data Standards to include “work roles” to broaden the scope of cyber functions, and to align with the new Federal cybersecurity coding structure. The revised codes have been expanded to three digits and extend beyond the Information Technology occupational series (See attachment 1).

In accordance with the Federal Cybersecurity Workforce Assessment Act, 2015, Consolidated Appropriations Act of 2016, and the Department of the Interior (DOI) Personnel Bulletin, 17-06, DOI will comply and assign the revised cybersecurity codes to positions descriptions (PD) which indicate the performance information technology, cybersecurity and cybersecurity related functions as well as those that do not perform the aforementioned functions. The mandatory coding data is intended to assist with identifying the recruitment, retention, training, development and skills gaps closures needed for this critical workforce.

This implementation is applicable to the following positions:

- All *encumbered* positions and their position descriptions and authorized and funded *vacant* positions and their position descriptions.
- All *standardized* position descriptions.
- All positions and their position descriptions which perform information technology, cybersecurity, and cyber-related functions, and are not in the GS-2210 Information Technology occupational series; and
- All positions and their position descriptions that do *not* perform information technology, cybersecurity or cyber-related functions.

### **Implementation of NICE coding structure**

Bureau/Office Human Resources (HR) offices will identify encumbered and vacant positions and collaborate with managers and the Office of the Chief Information Officer (OCIO) representatives, such as bureau Associate Chief Information Officers (ACIO) and Associate Chief Information Security Officers (ACISOs), to ensure all position descriptions are reviewed

and revised with appropriate Cybersecurity Data Standard Code. The codes represent the various work roles found in information technology, cybersecurity, and cyber-related functions.

- Cybersecurity Data Standard Codes within the range of “100” to “999” must be assigned to positions with substantial information technology, cybersecurity, and cyber-related functions.
- Cybersecurity Data Standard Code “000” must be assigned to positions that do *not* perform information technology, cybersecurity, and cyber-related functions.
- In some cases, a position can be assigned multiple codes with most critical function listed first.
- When multiple, substantial functions exist in a position, managers are allowed to code up to three functions per position. Managers should work with bureau HR offices to assign the Cybersecurity Data Standard Codes, beginning in descending order, with the most critical job function listed first.
- A Cyber Data Code Determination checklist has been provided for immediate use to ensure the proper code(s) have been assigned to each position description (See attachment 2).
- This checklist will be an attachment to all encumbered and vacant positions and their PDs/OF-8s.
- When advertising for new positions, bureau HR offices will utilize the checklist as part of the recruitment/hiring process.
- Bureau HR offices must ensure coded PD information has been entered into the Enterprise Human Resources Integration data warehouse, ensuring OPM receives the data by **April 4, 2018**. System updates to the Federal Personnel and Payroll System (FPPS), which will allow data input of the new 3-digit codes, are expected to be completed in August 2017.

### **Additional resources**

The Cybersecurity Data Standard Codes in the Federal Cybersecurity Coding Structure are also described in OPM’s Guide to Data Standards, available at: [www.opm.gov](http://www.opm.gov).



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, DC 20240

**APR 05 2017**

## **PERSONNEL BULLETIN NO: 17-06**

**SUBJECT:** Revised Cybersecurity Data Standard Codes Structure

### **1. Purpose.**

This personnel bulletin establishes the Department of the Interior (DOI) policy on the implementation of the revised Cybersecurity Coding requirement, in accordance with the Federal Cybersecurity Workforce Assessment Act of 2015, which requires the Federal Government to implement the National Initiative for Cybersecurity Education (NICE) coding structure or Cybersecurity coding structure. The U.S. Office of Personnel Management (OPM) will be tracking information technology, cybersecurity and cybersecurity-related vacancies across the Federal Government. DOI will be required to report its vacant positions by Cybersecurity Data Standard Codes. This will enable DOI to provide OPM insight into our skills needs and progress in closing skills gaps.

### **2. Background.**

In July 2013, OPM initiated the “Special Cybersecurity Workforce Project” to acquire and analyze data on the Federal cybersecurity workforce to identify and address the skills gaps within Federal agencies. As a result, Federal agencies had been tasked to assign Government-wide Cybersecurity Data Standard Codes to their positions with and without cybersecurity functions.

### **3. Authority.**

The Federal Cybersecurity Workforce Assessment Act of 2015 (Act), contained in the Consolidated Appropriations Act of 2016 (Public Law 114-113), enacted December 18, 2015.

### **4. Scope.**

This personnel bulletin applies to all positions which may or may not perform Information Technology, Cybersecurity or Cybersecurity-related functions within their organizations, to include:

- All *encumbered* positions and their positions descriptions and authorized and funded *vacant* positions and their positions descriptions.
- All Standardized Position Descriptions.
- All positions and their position descriptions which perform information technology, cybersecurity, and cyber-related functions, and are not in the GS-2210 Information Technology occupational series; and
- All positions that do *not* perform information technology, cybersecurity, and cyber-related functions.

## **5. Responsibilities.**

### **A. The Department**

In accordance with the Act, the Department shall do the following:

- Provide guidance to the bureau human resources offices and the Office of the Chief Information Officer (OCIO) on the implementation of the Cybersecurity coding structure.
- Submit a progress report on the implementation of the Cybersecurity coding structure to the appropriate Congressional committees until coding implementation is complete.

### **B. Human Resources**

Human Resources offices will ensure the NICE Cybersecurity codes are entered into the HR data systems i.e., *Federal Personnel Payroll Systems and Oracle Business Intelligence Enterprise Edition* and assigned to the appropriate positions.

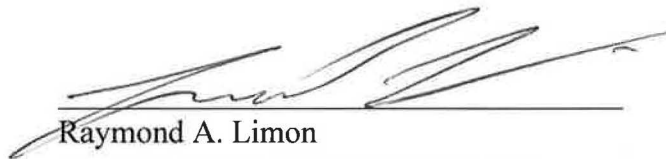
In collaboration with the Department's Office of Human Resources, the bureau Human Resources Offices will conduct annual audit reviews, utilizing the Cybersecurity Data Standard Code Determination checklist, to ensure the Cybersecurity Data Standard codes are continuously being assigned to the appropriate positions.

## **6. Resources**

Guidance on the implementation of this policy can be found within the implementation memorandum (See attachments).

## **7. Questions**

If there are questions or concerns regarding the Cybersecurity Coding requirement, please feel free to reach out to your perspective bureau Human Resources Offices or you can contact Kermit Howard at [Kermit\\_Howard@ios.doi.gov](mailto:Kermit_Howard@ios.doi.gov) at the Department's Office of Human Resources



Raymond A. Limon  
Director, Office of Human Resources

Attachments

November 15, 2016  
Version 1.0

## Federal Cybersecurity Coding Structure

The Federal Government will begin using the new cybersecurity codes (i.e., the Cybersecurity Data Standard) contained in this document upon the Office of Personnel Management's (OPM's) issuance of implementation guidance on the new cybersecurity codes.

The new cybersecurity codes align to the November 2, 2016, version of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The new cybersecurity codes supersede the cybersecurity codes initially implemented by OPM in July 2013.

Agencies will assign these cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions.

Reference: The Federal Cybersecurity Workforce Assessment Act (Act), contained in the Consolidated Appropriations Act of 2016 (Public Law 114-113), was enacted on December 18, 2015 (see pages 735-737 at <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>). The Act requires the Federal Government to implement the NICE coding structure.

### *Federal Cybersecurity Workforce Assessment Act of 2015*

#### *Section 303. National Cybersecurity Workforce Measurement Initiative.*

*(a) IN GENERAL.—The head of each Federal agency shall—*

*(1) identify all positions within the agency that require the performance of information technology, cybersecurity or other cyber-related functions; and*

*(2) assign the corresponding employment code under the National Initiative for Cybersecurity Education in accordance with subsection (b).*

*(b) EMPLOYMENT CODES.—*

*(1) PROCEDURES.—(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Director [of OPM], in coordination with the National Institute of Standards and Technology, shall develop a coding structure under the National Initiative for Cybersecurity Education.*

The **Employment Codes** called for in the Act are synonymous with the OPM cybersecurity codes assigned to each of the Work Roles in the November 2, 2016, version of the NICE Cybersecurity Workforce Framework (NICE Framework).

## Contents

Cybersecurity Codes.....	2
NICE Cybersecurity Workforce Framework .....	3
OPM Cybersecurity Codes Linked to the NICE Cybersecurity Workforce Framework .....	4
Table 1: Work Role Descriptions and New Cybersecurity Codes .....	4
Additional References .....	11
Table 2 – NICE Cybersecurity Workforce Framework Category Descriptions .....	11
Table 3 - NICE Cybersecurity Workforce Framework Specialty Area Descriptions with 2013 OPM Cybersecurity Codes .....	12

## Cybersecurity Codes

In its 2013 and subsequent versions of the Guide to Data Standards (see pages A-103 – A-109 at <http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf>), OPM assigned a unique two-digit cybersecurity code to each of the categories and specialty areas in the NICE Framework version 1.0.

In 2016, the NICE Framework evolved to offer specific Work Roles expanding on the specialty areas in version 1.0. OPM has adopted a three-digit cybersecurity code for each of the Work Roles.

The NICE Framework organizes *information technology (IT), cybersecurity and cyber-related* work into seven high-level categories shown in Table 2; Table 3 provides descriptions of the specialty areas within each of the categories, as well as the original two-digit cybersecurity codes assigned to the specialty areas; and Table 1 shows the Work Roles, their new three-digit cybersecurity codes, and their relationship with specialty areas and categories.

## NICE Cybersecurity Workforce Framework

The NICE Framework contains superset lists of tasks and knowledge, skills, and abilities (KSA) that are associated with cybersecurity work. Also in the NICE Framework, each Work Role is detailed showing the tasks and KSAs that fit within that Work Role.

It is intended that **ALL** *IT, cybersecurity and cyber-related* work is identifiable within the NICE Framework, and that work being performed by an *IT, cybersecurity or cyber-related* position is described by selecting one or more Work Roles from the NICE Framework relevant to that job or position and the mission or business processes being supported by that job or position. Alternatively, the Work Role(s) performed by an *IT, cybersecurity or cyber-related* position can be determined by first identifying in the NICE Framework the tasks carried out by the position and then selecting the Work Role(s) affiliated with those tasks.

Federal *IT, cybersecurity and cyber-related* positions may be comprised of more than one of the Work Roles described in the NICE Framework.

## OPM Cybersecurity Codes Linked to the NICE Cybersecurity Workforce Framework

Table 1: Work Role Descriptions and New Cybersecurity Codes

Category	Specialty Area	Work Role	OPM Code	Work Role Description
Securely Provision	Risk Management	Authorizing Official/Designating Representative	611	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	612	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development	Software Developer	621	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	622	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture	Enterprise Architect	651	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	652	Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.
	Technology R&D	Research & Development Specialist	661	Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts



Category	Specialty Area	Work Role	OPM Code	Work Role Description
				comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning	Systems Requirements Planner	641	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation	System Testing and Evaluation Specialist	671	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development	Information Systems Security Developer	631	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	632	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain	Data Administration	Database Administrator	421	Administers databases and/or data management systems that allow for the storage, query, and utilization of data.
		Data Analyst	422	Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management	Knowledge Manager	431	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support	Technical Support Specialist	411	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).
	Network Services	Network Operations Specialist	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration	System Administrator	451	Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Systems Analysis	Systems Security Analyst	461	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor	731	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Compliance Manager	732	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer	711	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	712	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management	Information Systems Security Manager	722	Responsible for the cybersecurity of a program, organization, system, or enclave.
		COMSEC Manager	723	Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).
	Strategic Planning and Policy	Cyber Workforce Developer and Manager	751	Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
		Cyber Policy and Strategy Planner	752	Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.
	Executive Cyber Leadership	Executive Cyber Leadership	901	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Acquisition and Program/Project Management	Program Manager	801	Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.
IT Project Manager		802	Directly manages information technology projects to provide a unique service or product.	

Category	Specialty Area	Work Role	OPM Code	Work Role Description
		Product Support Manager	803	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	804	Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.
		IT Program Auditor	805	Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst	511	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist	521	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response	Cyber Defense Incident Responder	531	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst	541	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze	Threat Analysis	Warning Analyst	141	Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.
	Exploitation Analysis	Exploitation Analyst	121	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis	All-Source Analyst	111	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and

Category	Specialty Area	Work Role	OPM Code	Work Role Description
				production requirements in support of planning and operations.
		Mission Assessment Specialist	112	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets	Target Developer	131	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
		Target Network Analyst	132	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.
	Language Analysis	Multi-Disciplined Language Analyst	151	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate	Collection Operations	All Source-Collection Manager	311	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors

Category	Specialty Area	Work Role	OPM Code	Work Role Description
				execution of tasked collection to ensure effective execution of the collection plan.
		All Source-Collection Requirements Manager	312	Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning	Cyber Intel Planner	331	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
		Cyber Ops Planner	332	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.
		Partner Integration Planner	333	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.
	Cyber Operations	Cyber Operator	321	Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.
Investigate	Cyber Investigation	Cyber Crime Investigator	221	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Digital Forensics	Forensics Analyst	211	Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	212	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Not Applicable	Not Applicable	Not Applicable	000	Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas.

## Cybersecurity Data Standard Code Determination Checklist

<b>Position Location:</b>	<b>Position Title, series &amp; grade/band:</b>
---------------------------	---

**Instructions:** Mandatory coding data is required for all position descriptions. Bureau HR offices should partner with managers and OCIO representatives, to review position descriptions and determine each position's Cybersecurity data code(s) located in attached.

1. Type of position. Please indicate if this position description is:

- Standardized   
  Encumbered   
  Vacant   
  Funded

2. Work roles/Functional Areas. This position performs duties in the following areas:

- Information technology   
  Cybersecurity   
  Cyber-related   
  None (Code is "000").

3. Cybersecurity Data codes. If multiple, substantial functions exist in a position, managers are allowed to assign up to three cybersecurity data codes per position. Most critical job function is listed first:

1. First data code: \_\_\_\_\_
2. Second data code: \_\_\_\_\_
3. Third data code: \_\_\_\_\_

This position has been reviewed and coded:

OCIO signature:	<b>DATE:</b>
-----------------	--------------

Manager Signature:	<b>DATE:</b>
--------------------	--------------

The code(s) have been annotated on the position description and/or OF-8, and entered into EHRI:

HR Signature:	<b>DATE:</b>
---------------	--------------

Code	Explanation
000	Not Applicable - Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas.
111	All-Source Analyst - All-Source Analysis - Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations. (Analyze)
112	Mission Assessment Specialist - All-Source Analysis - Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness. (Analyze)
121	Exploitation Analyst - Exploitation Analysis - Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks. (Analyze)
131	Target Developer - Targets - Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation. (Analyze)
132	Target Network Analyst - Targets - Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them. (Analyze)
141	Warning Analyst - Threat Analysis - Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments. (Analyze)
151	Multi-Disciplined Language Analyst - Language Analysis - Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects. (Analyze)
211	Forensics Analyst - Digital Forensics - Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents. (Investigate)
212	Cyber Defense Forensics Analyst - Digital Forensics - Analyzes digital evidence and investigates



computer security incidents to derive useful information in support of system/network vulnerability mitigation. (Investigate)

- 221 Cyber Crime Investigator - Cyber Investigation - Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. (Investigate)
- 311 All Source-Collection Manager - Collection Operations - Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan. (Collect and Operate)
- 312 All Source-Collection Requirements Manager - Collection Operations - Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations. (Collect and Operate)
- 321 Cyber Operator - Cyber Operations - Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations. (Collect and Operate)
- 331 Cyber Intel Planner - Cyber Operational Planning - Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace. (Collect and Operate)
- 332 Cyber Ops Planner - Cyber Operational Planning - Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions. (Collect and Operate)
- 333 Partner Integration Planner - Cyber Operational Planning - Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions. (Collect and Operate)
- 411 Technical Support Specialist - Customer Service and Technical Support - Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable). (Operate and Maintain)
- 421 Database Administrator - Data Administration - Administers databases and/or data management

systems that allow for the storage, query, and utilization of data. (Operate and Maintain)

- 422 Data Analyst - Data Administration - Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. (Operate and Maintain)
- 431 Knowledge Manager - Knowledge Management - Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content. (Operate and Maintain)
- 441 Network Operations Specialist - Network Services - Plans, implements, and operates network services/systems, to include hardware and virtual environments. (Operate and Maintain)
- 451 System Administrator - Systems Administration - Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts. (Operate and Maintain)
- 461 Systems Security Analyst - Systems Analysis - Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. (Operate and Maintain)
- 511 Cyber Defense Analyst - Cyber Defense Analysis - Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. (Protect and Defend)
- 521 Cyber Defense Infrastructure Support Specialist - Cyber Defense Infrastructure Support - Tests, implements, deploys, maintains, and administers the infrastructure hardware and software. (Protect and Defend)
- 531 Cyber Defense Incident Responder - Incident Response - Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. (Protect and Defend)
- 541 Vulnerability Assessment Analyst - Vulnerability Assessment and Management - Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. (Protect and Defend)
- 611 Authorizing Official/Designating Representative - Risk Management - Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009). (Securely Provision)
- 612 Security Control Assessor - Risk Management - Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of

the controls (as defined in NIST SP 800-37). (Securely Provision)

- 621 Software Developer - Software Development - Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs. (Securely Provision)
- 622 Secure Software Assessor - Software Development - Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. (Securely Provision)
- 631 Information Systems Security Developer - Systems Development - Designs, develops, tests, and evaluates information system security throughout the systems development life cycle. (Securely Provision)
- 632 Systems Developer - Systems Development - Designs, develops, tests, and evaluates information systems throughout the systems development life cycle. (Securely Provision)
- 641 Systems Requirements Planner - Systems Requirements Planning - Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions. (Securely Provision)
- 651 Enterprise Architect - Systems Architecture - Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures. (Securely Provision)
- 652 Security Architect - Systems Architecture - Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes. (Securely Provision)
- 661 Research & Development Specialist - Technology R&D - Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. (Securely Provision)
- 671 System Testing and Evaluation Specialist - Test and Evaluation - Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results. (Securely Provision)
- 711 Cyber Instructional Curriculum Developer - Training, Education, and Awareness - Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. (Oversee and Govern)
- 712 Cyber Instructor- Training, Education, and Awareness - Develops and conducts training or education of personnel within cyber domain. (Oversee and Govern)
- 722 Information Systems Security Manager - Cybersecurity Management - Responsible for the

- cybersecurity of a program, organization, system, or enclave. (Oversee and Govern)
- 723 COMSEC Manager - Cybersecurity Management - Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009). (Oversee and Govern)
- 731 Cyber Legal Advisor - Legal Advice and Advocacy - Provides legal advice and recommendations on relevant topics related to cyber law. (Oversee and Govern)
- 732 Privacy Compliance Manager - Legal Advice and Advocacy - Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams. (Oversee and Govern)
- 751 Cyber Workforce Developer and Manager - Strategic Planning and Policy - Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements. (Oversee and Govern)
- 752 Cyber Policy and Strategy Planner - Strategic Planning and Policy - Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives. (Oversee and Govern)
- 801 Program Manager - Acquisition and Program/Project Management - Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities. (Oversee and Govern)
- 802 IT Project Manager - Acquisition and Program/Project Management - Directly manages information technology projects to provide a unique service or product. (Oversee and Govern)
- 803 Product Support Manager - Acquisition and Program/Project Management- Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components. (Oversee and Govern)
- 804 IT Investment/Portfolio Manager - Acquisition and Program/Project Management - Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities. (Oversee and Govern)
- 805 IT Program Auditor - Acquisition and Program/Project Management - Conducts evaluations of an IT program or its individual components, to determine compliance with published standards. (Oversee and Govern)
- 901 Executive Cyber Leadership - Executive Cyber Leadership - Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations. (Oversee and Govern)