October 18, 2017

Version 2.0

**Federal Cybersecurity Coding Structure**

This document explains the coding structure used by the Federal Government to identify positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

The Federal Cybersecurity Workforce Assessment Act of 2015 (Act) required the Office of Personnel Management (OPM) to establish procedures to implement the National Initiative for Cybersecurity Education (NICE) coding structure and to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions. To comply with the Act, OPM updated the 2013 cybersecurity codes (i.e., the Cybersecurity Data Standard), contained in the Guide to Data Standards, to map to the August 2017 version of the NICE coding structure.

With the issuance of [OPM’s January 2107 guidance memo](https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity), Federal agencies began assigning the new, 2017 cybersecurity codes to positions with information technology, cybersecurity, or other 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>).

*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 the OPM cybersecurity codes.]

**Cybersecurity Codes**

The Federal Government’s use of cybersecurity codes (i.e., the Cybersecurity Data Standard) [began in 2013](https://www.chcoc.gov/content/special-cybersecurity-workforce-project). The codes have always been based on the NICE Cybersecurity Workforce Framework (NICE Framework), which is explained more in the next section. The first version of the OPM cybersecurity codes contained 2-digit codes that mapped to the Categories and Specialty Areas described in [version 1.0](https://www.nist.gov/sites/default/files/documents/2017/04/04/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf) of the NICE Framework. Under the original coding process, agencies were allowed to assign only one cybersecurity code to a position. The new, second version of the OPM cybersecurity codes contains 3-digit codes that map to the Work Roles described in the most current [NICE Framework](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf). Under this new coding process, agencies may assign up to three cybersecurity codes to a position.

The new, 2017 cybersecurity codes supersede the first version of cybersecurity codes.

The new cybersecurity codes may be viewed in Table 1 of this document and in [OPM’s Guide to Data Standards](https://dw.opm.gov/datastandards/referenceData/2273/current?index=C). The obsolete, first version of cybersecurity codes may be viewed in Table 2 of this document and at <http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf>, pages A-103 – A-109.

**NICE Framework**

The [NICE Framework](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf) organizes information technology, cybersecurity, and cyber-relatedwork and, based on extensive job analyses, groups together work and workers that share common major functions, regardless of job titles or other occupational terms.

Seven Categories form the overarching structure of the NICE Framework. Categories are composed of subgroupings of 33 Specialty Areas. Fifty-two Work Roles are grouped within the Specialty Areas. The Work Roles include a list of common tasks and the knowledge, skills, and abilities needed to perform the role. (See diagram below.) The OPM, 3-digit cybersecurity codes map to the Work Roles.



It is intended that all information technology, cybersecurity, and cyber-related work is identifiable within the NICE Framework, and that work being performed by an information technology, 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 information technology, 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 information technology, cybersecurity, and cyber-related positions may be comprised of more than one of the Work Roles described in the NICE Framework. As information technology, cybersecurity, and cyber-related work continues to evolve, we anticipate the NICE Framework and OPM cybersecurity codes will also expand to capture this work.

NICE has created a webpage with resources designed to support the NICE Framework. This page can be accessed at <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>.

**Cybersecurity Codes Aligned with NICE Framework**

Table 1, below, depicts the alignment of the new, 3-digit cybersecurity codes with the NICE Framework. Table 2, on pages 12-20, contains a crosswalk of the now-obsolete 2013 2-digit cybersecurity codes with the 2017 3-digit cybersecurity codes. We note that the previous 2-digit coding is just a point of reference for agencies as they become familiar with the new codes.

**Table 1: OPM 2017 Cybersecurity Codes Aligned to NICE Framework**

| **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 | Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. |
| Technology R&D | Research & Development Specialist | 661 | Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts 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 secure storage, query, protection, and utilization of data. |
| Data Analyst | 422 | Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow 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 | Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures). |
| 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 Officer/Privacy Compliance Manager | 732 | Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response 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.  |
| Communications Security (COMSEC) Manager  | 723 | Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS). |
| 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 and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. |
| 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. |
| Program/Project Management and Acquisition | Program Manager | 801 | Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities. |
| IT Project Manager | 802 | Directly manages information technology projects. |
| 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 investments that align with the overall needs of mission and 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  | Threat/Warning Analyst  | 141 | Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/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 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 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 to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations. |
| Investigate  | Cyber Investigation  | Cyber Crime Investigator | 221 | Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. |
| Digital Forensics  | Law Enforcement/Counterintelligence Forensics Analyst | 211 | Conducts detailed 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. |

Please reference the [NICE Framework](https://doi.org/10.6028/NIST.SP.800-181) to learn more about the full context of the Work Roles.

**Table 2: CROSSWALK of 2013 2-Digit Cybersecurity Codes (Now Obsolete)**

**with 2017 3-Digit Cybersecurity Codes,**

**Aligned to NICE Framework**

|  |
| --- |
| The table below shows the relationship of the 2-digit cybersecurity codes first used by agencies to identify their cybersecurity workforce in 2013 with the 3-digit cybersecurity codes required to be used today.The crosswalk can serve as a guide when assigning the new codes for positions that already have a properly assigned 2-digit code.  For example, if a *correctly coded PD/ position* was originally old code 62, then an agency may want to use the crosswalk and first look at new codes 621 and 622 to see if one or both match the position.Important Note: The new coding process allows an agency to assign up to three codes per position, while the old coding process allowed for only one code. Using this crosswalk to code a position will most likely not offer three unique substantial functions (three 3-digit cybersecurity codes) from the old single 2-digit code. As such, an agency should follow its own guidance for assigning up to three of the new 3-digit cybersecurity codes for each position. Previous 2-digit coding is just a point of reference that might help speed up the process. |

| **Category****and** **OPM 2013 Code** | **Specialty Area****and** **OPM 2013 Code** | **Work Role** | **OPM 2017 Code** | **Work Role Description** |
| --- | --- | --- | --- | --- |
| Securely Provision60

|  |
| --- |
|  |

 | Risk Management61 | 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 Development62 | 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 Architecture65 | 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 | Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. |
| Technology R&D66 | Research & Development Specialist | 661 | Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.  |
| Systems Requirements Planning 64 | Systems Requirements Planner | 641 | Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions. |
| Test and Evaluation 67 | 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 Development63 | 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 Maintain40 | Data Administration42 | Database Administrator | 421 | Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data. |
| Data Analyst | 422 | Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. |
| Knowledge Management43 | 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 41 | 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 Services44 | Network Operations Specialist | 441 | Plans, implements, and operates network services/systems, to include hardware and virtual environments. |
| Systems Administration45 | System Administrator | 451 | Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures). |
| Systems Analysis46 | Systems Security Analyst | 461 | Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. |
| Oversee and Govern70 | Legal Advice and Advocacy 73 | Cyber Legal Advisor | 731 | Provides legal advice and recommendations on relevant topics related to cyber law.  |
| Privacy Officer/Privacy Compliance Manager | 732 | Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams. |
| Training, Education, and Awareness 71 | 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 Management72/74 | Information Systems Security Manager | 722 | Responsible for the cybersecurity of a program, organization, system, or enclave.  |
| Communications Security (COMSEC) Manager  | 723 | Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS). |
| Strategic Planning and Policy75 | 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 and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. |
| Executive Cyber Leadership90 | 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. |
| Program/Project Management and Acquisition80 | Program Manager | 801 | Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities. |
| IT Project Manager | 802 | Directly manages information technology projects. |
| 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 investments that align with the overall needs of mission and 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 50 | Cyber Defense Analysis51 | 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 52 | Cyber Defense Infrastructure Support Specialist | 521 | Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.  |
| Incident Response 53 | Cyber Defense Incident Responder | 531 | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. |
| Vulnerability Assessment and Management54 | 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. |
| Analyze10 | Threat Analysis 14 | Threat/Warning Analyst  | 141 | Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments. |
| Exploitation Analysis 12 | 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 Analysis11 | 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 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. |
| Targets13 | 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 AnalysisN/A | 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 30 | Collection Operations 31 | 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 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 33 | 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 32 | Cyber Operator | 321 | Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations. |
| Investigate 20 | Cyber Investigation 22 | Cyber Crime Investigator | 221 | Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. |
| Digital Forensics 21 | Law Enforcement/Counterintelligence Forensics Analyst | 211 | Conducts detailed 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 Applicable00 | Not Applicable00 | Not Applicable | 000 | Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas. |