

THE GUIDE TO DATA STANDARDS

Part A: Human Resources

Code	Name / Explanation
00	Not Applicable - Position does not involve work in one or more cybersecurity functions.
10	Analyze - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
11	All Source Intelligence - Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
12	Exploitation Analysis - Analyzes collected information to identify vulnerabilities and potential for exploitation.
13	Targets - Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
14	Threat Analysis - Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
20	Investigate - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.
21	Digital Forensics - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
22	Investigation - Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
30	Collect and Operate - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
31	Collection Operations - Executes collection using appropriate strategies and within the priorities established through the collection management process.

THE GUIDE TO DATA STANDARDS

Part A: Human Resources

- 32 Cyber Operations - Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- 33 Cyber Operations Planning - Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
- 40 Operate and Maintain - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
- 41 Customer Service and Technical Support - Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
- 42 Data Administration - Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
- 43 Knowledge Management - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
- 44 Network Services - Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
- 45 System Administration - Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
- 46 Systems Security Analysis - Conducts the integration/testing, operations, and maintenance of systems security.

Part A: **Human Resources**

- 50 Protect and Defend - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.
- 51 Computer Network Defense (CND) Analysis - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
- 52 Computer Network Defense (CND) Infrastructure Support - Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.
- 53 Incident Response - Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
- 54 Vulnerability Assessment and Management - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
- 60 Securely Provision - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).
- 61 Information Assurance (IA) Compliance - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
- 62 Software Assurance and Security Engineering - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
- 63 Systems Development - Works on the development phases of the systems development lifecycle.

THE GUIDE TO DATA STANDARDS

Part A: Human Resources

- 64 Systems Requirements Planning - Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
- 65 Systems Security Architecture - Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
- 66 Technology Research and Development - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
- 67 Test and Evaluation - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
- 70 Oversight and Development - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.
- 71 Education and Training - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.
- 72 Information Systems Security Operations (Information Systems Security Officer [ISSO]) - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
- 73 Legal Advice and Advocacy - Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- 74 Security Program Management (Chief Information Security Officer [CISO]) - Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel,

Part A: **Human Resources**

infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

- 75 Strategic Planning and Policy Development - Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.
- 80 Cybersecurity Program/Project Management - Manages one or more cybersecurity project(s) or program(s) to provide products and/or services. Coordinates, communicates and integrates cybersecurity projects and program activities. Ensures cybersecurity work efforts achieve the intended or specified outcomes. May encompass the decision-making and negotiation responsibilities involved in executing the program efforts.
- 90 Cybersecurity Supervision, Management, and Leadership - Supervises, manages, and/or leads work and workers performing cybersecurity work (i.e., the work described in the Categories and Specialty Area codes with values 10-75).