U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY SERVICE

Version: March 2025

DHS Cybersecurity Service Capabilities Guide

The DHS Cybersecurity Service Capability Framework

The DHS Cybersecurity Service uses a research-based framework to provide a common language for cybersecurity work and clearly define the qualifications needed to successfully fulfill the Department's cybersecurity mission. This framework is embedded across all aspects of the DHS Cybersecurity Service from selection to development to and performance management.

The DHS Cybersecurity Service Capability Framework comprises:

Categories

Groups of capabilities and underlying competencies that form a cohesive theme: Professional, Leadership, and Technical.

Capabilities

Groups of interrelated knowledge, skills, abilities, behaviors, and other characteristics that contribute to success in a particular area.

Underlying Competencies

Skills and behaviors that can be observed. These underly each of the capabilities.

Before You Apply

1. If you have worked for several years as a cybersecurity professional, you should familiarize yourself with the technical capabilities and identify your primary technical capability. When DHS recruits for specific opportunities, they are often associated with a primary technical capability, which is the focus of assessments all applicants must complete to demonstrate expertise relevant to that opportunity.

2. Read through the professional capabilities to familiarize yourself with the skills and abilities expected of all DHS Cybersecurity Service employees.

3. If you are interested in pursuing a role in the Leadership or Executive Tracks, familiarize yourself with the leadership capabilities.

Technical Capabilities

DHS Cybersecurity Service employees work across different cybersecurity specializations. At DHS, we call these specializations **technical capabilities.** DHS uses technical capabilities to structure DHS Cybersecurity Service careers and match applicants to job opportunities. The following capabilities define and describe the cybersecurity work performed across DHS (e.g., cybersecurity engineering, digital forensics, and vulnerability assessment). Most DHS Cybersecurity Service employees join with a primary technical capability, reflecting most of their cybersecurity technical expertise and experience.

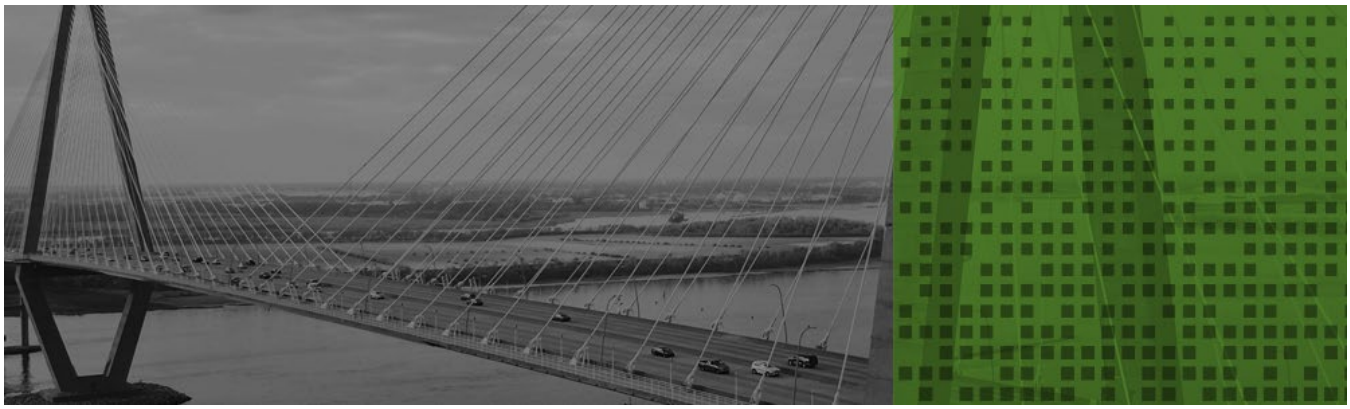
Use the list below to navigate to a specific technical capability.

Technical Capabilities and Underlying Technical Competencies

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Architecture** ▪ Develops system concepts and works on the capabilities phases of the systems development life cycle. ▪ Translates technology and environmental conditions (e.g., laws, regulations, policies, and technical standards) into system and security designs and processes. ▪ Provides recommendations for investment standards and policies that drive how controls will be applied across the organization.	▪ **Systems Requirements Analysis**: Reviews security and privacy requirements to determine system needs and translates those requirements into secure technical and operational specifications. Conducts and evaluates design review based on provided security requirements. Conducts security risk assessments, gap analyses, and business impact analyses to detect system weaknesses, identify the depth and breadth of needed security controls, and make targeted recommendations to address issues and mitigate risks. ▪ **Secure Network Design**: Designs and evaluates networks that are secure from known and perceived methods of cyber attack on all elements including but not limited to wired and wireless elements, Cloud-based, and virtual environments incorporating secure controls. Establishes defense in-depth mechanisms to detect, deflect or mitigate cyber attacks on networks and communications systems and structures. Maintains appropriate levels of resiliency to maintain viability of the network. ▪ **Secure Software Design**: Designs and evaluates software that is secure from known and perceived methods of cyberattack. Analyzes software risks, understands likely points of attack, and decides how software will deal with potential attack. Conducts secure code review in accordance with software assurance best practices. Assesses systemic threats in the deployment environment and vulnerabilities of application. ▪ **Secure Systems Development**: Executes and/or assists with development based on secure design specifications, utilizing secure tools and methodologies. Takes into consideration security controls, recovery strategies, contingency plans, and testing and evaluation. Tracks and corrects system defects through testing and implementation phases. ▪ **Systems Testing and Evaluation**: Provides oversight of systems testing and evaluation and test case development and mapping. Develops objectives and criteria for testing program. Approves and evaluates testing framework. Validates and ensures completion of contingency planning. ▪ **Regulatory Advisory**: Provides IT security recommendations and advice to leadership and staff based on relevant guidelines, organizational policy, and other approved guidance. Advocates for policy changes that will support new initiatives or required changes or enhancements in support of security and privacy initiatives.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Defensive Operations—Intelligence Collection and Analysis** ▪ Responsible for the integration, management, and execution of all aspects of the cyber attack lifecycle to inform cyber defensive operations. ▪ Plans and executes end-to-end cybersecurity operations to defend protected assets. ▪ Plans collection operations, retrieves and analyzes key intelligence data. ▪ Understands where to focus surveillance. ▪ Oversees specialized denial and deception operations and collection of cybersecurity information that informs and develops the end-to-end operations.	▪ **Intelligence Collection**: Identifies and gathers and disseminates information on cyber threats using various intelligence collection tools and methods. Collects information on threat actors seeking to conduct cyber operations against homeland networks. Identifies information needs and requirements of customers and formulates collection plans and strategies to meet those needs. ▪ **Intelligence Analysis**: Analyzes and interprets all-source intelligence on current and emerging cyber threats to identify and evaluate the intent and capabilities of cyber actors using Intelligence Community analytic standards. Contributes to the intelligence cycle by evaluating intelligence information and identifying customer needs for finished intelligence analysis. Collaborates with counterparts, partners, and stakeholders. Coordinates intelligence products with counterparts in the Intelligence Community. Provides cyber intelligence and analysis to inform cyber operations. Produces finished intelligence assessments that contextualize all-source intelligence with cybersecurity expertise and Intelligence Community analytic tradecraft to identify and evaluate cyber threats. Documents and presents intelligence analyses and findings to senior government officials and other decision makers, planners, and network defenders. ▪ NOTE: There are two subtypes of Cybersecurity Defensive Operations. An individual whose primary technical capability is Cybersecurity Defensive Operations—Intelligence Collection and Analysis focuses on the underlying competencies above.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Defensive Operations—Planning, Execution, and Analysis** ▪ Responsible for the integration, management, and execution of all aspects of the cyber attack lifecycle to inform cyber defensive operations. ▪ Plans and executes end-to-end cybersecurity operations to defend protected assets. ▪ Plans collection operations, retrieves and analyzes key intelligence data. ▪ Understands where to focus surveillance. ▪ Oversees specialized denial and deception operations and collection of cybersecurity information that informs and develops the end-to-end operations.	▪ **Operations Planning and Execution**: Creates end-to-end tactical and strategic level cyber operations plans based on technical cybersecurity understanding, applicable policies, and cyber rules of engagement. Develops primary and contingency action plans and selects the most appropriate and effective methods of defense/attack that align with operational protocols. Employs available capabilities for mounting defensive/offensive cyber operations against identified threats. Applies knowledge of national strategies, plans, policies, and directives for offensive and defensive cyber operations (e.g., DoD Directive 3600.1, DCIDs, NSPDs, HSPDs). ▪ **Operations Analysis**: Preemptively looks for indicators of compromise. Examines and integrates digital forensics and incident response data to bolster defenses at each step of the operations process. Works with intelligence components to understand identified intrusion sets and deviations. Completes reverse malware analysis and engineering. ▪ NOTE: There are two subtypes of Cybersecurity Defensive Operations. An individual whose primary technical capability is Cybersecurity Defensive Operations—Planning, Execution, and Analysis focuses on the underlying competencies above.



TECHNICAL CAPABILITY

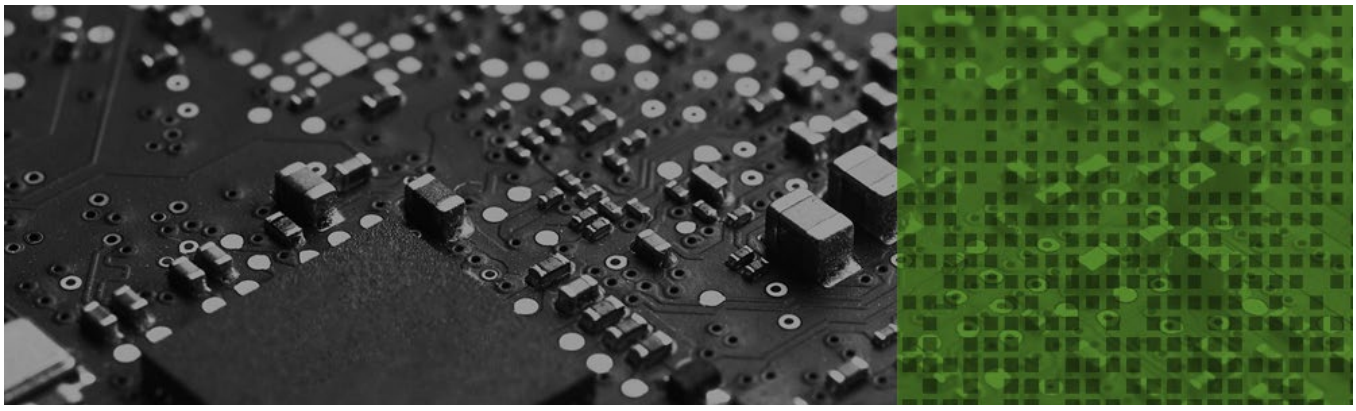
Cybersecurity Engineering

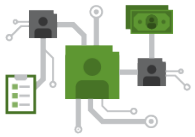
- Conducts software, hardware, and systems engineering to develop new and refine/enhance existing technical capabilities, ensuring full integration with security objectives, principles and processes.
- Builds practical solutions in full consideration of lifecycle of costs, acquisitions, program and projects, management and budget.
- Identifies engineering requirements for, and ensures interoperability of, internal and external systems.
- Demonstrates strategic risk understanding, considering impact of security breaches or vulnerabilities in every aspect of the engineering process.
- Stays current on emerging technologies, and their applications to current and emerging business processes (e.g., cloud, mobile), and identifies and recommends methods for incorporating promising technologies to meet organizational cybersecurity requirements.

TECHNICAL COMPETENCY

- **Cybersecurity Hardware Engineering**: Applies knowledge of the principles, methods, and tools for designing, developing, and testing computer or computer-related equipment. Responsible for secure supply chain assurance.
- **Cybersecurity Systems Engineering**: Provides security-focused systems engineering support and inputs throughout the entire design lifecycle, including equipment selection, implementation and as-built documentation, factory and on-site installation, validation and cybersecurity system optimization, and ensuring interoperability with DHS systems, where appropriate. Leverages existing capabilities to meet business needs.
- **Secure Software/Application Design**: Designs, develops and evaluates software and applications that are secure. Analyzes risks, understands likely points of attack, and identifies how software/applications will deal with potential attack. Communicates design principles and works with applicable stakeholders to ensure security best practices are followed throughout the lifecycle. Assesses systemic threats, vulnerabilities and impacts in deployment environment and application.
- **Cybersecurity Capability/Solutions Evaluation**: Researches and analyzes cybersecurity services or capabilities to determine their potential for meeting organizational standards and business and mission needs/requirements. Identifies gaps in coverage for future remediation.
- **Cybersecurity Testing and Evaluation**: Supports the in-depth, end-to-end testing, validation and interpretation of security events to ensure secure design and development in alignment with established security protocols, certification and accreditation processes and contingency plans. Calibrates tests to provide meaningful measures of risks. Oversees and coordinates hands-on testing of management, operational, and technical controls and works with relevant experts as needed. Evaluates and assigns security risk value for systems approval prior to implementation and corrects or supplies remediation or mitigation. Effectively prioritizes cybersecurity events.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
Cybersecurity Policy ▪ Applies knowledge of information security to define the organization's direction and direct resources to achieve the mission. ▪ Develops and recommends policy changes to support mission needs. ▪ Manages security implications within the organization as directed.	▪ **Strategic Planning**: Designs and supports a cybersecurity strategy that aligns to the organization's broader vision, mission, and business goals. Ensures sound principles and best practices are implemented in the delivery of planning and management services. Advises leadership of risks and benefits to organizational strategy. ▪ **Policy Advisement**: Provides guidance to stakeholders on cybersecurity policy implementation and interpretation. ▪ **Cybersecurity Policy Development and Writing**: Assesses cybersecurity policy needs and collaborates with stakeholders to develop and revise cybersecurity policies and programs. Translates applicable laws, statutes, and regulatory documents and integrates into policy. ▪ **Cybersecurity Governance**: Applies knowledge of laws, government regulations, executive orders, agency rules, government organization and functions, and current Administration requirements to cybersecurity. ▪ **Cybersecurity Legislative Affairs**: Leads the Department's engagement with the Legislative Branch to achieve and maintain the necessary authorities and resources required to meet mission critical priorities.



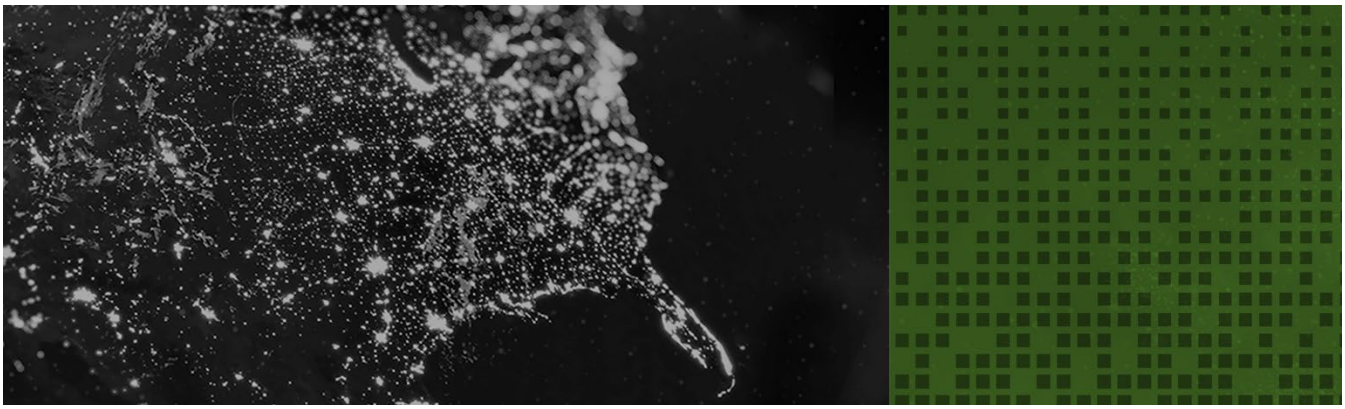
TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Program Management** Manages information security programs within the organization, to include strategic, personnel, security infrastructure, policy enforcement, emergency planning, security awareness, and acquisition considerations.	▪ **Cybersecurity Program Design**: Drives development of cybersecurity programs based on internal and external requirements. Understands the operating environment (e.g. domain, agencies, relationships, culture), scope, and external influences (cyber threat landscapes, applicable authorities and directives) and how interdependencies impact program design. Incorporates compliance with privacy requirements into all elements of program design. Reviews current and future cybersecurity programs and provides recommendations and findings to justify business case. Defines cybersecurity and performance metrics for evaluating program outcomes or impact. ▪ **Cybersecurity Program Execution**: Leads, coordinates, communicates, integrates, and is accountable for the overall success of cybersecurity programs, ensuring alignment with critical agency cybersecurity priorities. Safeguards private and classified information. Purposefully shares intellectual capital and relevant information to appropriate stakeholders and partners. Evaluates programs or its individual components to determine compliance with established organizational and external standards. ▪ **Cybersecurity Investment Management**: Manages or reviews cybersecurity capabilities, responsibilities and requirements to ensure that they align with the overall needs of mission and business enterprise priorities. Applies knowledge of the principles and methods of capital investment analysis and business case analysis, including Earned Value Management (EVM) and/or return on investment analysis.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
Cybersecurity Research and Development ▪ Conducts technology and/or feasibility research, development, and assessments. ▪ Provides, builds, tests and supports a prototype capability and/or evaluates its security and utility. ▪ Plans, conducts or oversees comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. ▪ Ensures appropriate security measures are considered throughout each phase of the R&D lifecycle.	▪ **Cybersecurity Research Planning**: Sets strategic thresholds and objectives for research and development efforts. Applies a systematic, rigorous, and disciplined scientific approach to research planning that addresses current and future security threats and vulnerabilities. Prioritizes research and development activities to achieve the greatest impact. Considers current events, marketplace developments, and emerging and projected threats and integrates into planning activities. ▪ **Cybersecurity Research Development and Delivery**: Designs, models, develops and prototypes capabilities to enhance cybersecurity and detect vulnerabilities. Applies evidence-based research results into adopted technologies, especially for emerging technologies and threats. ▪ **Cybersecurity Research Testing and Evaluation**: Evaluates and quantifies success of research and development initiatives to meet defined requirements. Assesses developed capabilities against specifications and requirements. Validates functionality at capability and sub-capability levels.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Risk Management and Compliance** ▪ Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to ensure that existing and new information technology systems meet the Department's cybersecurity and risk requirements, and provide decision makers with the knowledge to make well-informed risk decisions. ▪ Ensures that strategic considerations drive investment and operational decisions with regard to managing risk to organizational operations (including mission, function, image and reputation), organizational assets, individuals, other organizations (collaborating or partnering with federal agencies and contractors) and the nation. ▪ Understands and utilizes the National Institute of Standards and Technology (NIST) series of documents.	▪ **Organizational Risk Strategy**: Determines the adverse impact or consequences to the organization in order to guide and inform subsequent risk management processes and tasks. Considers risk assumptions and organizational tolerance for risk to inform strategic decision making. ▪ **Organizational Risk Assessment**: Identifies, selects, tailors, implements, documents and assesses the security and privacy controls necessary to protect the system and the organization commensurate with the risk to organizational operations and assets. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. ▪ **Organizational Risk Management**: Authorizes system operation based upon a determination of the risk to organizational operations and assets. Monitors and maintains an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions. Reports on the security state of the system to appropriate organizational stakeholders. ▪ **Policy Interpretation**: Translates strategy into policy, and determines policy impact on strategy. Interprets policy and converts into appropriate procedures, contracts and performance measures. Determines level of risk tolerance for policy.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Cybersecurity Threat Analysis** ▪ Collects, analyzes, and reports on cybersecurity threats and threat actors to support operations. ▪ Understands and analyzes different sources of information (e.g., INTs open source, law enforcement data) on specific topics or targets. ▪ Provides tactical/operational analysis, including attribution of cyber actors using a variety of analytic techniques and tools. ▪ May also provide strategic-level analysis to support broader mission. ▪ Develops and communicates situational awareness of local, regional, and international cybersecurity threats impacting stakeholder missions and interests.	▪ **Intelligence Analysis**: Analyzes and interprets all-source intelligence on current and emerging cyber threats using Intelligence Community analytical standards. Shares intelligence and analysis with customers and partners and coordinates with partner agencies. Provides cyber intelligence and analysis to inform cyber operations. Produces finished intelligence assessments that contextualize all-source intelligence with cybersecurity expertise and Intelligence Community analytic tradecraft to identify and evaluate cyber threats. Documents and presents intelligence analyses and findings to senior government officials and other decision makers and network defenders. **Warning Analysis**: Identifies, develops, shares or otherwise contextualizes cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments. Presents and explains findings in actionable terms; builds a case for action. ▪ **Threat Assessment**: Identifies the potential impact of organizations, entities, circumstances, and events that have the potential to harm the enterprise architecture, networks, communications, applications, and systems. Analyzes cybersecurity threats, including insider threats, to determine their probability and consequences. Develops mitigation strategies and assesses the benefits and risks to inform resource requirements of each. Performs scanning and probing activities to augment assessment.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Data Science** ▪ Examines data with the goal of providing new insight for the purposes of cybersecurity. ▪ Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data analytics, and research purposes. ▪ Applies understanding of cybersecurity field to inform analytical methodologies and algorithms selected for implementation. ▪ Designs, builds, implements, integrates, and maintains systems and tools for data trend and pattern analysis of cyber data. ▪ Applies knowledge of statistics and mathematical theory to develop and integrate new and emerging technologies, such as machine learning and deep learning concepts and techniques. ▪ Communicates insights gained to mission user.	▪ **Data Collection and Ingestion**: Integrates data from several disparate sources, which are stored using different technologies, to provide a unified view of the data. Collects and organizes complex data. ▪ **Data Management**: Cleans, converts, and standardizes data for analysis. Provides oversight to enterprise data management systems (e.g., SPLUNK) and cloud-based systems (e.g., AWS). Manages web data, log data, and threat data analytics, using a variety of tools including Google Analytics. Applies knowledge of essential cybersecurity policies to data management. ▪ **Statistical Modeling**: Uses various tools (e.g., SPSS, SAS, R, STATA) and methodologies for analyzing and interpreting complex data to discover new patterns and behaviors and to provide usable information to decision makers and other users. ▪ **Data Visualization**: Uses visualization tools (e.g., R, Tableau, Flare, Google Visualization API, RGIS) to design and exhibit graphic representations of data findings to facilitate understanding by business users and decision-makers.



TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Digital Forensics** ▪ Collects, processes, analyzes, interprets preserves, and presents digital evidence in support of network vulnerability mitigation, intelligence operations, and different types of investigations (including but not limited to administrative, criminal, counterintelligence and law enforcement). ▪ Applies Tactics, Techniques and Procedures (TTP) for investigative processes.	▪ **Forensic Analysis**: Applies the principles and techniques for gathering, recovering, analyzing, interpreting, and preserving and presenting information and digital evidence (from computers, mobile devices, websites, network packets, etc.) to support legal prosecution or other departmental requirements. Transforms information to make it readable and interpretable and uses forensic artifacts, data, and reports to understand and/or reconstruct a digital process, event or activity. ▪ **Cyber Investigation**: Applies TTPs for a full range of investigative tools and processes, and conducts activities in accordance with applicable laws, policies, guidelines regulations and procedures. ▪ **Reverse Engineering**: Applies various techniques and tools (e.g., hexadecimal dumper, disassembler, debugger) to analyze software/hardware, retrieve its source code, and understand its component parts, functions, and purpose to identify the software's underlying vulnerabilities and exploitable weaknesses. ▪ **Malware Analysis**: Applies knowledge of malicious software programs and code that interfere with normal computer functions or send data to unauthorized parties.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Mitigation and Response** ▪ Tracks and responds to prioritized urgent IT and cyber events and indicators of compromise (IOCs) to mitigate threats to networks, systems, and applications. ▪ Investigates and analyzes response activities and employs various advanced response and recovery approaches as appropriate. ▪ Applies understanding of tactics, techniques, and procedures for investigative processes, including identifying adversaries' TTPs and applying corresponding defense or security controls. ▪ Conducts root cause analysis and response coordination, providing recommendations for mitigation. ▪ Executes recovery action plans and adapts plans to handle new developments.	▪ **Incident Response and Recovery**: Uses information known about incidents and their effects on networks, systems, and applications to identify and prioritize short- and long-term recovery and repair actions. Creates recovery action plans for repairs, including mitigation strategies for interim system vulnerabilities/deficiencies. Handles incidents in accordance with NIST stages of incident handling guidelines. Executes recovery action plans and adapts plans to handle new developments. ▪ **Network Monitoring and Defense**: Applies knowledge of defensive measures to detect, respond, and protect information, information systems, and networks from threats. Proactively analyzes network traffic for patterns using analytic tools and data science methodologies. ▪ **Malware Analysis**: Applies knowledge of malicious software programs and code that interfere with normal computer functions or send data to unauthorized parties to identify threat actors' TTPs (via root cause analysis).
 **Secure Network Operations** Understands the installation, configuration, testing, operation, maintenance, and management of networks and their firewalls, including hardware and software, which permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.	▪ **Network Engineering**: Plans, implements, and supports computer networks that organizations rely on to access, share, and store information. ▪ **Operating Systems**: Applies knowledge of computer network, desktop, mobile, and mainframe operating systems and their applications. ▪ **Distributed Systems**: Applies knowledge of the principles, theoretical concepts, and tools underlying distributed computing systems, including their associated components and communication standards. ▪ **Network Management**: Manages the operation, administration, and maintenance of network and telecommunication systems and linked systems and peripherals.

TECHNICAL CAPABILITY

Secure Software Engineering

- Conducts software system planning and development to create new, and enhance existing, technical solutions, following industry best practices for quality, security, scalability, and reliability.
- Develops software using modern best practices and cross-functional knowledge of the entire software development landscape including agile methodologies, continuous integration and continuous deliver (CI/CD) processes, automated testing, and secure system design and analysis.
- Creates software that accounts for common and uncommon security risks throughout the software development lifecycle (SDLC) and reviews existing systems and software development processes for potential security issues.
- Stays current on emerging technologies, trends, and practices and recommends pathways to implement such improvements to meet organizational goals and requirements.

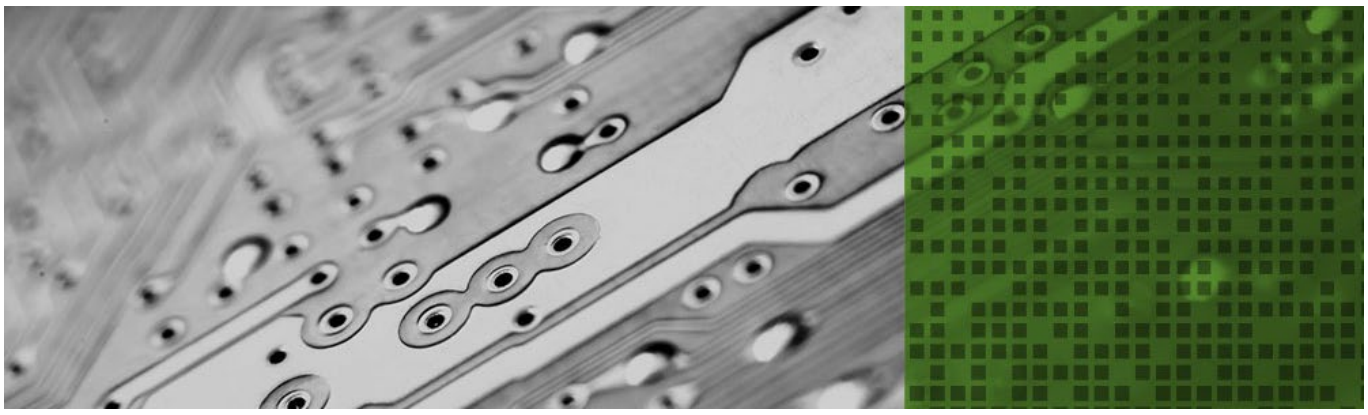
TECHNICAL COMPETENCY

- **System Design**: Designs, develops, and evaluates software and applications that are secure, scalable, reliable, and redundant. Analyzes risks, understands likely points of attack and points of failure, and identifies how software/applications will deal with potential risks. Designs systems to ingest, process, store, scale, and return data, including connections to other systems such as databases and external APIs. Communicates design principles and works with applicable stakeholders to ensure security, software, and infrastructure best practices are followed throughout the lifecycle. Researches and analyzes available software services or capabilities to determine their potential for meeting organizational standards and business and mission needs/requirements. Assesses systemic threats, vulnerabilities, scalability challenges, and impacts in deployment environment and application.
- **System Testing and Evaluation**: Supports in-depth unit, functional, and end-to-end testing; validation; and remediation in alignment with established best practices. Recognizes adequate code coverage and differentiates categories of coverage in order to prioritize test cases based on risk. Recognizes the role of test automation in the overall SDLC and identifies, prioritizes, and remediates issues from automated reports, including assessing the risk level for security issues and bugs.
- **Developer and Security Operations**: Coordinates with DevSecOps engineers to ensure tools are configured properly for the given code environments. Identifies the role and importance of CI/CD in a modern software engineering practice. Monitors CI/CD pipelines and deployments for issues related to source code quality, security, and stability; interprets results and takes corrective actions.
- **Code Authoring and Review**: Writes secure, documented, appropriately complex, and maintainable source code resulting in reliable systems to solve business problems. Recognizes and addresses source code vulnerabilities. Accounts for expected and unexpected errors and exceptions at each level of a system and handles them appropriately. Interprets and evaluates existing code to understand functionality while assessing for security vulnerabilities, performance issues, and reliability.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Physical, Embedded, and Control Systems Security** Applies expertise to understand designs, protocols, and physical configurations of purpose-built interconnected systems—such as industrial control systems, physical systems, and embedded systems—and can define and implement comprehensive countermeasures to detect threats and maintain the overall cybersecurity posture of these systems.	▪ **Embedded Compute Systems**: Applies knowledge of specifications and uses of specialized physical, virtual or compute systems that communicate with interconnected systems and/or devices (e.g., automobiles, GPS, telecom applications). ▪ **ICS/SCADA**: Applies knowledge of computer-controlled systems that monitor and impact industrial processes deployed across physical systems and elements of the Critical National Infrastructure (e.g., nuclear power plants, reprocessing facilities, chemical plants, oil refineries, ports, maritime transport systems, ships and aircraft). ▪ **Internet of Things**: Applies knowledge of the foundations of architectures, applications, security, and protocols that underpin the Internet of Things. Actively monitors and supports the design/build/configure/operate/maintain cycle of interconnected systems. ▪ **Building/Facilities Automation**: Applies knowledge of cybersecurity vulnerabilities in facilities' underlying systems (e.g., access control, HVAC) to secure against intrusion or misuse and detect and defend the security posture.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Security System Operations and Maintenance** ▪ Implements, configures, and manages security devices and systems (such as firewalls, intrusion detection and log collectors, and vulnerability scanners) in accordance with policies, procedures, and best practices. ▪ Installs, manages, and monitors security measures to support mitigation efforts; shares relevant information with system and network administrators.	▪ **Security Systems Administration**: Performs administrative functions necessary to maintain the security of relevant systems. Operates and maintains processes and tools that allow for agile response to cyber incidents. Aggregates information into a security system status and periodically reports this information to appropriate authorities. Takes action to mitigate any issues that may compromise security. Manages system changes, working with key personnel to ensure systems security is not compromised during systems changes or transitions from development to production. Continuously evaluates security systems configuration. ▪ **Security Implementation Knowledge**: Knowledge of systems implementation activities required to ensure successful transition from development to production and operation. Knowledge of user acceptance testing. Understanding of contingencies and risk mitigation that may compromise security. Awareness of the preparation, training, and education of user community required to support implementation efforts. ▪ **Information Systems Security Monitoring**: Collects, organizes, analyzes, reports and acts on information related to security activities and events on computer networks, systems, and applications. Continuously monitors enterprise systems to identify unauthorized and/or malicious activities and events to maintain the security posture of the system. Classifies the threat and risk levels of activities and events and follows appropriate notification and escalation procedures. ▪ **Continuity of Security Operations**: Executes plans and procedures to respond to security incidents that interrupt ongoing cybersecurity operations that minimize damage, restore operations, maintain system integrity, and maximize system resilience. Executes incident response and containment procedures per established protocols. Adapts to changing or unforeseen circumstances and adjusts COOP plans and procedures to address these circumstances. Communicates information and courses of action to leadership and other appropriate parties.

TECHNICAL CAPABILITY	TECHNICAL COMPETENCY
 **Vulnerability Assessment** ▪ Conducts assessments of threats and vulnerabilities on networks/systems software and hardware, and develops and recommends appropriate mitigation countermeasures. ▪ Develops and conducts tests of systems to evaluate compliance with specifications and requirements in accordance with policy, benchmarks and industry best practices, by validating technical, functional, and performance characteristics of systems or their elements. ▪ Coordinates and aligns with program offices and various stakeholders.	▪ **Vulnerability Risk Assessment**: Applies knowledge of the tactics, techniques and procedures (TTP) of cyber exploitation and attack to identify, quantify, prioritize, and report vulnerabilities in enterprise architectures, networks, communications, applications, and systems. Analyzes and recommends mitigation of proposed countermeasures and evaluates their system or mission risk, impact, and effectiveness post-implementation. Works with systems engineering and development teams to recommend remediation strategies throughout the systems development life cycle (SDLC). ▪ **Penetration Testing**: Designs, simulates, and executes attacks on networks and systems by using existing and emerging methods and TTPs to make attributions, attack systems and exploit vulnerabilities. Documents methodologies, findings and impacts, and recommends mitigation and remediation techniques.



Professional Capabilities

The following define and describe what are commonly referred to as "soft-skills." Professional capabilities are required for successful demonstration of all DHS cybersecurity work and as such, all DHS Cybersecurity Service employees are expected to demonstrate proficiency within their roles.

Use the list below to navigate to a specific professional capability.

Professional Capabilities and Underlying Competencies

PROFESSIONAL CAPABILITY	PROFESSIONAL COMPETENCY
Continual Learning ▪ Uses efficient learning techniques to acquire and apply new knowledge and skills. ▪ Pursues training, feedback, or other opportunities for self-learning and ongoing development.	▪ **Self-Development:** Continually seeks to learn new information and expand skills through informal and formal training opportunities. Solicits feedback from others to identify areas for improvement and growth. Independently seeks out novel opportunities to learn and develop. ▪ **Initiative:** Proactively determines what is needed to meet mission objectives and assumes responsibility for carrying out the work without being told. ▪ **Inquisitiveness:** Demonstrates the intellectual curiosity needed to tackle challenging problems with the innate desire to continuously search until an answer is found. Generates innovative, "outside-the-box" ideas and solutions.

PROFESSIONAL CAPABILITY	PROFESSIONAL COMPETENCY
Critical Analysis Practices the objective analysis and evaluation of an issue to form a judgment or decision that impacts a task, process, or program.	▪ **Problem Solving:** Uses inductive and deductive reasoning to make inferences, test hypotheses, and reach conclusions. Weighs relevance and accuracy of information to generate alterative solutions and recommendations. Identifies and analyzes challenges, issues, and setbacks. ▪ **Analysis:** Leverages the appropriate tools, technology, and processes to systematically gather, synthesize, organize, review, and assess available relevant information to draw sound and logical conclusions. ▪ **Creativity:** Conceptualizes, creates, and recommends new designs and processes based on new ideas. When confronted with unexpected challenges, questions conventional approaches and offers novel solutions. ▪ **Situational Awareness:** Operates with knowledge of the dynamics of the relevant environment, knows and understands what is happening in the current situation, and is able to predict and adapt to how circumstances are likely to change over time.
Customer Orientation Supports stakeholders and colleagues in an empathetic manner to resolve business and technical problems.	▪ **Empathy:** Understands the feelings, thoughts, and experiences of stakeholders and colleagues and responds with compassion to resolve difficulties. ▪ **Problem Resolution:** Understands stakeholder and colleague problems, offers appropriate, ethical solutions, executes effective problem solving, and continues support until resolution. ▪ **Technical Support:** Provides enterprise level technical support to customers and partners and works to resolve complex user issues; works with professionalism and a sense of urgency to deliver solutions that meet customer and partner needs.

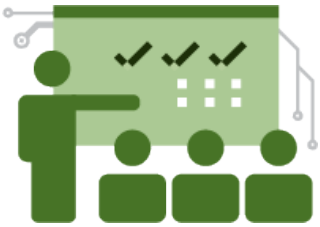
PROFESSIONAL CAPABILITY	PROFESSIONAL COMPETENCY
Effective Communication ▪ Communicates and understands complex ideas (e.g., technical, security, and risk-related). ▪ Appropriately consolidates and recapitulates information to a variety of technical and non-technical audiences across levels.	▪ **Verbal Communication:** Presents oral and written information in a concise, logical, objective and grammatically correct manner. Differentiates and clearly conveys materials as facts, opinions, or conjectures. Uses active listening skills to check for understanding. ▪ **Technical Communication:** Adjusts the level of technical detail based on the needs and perspectives of the audience, and translates highly technical concepts accordingly. Engages with key stakeholders and leadership to communicate the importance of technical findings and their mission/business impact. ▪ **Persuasion:** Constructively influences others to consider alternative points of view, accept recommendations, cooperate with colleagues, or alter their behavior in alignment with mission goals. ▪ **Constructive Feedback:** Solicits, listens to, and acts on constructive feedback to enhance technical, professional, or managerial capabilities. Proactively and professionally provides constructive feedback to others to enhance their capabilities and/or aid their development.
Partnerships ▪ Encourages and facilitates cooperation, trust, and group identity with others by fostering commitment and team spirit. ▪ Works with others to achieve shared goals.	▪ **Collaboration:** Identifies and pursues shared goals and works constructively with others to achieve results aligned to stakeholder and business needs. Seeks opportunities to break down silos and facilitate information sharing between team members. ▪ **Negotiation:** Understands different perspectives, works to find mutually-acceptable solutions, and identifies opportunities for consensus. ▪ **Relationship Building:** Develops networks, builds alliances and coalitions, and partners across departments to build strategic relationships with the intent of achieving mission goals.

PROFESSIONAL CAPABILITY	PROFESSIONAL COMPETENCY
Professional Conduct ▪ Demonstrates trustworthy and ethically grounded business practices. ▪ Considers the impact and influence of various stakeholders and decision-makers.	▪ **Business Acumen:** Understands the organization's operating model, financials, and culture and ensures that initiatives and work products align with short and long-term objectives. Demonstrates accountability and responsibility for own work. Plans, prioritizes, and balances assignments to ensure timely and effective completion of tasks; makes adjustments as needed to adapt to changing situations. ▪ **Ethics and Integrity:** Upholds transparency in dealings, impartiality, appropriate standards of conduct, trustworthiness, and ethical behavior in all work activities. Appropriately handles classified or sensitive information including, but not limited to, proprietary information, law enforcement sensitive, Personally Identifiable Information, Protected Health Information, and other limited distribution data. Acts with a public service orientation, considering the public good and mission objectives. ▪ **Stewardship:** Proactively establishes, monitors, and advocates for internal controls (e.g., policies and procedures) to ground ethical business practices. Makes effective and efficient use of time and other available resources. ▪ **Political Savvy:** Identifies, understands, and successfully navigates formal and informal cultural norms, power dynamics, and political complexities within the workplace that impact the organization and external partnerships.
Resilience ▪ Exhibits high levels of commitment and control around work activities, even in non-ideal circumstances. ▪ Conveys an openness to new experiences and challenges. ▪ Recovers effectively after experiencing stressful or adverse situations.	▪ **Adaptability and Flexibility:** Adjusts easily to a variety of situations and can quickly change approach or methodology to effectively and successfully meet objectives. In the face of unforeseen impediments, applies existing knowledge to new experiences and situations. ▪ **Ambiguity Tolerance:** Works comfortably in situations without complete information, a clear set of guidelines, or clarity about desired outcomes. Perceives ambiguous situations as a challenge rather than a threat, and continues to deliver solutions in the face of uncertainty. ▪ **Perseverance:** Sets high professional standards to achieve results and remains professional and goal-focused when confronted with challenges, roadblocks, or adverse conditions. Rebounds from setbacks without getting discouraged.

Leadership Capabilities

In addition to professional and technical capabilities, those leading cybersecurity work, people, and organizations requires the highest levels of proficiency in the following areas.

Use the list below to navigate to a specific leadership capability.



Leadership Capabilities and Underlying Competencies

LEADERSHIP CAPABILITY	LEADERSHIP COMPETENCY
Leading Change ▪ Anticipates and brings about strategic change, both within and outside the department, to meet organizational goals. ▪ Establishes a vision and facilitates the methods needed to enable others to implement that vision.	▪ **Strategic Foresight:** Formulates objectives and implements plans consistent with the long-term interests of the department in a global environment. Proactively identifies potential challenges, obstacles, and impediments and alters strategy appropriately. Prudently capitalizes on opportunities and appropriately manages risks in a constructive fashion. Takes a strategic view and builds a shared vision for others. ▪ **Environmental Awareness:** Understands and keeps up to date on local, regional, national, and international policies and trends that affect the department, shape stakeholders' views, and influence daily work. Maintains awareness of the department and organization's impact on external stakeholders. ▪ **Change Sponsorship:** Recognizes and acts in support of large- and small-scale changes necessary for organizational improvement. Acts as a catalyst for organizational and departmental change and influences others to translate vision into action. Proactively anticipates and addresses potential sources of resistance.

LEADERSHIP CAPABILITY	LEADERSHIP COMPETENCY
Leading Individuals and Teams ▪ Guides employees toward meeting the department's vision, mission, and goals. ▪ Facilitates cooperation and teamwork and supports constructive resolution of conflicts.	▪ **Conflict Resolution:** Encourages creative tension and differences of opinions while anticipating and taking steps to prevent counter-productive confrontations or dysfunctional behaviors. Actively addresses, manages, and resolves conflicts and disagreements in a timely and constructive manner. ▪ **Staff Development:** Enhances others' ability to perform and contribute to current and future department needs by providing ongoing feedback and facilitating opportunities to learn through formal, experiential, and informal methods. Proactively plans ahead to develop and maintain a bench of talent able to grow within the organization. ▪ **Team Building:** Inspires and fosters shared commitment, spirit, pride, and trust in others. Facilitates cooperation and motivates team members to accomplish group goals. Empowers others to achieve results. Delegates assignments, tasks, and opportunities effectively to the lowest organizational level capable of accomplishment. ▪ **Accountability:** Holds self and others accountable for delivering high-quality, timely, and cost-effective results. Determines objectives, sets priorities, and delegates work. Accepts responsibility for mistakes. Complies with established control systems and rules.
Leading Organizations ▪ Uses clear vision and strategic alignment of business, human capital, cultural and information system elements to create momentum. ▪ Monitors, evaluates, and manages the organization, oversees performance management, and adjusts elements as needed to maximize organizational effectiveness.	▪ **Shared Vision and Alignment:** Creates clear vision with strategic alignment between business, human capital, and information system elements to maximize organization productivity. Builds and sustains organizational momentum to achieve the vision through communication, clarity, and commitment. ▪ **Cultural Adaptability:** Understands, assimilates, and adapts to achieve results in various cultures (e.g., team, departmental, organizational), and strategically shapes modes of engagement (e.g., communicating, motivating, and managing) to maximize organizational effectiveness. ▪ **Organizational Effectiveness:** Monitors and manages the organization's ability to meet objectives and achieve its mission through several key areas, including leadership development, organization design, deploying smart processes, technology, etc.

LEADERSHIP CAPABILITY	LEADERSHIP COMPETENCY
Leading Organizations (cont.) ▪ Uses clear vision and strategic alignment of business, human capital, cultural and information system elements to create momentum. ▪ Monitors, evaluates, and manages the organization, oversees performance management, and adjusts elements as needed to maximize organizational effectiveness.	▪ **Organizational Performance Management:** Establishes organizational (or enterprise) performance outcomes and milestones to advance or achieve the organization's mission. Provides constructive feedback and recommendations to improve organizational performance at all levels. ▪ **Organizational Evaluation:** Leverages a systemic process to monitor and assess the performance of an organization and understand the environmental factors that influence it. Directs actions based on assessments to build organizational accountability and efficiency.
Resource Management ▪ Develops, deploys, and oversees the utilization of the department's human capital, financial, and technological resources in an effective manner that appropriately balances mission needs and stewardship.	▪ **Planning, Programming, Budgeting, and Execution (PPBE):** Oversees and executes the Planning, Programming, and Budgeting, and Execution process to achieve the best mix of manpower, material, and support within fiscal constraints. Ensures organization exercises effective stewardship and internal controls for all resources. ▪ **Time Management:** Manages the investment of time required by staff, contractor, and other stakeholders to ensure that work is completed efficiently at an appropriate level of effort. Prioritizes and identifies more critical and less critical activities and adjusts primary concerns appropriately. ▪ **Human Capital Management:** Plans, develops, and manages the workforce based on organizational goals, budget considerations, and staffing needs. Ensures employees are appropriately recruited, selected, appraised, and rewarded; proactively acts to effectively address performance problems, disciplinary issues, and developmental needs. Manages a multi-sector workforce and a variety of work situations. ▪ **Technology Management:** Keeps up to date on technological developments. Makes effective use of appropriate technology to achieve results. Ensures appropriate access to and security of technology systems. Ensures that organizational requirements for systems are documented and updated, as appropriate.

Visit Apply to learn more about the application process or contact our recruiting team with questions.