U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY SERVICE

Version: January 2022

Technical Capabilities Guide

Background

The Department of Homeland Security (DHS) Cybersecurity Service employees work across different cybersecurity specializations. At DHS, we call these specializations technical capabilities. Each technical capability is composed of several underlying technical competencies.

DHS uses technical capabilities to structure DHS Cybersecurity Service careers and match applicants to job opportunities.

Most DHS Cybersecurity Service employees join with a primary technical capability, reflecting the majority of their cybersecurity technical expertise and experience. Those just beginning a career in cybersecurity work with DHS to identify and develop a primary technical capability.

Before You Apply

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.

When DHS recruits for general opportunities by Career Track, you will be asked to select your primary technical capability immediately after applying. Your response will determine the focus of assessments you must then complete to demonstrate your expertise.

In limited circumstances, you may also have a secondary technical capability, which you may also indicate in the application process for both specific opportunities and general opportunities by Career Track.

TECHNICAL CAPABILITY	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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 ▪ Secure Network Design ▪ Secure Software Design ▪ Secure Systems Development ▪ Systems Testing and Evaluation ▪ Regulatory Advisory
Cybersecurity 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 ▪ Data Management ▪ Statistical Modeling ▪ Data Visualization

TECHNICAL CAPABILITY	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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 ▪ Intelligence Analysis 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.
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 ▪ Operations Analysis 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	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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.	▪ Cybersecurity Hardware Engineering ▪ Cybersecurity Systems Engineering ▪ Secure Software/Application Design ▪ Cybersecurity Capability / Solutions Evaluation ▪ Cybersecurity Testing and Evaluation
Cybersecurity Policy **Note:** Always a secondary capability	▪ 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 ▪ Policy Advisement ▪ Cybersecurity Policy Development and Writing ▪ Cybersecurity Governance ▪ Cybersecurity Legislative Affairs
Cybersecurity Program Management **Note:** Always a secondary capability	▪ 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 ▪ Cybersecurity Program Execution ▪ Cybersecurity Investment Management

TECHNICAL CAPABILITY	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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 ▪ Cybersecurity Research Development and Delivery ▪ Cybersecurity Research Testing and Evaluation
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 ▪ Organizational Risk Assessment ▪ Organizational Risk Management ▪ Policy Interpretation

TECHNICAL CAPABILITY	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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 [intelligence], 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.	▪ Warning Analysis ▪ Threat Assessment Intelligence Analysis
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 ▪ Cyber Investigation ▪ Reverse Engineering Malware Analysis
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 ▪ Network Monitoring and Defense ▪ Malware Analysis

TECHNICAL CAPABILITY	DESCRIPTION	UNDERLYING TECHNICAL COMPETENCIES
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 ▪ ICS/SCADA ▪ Internet of Things ▪ Building/Facilities ▪ Automation
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 ▪ Operating Systems ▪ Distributed Systems ▪ Network Management
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 ▪ Systems Implementation Knowledge ▪ Information Systems Security Monitoring Continuity of Security Operations
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 ▪ Penetration Testing

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