Appendix 1 – National Cybersecurity Workforce Framework Communications Sector Recommended KSAs

Knowledge, Skills, Abilities (KSAs)	Applicability
Acknowledges and incorporates the values and interests of supervisors and/or leaders to produce results in-line with organizational vision.	Applicable
Initiates, maintains and facilitates the flow of needed information through organization following chain of command structure	Updated
Requests needed resources in order to meet organizational expectations.	Applicable
Analyzes threat information from multiple sources, disciplines, and Federal/State/Local agencies. Synthesizes and places intelligence information in context draws insights about the possible implications.	Updated
Accurately identifies and analyzes data and problems.	Applicable
Demonstrates the ability to identify and evaluate problems or issues	Applicable
Takes action to monitor and control time and costs	Applicable
Skill in analyzing network traffic capacity and performance characteristics.	Applicable
Adapts effectively to changing priorities/assignments.	Applicable
Effectively plans, prioritizes, and manages multiple projects.	Applicable
Treats change and new situations as opportunities for learning or growth	Applicable
Actively works across function on broad projects to achieve broad objectives.	Applicable
Builds strong partnerships by genuinely seeking out others' opinions and ideas.	Applicable
Can gain the cooperation of others	Applicable
Can support delivery of services or solutions in own capability group	Applicable
Contributes actively in team activities, sharing experience and ideas	Applicable
Draws upon colleagues' expertise to deliver results.	Applicable
Establishes and maintains effective working relationships with others	Applicable
Gains agreements with peers and business partners to support ideas and uses sound rationale to explain the value of actions	Applicable
Listens to customer concerns to identify their core needs.	Applicable
Listens to others and leverages their input to improve service and products.	Applicable
Works co-operatively with other managers to achieve team goals	Applicable
Works effectively with colleagues to accomplish goals and drive change.	Applicable
Executes collection using appropriate strategies within the priorities established through the collection management process.	Applicable
Knowledge of multi-channel user access technologies and use cases including mobile technology.	Applicable
Ability to decrypt digital data collections.	Applicable
Knowledge of anti-forensics tactics, techniques, and procedures (TTPs).	Applicable
Knowledge of common forensic tool configuration and support	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
applications (e.g., VMware, Wireshark).	
Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	Applicable
Knowledge of data carving tools and techniques (e.g., Foremost).	Applicable
Knowledge of deployable forensics.	Applicable
Knowledge of investigative implications of hardware, operating systems, and network technologies.	Applicable
Knowledge of server diagnostic tools and fault identification techniques.	Applicable
Knowledge of types and collection of persistent data.	Applicable
Knowledge of types of digital forensics data and how to recognize them.	Applicable
Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Applicable
Skill in analyzing volatile data.	Applicable
Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Applicable
Skill in developing and executing technical training programs and curricula.	Applicable
Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Applicable
Skill in identifying forensic footprints.	Applicable
Skill in preserving evidence integrity according to standard operating procedures or national standards.	Applicable
Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, Forensic Tool Kit [FTK]).	Applicable
Knowledge of basic concepts and practices of processing digital forensic data	Applicable
Knowledge of machine learning	Applicable
Knowledge of statistical methods	Applicable
Skill In data presentation and visual analytics	Applicable
Skill in experimental design	Applicable
Skill in pattern recognition and anomaly detection	Applicable
Skill in working with structured data	Applicable
Skill in working with unstructured data	Applicable
Knowledge of interpreted and compiled computer languages.	Applicable
Knowledge of low-level computer languages (e.g., assembly languages).	Applicable
Knowledge of programming language structures and logic.	Applicable
Knowledge of secure coding technologies.	Applicable
Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).	Applicable
Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode).	Applicable
Skill in reading Hexadecimal data.	Applicable
Skill in using binary analysis tools (e.g., Hexedit, command code xxd,	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
hexdump).	
Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) in a modern programming language (e.g., Java, C++).	Applicable
Knowledge of application development languages and scripting languages	Applicable
Skill in multiple application development and scripting languages (e.g. Java, C.net, Objective C, SQL, HTML, XML …)	Applicable
Skill in programming or development in at least one of the following languages: .NET (ASP.NET), Java, Perl, Python, Ruby, C/C++/ObjectiveC	Applicable
Skill in writing SQL queries to generate custom reports	Applicable
Skill with application security on multiple technology platforms (e.g. J2SE, Struts/Spring, SQL, SSO, HTML5, etc…)	Applicable
Skill with OSS (Open Source Software), must have extensive experience in Java technology, frameworks and security.	Applicable
Ability to apply supply chain risk management standards.	Applicable
Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations.	Applicable
Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities).	Applicable
Knowledge of common attack vectors on the network layer.	Applicable
Knowledge of content development.	Applicable
Knowledge of cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities.	Applicable
Knowledge of cyber defense policies, procedures, and regulations.	Applicable
Knowledge of defense-in-depth principles and network security architecture.	Applicable
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Applicable
Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]).	Applicable
Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Applicable
Knowledge of intrusion detection methodologies and techniques for detecting host-and network-based intrusions via intrusion detection technologies.	Applicable
Knowledge of Intrusion Detection System (IDS) tools and applications.	Applicable
Knowledge of malware analysis concepts and methodology.	Applicable
Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Applicable
Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
operations, SSL security, REST/JSON processing).	
Knowledge of the types of Intrusion Detection System (IDS) hardware and software.	Applicable
Knowledge of virtual machine aware malware, debugger aware malware, and packing.	Applicable
Skill in analyzing anomalous code as malicious or benign.	Applicable
Skill in collecting data from a variety of cyber defense resources.	Applicable
Skill in deep analysis of captured malicious code (e.g., malware forensics).	Applicable
Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Applicable
Skill in identifying obfuscation techniques.	Applicable
Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (TTP).	Applicable
Skill in mimicking threat behaviors.	Applicable
Skill in protecting a network against malware.	Applicable
Skill in tuning sensors.	Applicable
Skill of identifying capturing, containing, and reporting malware.	Applicable
Knowledge of malware packing and obfuscation techniques	Applicable
Skill in conducting information searches.	Applicable
Skill in the basic operation of computers.	Applicable
Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage).	Applicable
Knowledge of circuit analysis.	Applicable
Knowledge of microprocessors.	Applicable
Skill in physically disassembling personal computers (PCs).	Applicable
Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	Applicable
Knowledge of collection management processes, capabilities, and limitations.	Applicable
Knowledge of secure configuration management techniques.	Applicable
Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers).	Applicable
Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs]).	Applicable
Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware).	Applicable
Knowledge of critical information technology (IT) procurement requirements.	Applicable
Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	Applicable
Knowledge of import/export control regulations and responsible	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
agencies for the purposes of reducing supply chain risk.	
Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	Applicable
Skill in evaluating the trustworthiness of the supplier and/or product.	Applicable
Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	Applicable
Knowledge of electronic evidence law.	Applicable
Knowledge of International Traffic in Arms Regulation (ITARs) and relevance to cybersecurity.	
Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence).	Applicable
Knowledge of legal rules of evidence and court procedure.	Applicable
Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Applicable
Knowledge of relevant laws, policies, procedures, or governance related to work impacting critical infrastructure.	Applicable
Knowledge of online banking and pertinent US regulations	Applicable
Knowledge of cryptography and cryptographic key management concepts.	Applicable
Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	Applicable
Knowledge of encryption methodologies.	Applicable
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.	Applicable
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.	Applicable
Ability to interpret and incorporate data from multiple tool sources.	Applicable
Knowledge of concepts and practices of processing digital forensic data.	Applicable
Knowledge of data administration and data standardization policies and standards.	Applicable
Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of data mining and data warehousing principles.	Applicable
Knowledge of database theory.	Applicable
Knowledge of sources, characteristics, and uses of the organization’s data assets.	Applicable
Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines).	Applicable
Knowledge of the characteristics of physical and virtual data storage media.	Applicable
Skill in data mining techniques.	Applicable
Skill in developing data dictionaries.	Applicable
Skill in developing data repositories.	Applicable
Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Direct Algorithm [MD5]).	Applicable
Skills in data reduction.	Applicable
Knowledge of database structure and queries	Applicable
Skill in Extract Transform Load (ETL) processes	Applicable
Knowledge of advanced data remediation security features in databases.	Applicable
Skill in allocating storage capacity in the design of data management systems.	Applicable
Skill in designing databases.	Applicable
Skill in optimizing database performance.	Applicable
Knowledge of advanced data encryption (e.g., Column and Tablespace Encryption) security features in databases, including built-in cryptographic key management features.	Applicable
Knowledge of database management systems, query languages, table relationships, and views.	Applicable
Knowledge of database systems.	Applicable
Knowledge of Java-based database access application programming interface (API) (e.g., Java Database Connectivity [JDBC]).	Applicable
Knowledge of query languages such as Structured Query Language (SQL).	Applicable
Skill in conducting queries and developing algorithms to analyze data structures.	Applicable
Skill in generating queries and reports.	Applicable
Skill in maintaining databases.	Applicable
Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	Applicable
Knowledge of embedded systems and internet of things.	Applicable
Knowledge of digital rights management.	Applicable
Knowledge of symmetric key rotation techniques and concepts.	Applicable
Knowledge of Virtual Private Network (VPN) security.	Applicable
Skill in using Public-Key Infrastructure (PKI) Software Development Kit (SDK) to add encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Applicable
Skill in using Virtual Private Network (VPN) devices and encryption.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of enterprise messaging systems and associated software.	Applicable
Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Updated
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Applicable
Knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DODAF], Federal Enterprise Architecture Framework [FEAF]).	Applicable
Knowledge of the nature and function of the relevant information structure.	Applicable
Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Applicable
Accepts responsibility for own decisions and actions.	Applicable
Acts with highest level of integrity, generating trust and protecting client interests	Applicable
Adheres to all Bank and FRS policies, bulletins and ethical guidelines.	Not Applicable
Demonstrates a consistency between actions and words.	Applicable
Follows set processes and methods	Applicable
Follows through on commitments	Applicable
Analyzes collected information to identify vulnerabilities and potential for exploitation.	Applicable
Knowledge of external organizations and academic institutions dealing with cybersecurity issues.	Applicable
Knowledge of social dynamics of computer attackers in a global context.	Applicable
Knowledge of Theories of Crime	Applicable
Knowledge of Underground Economy	Applicable
Knowledge of Financial Industry Investment Banking Products and Processing (i.e. Equities, FX, Fixed Assets, Derivatives)	Not Applicable
Knowledge of Financial Industry Payments Systems (i.e. Cash, Credit Cards)	Not Applicable
Knowledge of regulatory bodies and their responsibilities (FCC, FTC, SEC, etc.)	Updated
Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).	Applicable
Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Applicable
Skill in setting up a forensic workstation.	Applicable
Knowledge of Human Factors/Digital Ergonomics	Applicable
Establishes relationships with and learns more about associates from other countries, cultures and backgrounds	Applicable
Keeps current on key economic, social and political trends throughout the world and their potential impact on business	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Applicable
Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]).	Applicable
Knowledge of network hardware devices and functions.	Applicable
Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.	Applicable
Knowledge of human-computer interaction principles.	Applicable
Skill in the use of social engineering techniques.	Applicable
Knowledge of authentication, authorization, and access control methods.	Applicable
Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	Applicable
Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).	Applicable
Knowledge of policy-based and risk-adaptive access controls.	Applicable
Skill in developing and applying security system access controls.	Applicable
Skill in developing and applying user credential management system.	Applicable
Skill in maintaining directory services.	Applicable
Knowledge of database procedures used for documenting and querying reported incidents.	Applicable
Knowledge of disaster recovery and continuity of operations plans.	Applicable
Knowledge of enterprise incident response program, roles, and responsibilities.	Applicable
Knowledge of incident categories, incident responses, and timelines for responses.	Applicable
Knowledge of incident response and handling methodologies.	Applicable
Knowledge of root cause analysis for incidents.	Applicable
Skill in performing root cause analysis for incidents.	Applicable
Skill in recovering failed servers.	Applicable
Skill in using incident handling methodologies.	Applicable
Knowledge of fault tolerance.	Applicable
Knowledge of information assurance (IA) principles and methods that apply to software development.	Applicable
Knowledge of information assurance (IA) principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data.	Applicable
Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Applicable
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of organization's enterprise information security architecture system.	Applicable
Knowledge of parallel and distributed computing concepts.	Applicable
Knowledge of the Security Assessment and Authorization (SA&A) process.	Applicable
Skill in applying confidentiality, integrity, and availability principles.	Applicable
Skill in designing security controls based on information assurance (IA) principles and tenets.	Applicable
Skill in determining how a security system should work, including its resilience and dependability capabilities, and how changes in conditions, operations, or the environment will affect these outcomes.	Applicable
Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	Applicable
Skill in performing damage assessments.	Applicable
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Applicable
Skill in securing network communications.	Applicable
Knowledge of frameworks for authorization and entitlement management (e.x. EPV, SSO, etc)	Applicable
Knowledge of an organization's information classification program and procedures for level information loss.	Applicable
Knowledge of Risk Management Framework (RMF) requirements.	Applicable
Skill in creating policies that reflect system security objectives.	Applicable
* Knowledge of cybersecurity principles.	Applicable
Knowledge of basic system administration, network, and operating system hardening techniques.	Applicable
Knowledge of current and emerging threats/threat vectors.	Applicable
Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities.	Applicable
Knowledge of front-end collection systems, including network traffic collection, filtering, and selection.	Applicable
Knowledge of host and network access control mechanisms (e.g., access control list).	Applicable
Knowledge of information security systems engineering principles.	Applicable
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Applicable
Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Applicable
Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Applicable
Knowledge of network traffic analysis methods.	Applicable
Knowledge of security event correlation tools.	Applicable
Knowledge of security system design tools, methods, and techniques.	Applicable
Knowledge of signature implementation impact.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	Applicable
Knowledge of the Enterprise Network Defense (END) provider reporting structure and processes within one's own organization.	Applicable
Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	Applicable
Skill in developing and deploying signatures.	Applicable
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Applicable
Skill in implementing, maintaining, and improving established security practices.	Applicable
Skill in reading and interpreting signatures (e.g., Snort).	Applicable
Demonstrated capability of designing and implementing global best practices and processes	Applicable
Knowledge of Security Design Patterns for Applications	Applicable
Knowledge of user access methods and privilege activity	Applicable
Skill with security technologies such as Firewalls, IDS/IPS, Web Proxies, DLP, etc.	Applicable
Knowledge of information technology (IT) architectural concepts and frameworks.	Applicable
Knowledge of remote access technology concepts.	Applicable
Knowledge of the enterprise information technology (IT) architecture.	Applicable
Knowledge of security architecture frameworks	Applicable
Skill in application, data, and infrastructure architecture disciplines.	Applicable
Skill in architecture and design across multiple systems	Applicable
Knowledge of measures or indicators of system performance and availability.	Applicable
Knowledge of performance tuning tools and techniques.	Applicable
Skill in conducting audits or reviews of technical systems.	Applicable
Skill in identifying and anticipating server performance, availability, capacity, or configuration problems.	Applicable
Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	Applicable
Skill in monitoring and optimizing server performance.	Applicable
* Knowledge of computer networking concepts and protocols, and network security methodologies.	Applicable
Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results.	Applicable
Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications.	Applicable
Knowledge of communication methods, principles, and concepts (e.g., encoding, signaling, multiplexing) that support the network infrastructure.	Applicable
Knowledge of Extensible Markup Language (XML) schemas.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of how network services and protocols interact to provide network communications.	Applicable
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI]).	Applicable
Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management.	Applicable
Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Applicable
Knowledge of network design processes, including security objectives, operational objectives, and tradeoffs.	Applicable
Knowledge of network protocols (e.g., Transmission Critical Protocol/Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]), and directory services (e.g., Domain Name System [DNS]).	Applicable
Knowledge of networking protocols.	Applicable
Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways.	Applicable
Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., tables, PC, Cloud, etc.).	Applicable
Skill in deploying Service Gateway at the network edge as the first point of contact or proxy into enterprise infrastructure handling layer 7 protocols (e.g., web, XML SOAP, REST, or legacy protocols [EDI]).	Applicable
Skill in establishing a routing schema.	Applicable
Skill in implementing enterprise key escrow systems to support data-at-rest encryption.	Applicable
Skill in installing, configuring, and troubleshooting local area network (LAN) and wide area network (WAN).	Applicable
Skill in network mapping and recreating network topologies.	Applicable
Skill in using sub-netting tools.	Applicable
Knowledge of Telephony	Updated
Identifies the possibility of new deals, extensions and ad-hoc service aspects	Applicable
Integrates information from a variety of sources, detects trends, associations and cause-effect relationships to drive actions	Applicable
Proposes innovations	Applicable
Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels.	Applicable
Ability to match the appropriate knowledge repository technology for a given application or environment.	Applicable
Knowledge of knowledge-base capabilities for identifying the solutions to less common and more complex system problems.	Applicable
Skill in conducting knowledge mapping (e.g., map of knowledge repositories).	Applicable
Skill in conducting open source research for troubleshooting novel client-level problems (e.g., online development communities, system security blogging sites).	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Skill in the measuring and reporting of intellectual capital.	Applicable
Skill in using knowledge management technologies.	Applicable
* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Applicable
Ability to determine impact of technology trend data on laws, regulations, and/or policies.	Applicable
Knowledge of Import/Export Regulations related to cryptography and other security technologies.	Applicable
Skill in tracking and analyzing technical and legal trends that will impact cyber activities.	Applicable
Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Applicable
Knowledge of process engineering concepts.	Applicable
Knowledge of structured analysis principles and methods.	Applicable
Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Applicable
Knowledge of computer algorithms.	Applicable
Knowledge of information theory, including source coding, channel coding, algorithm complexity theory, and data compression.	Applicable
Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	Applicable
Skill in creating and utilizing mathematical or statistical models.	Applicable
Skill in design modeling and building use cases (e.g., unified modeling language).	Applicable
Skill in developing data models.	Applicable
Knowledge and experience in the Instructional System Design (ISD) methodology.	Applicable
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Applicable
Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, v3 [ITIL]).	Applicable
Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, Voice over Internet Protocol [VoIP], Instant Messenger [IM], web forums, direct video broadcasts).	Applicable
Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fidelity [WI-FI]).	Applicable
Knowledge of Wireless Fidelity (WI-FI).	Remove - redundant
Skill in applying host/network access controls (e.g., access control list).	Applicable
Skill in conducting server planning, management, and maintenance.	Applicable
Skill in correcting physical and technical problems that impact server performance.	Applicable
Skill in diagnosing connectivity problems.	Applicable
Skill in diagnosing failed servers.	Applicable
Skill in testing and configuring network workstations and peripherals.	Applicable
Skill in using network management tools to analyze network traffic	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
patterns (e.g., simple network management protocol).	
Knowledge of complex data structures.	Applicable
Knowledge of computer programming principles such as object-oriented design.	Applicable
Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Applicable
Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Applicable
Knowledge of how to troubleshoot basic systems and identify operating systems-related issues.	Applicable
Knowledge of operating systems.	Applicable
Knowledge of server and client operating systems.	Applicable
Knowledge of systems administration concepts.	Applicable
Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications).	Applicable
Knowledge of virtualization technologies and virtual machine development and maintenance.	Applicable
Knowledge of Windows and Unix ports and services.	Applicable
Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat).	Applicable
Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Applicable
Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [VBS]) on Windows and Unix systems (e.g., tasks such as parsing large data files, automating manual tasks, fetching/processing remote data).	Applicable
Skill in system administration for Unix/Linux operating systems.	Applicable
Skill in using virtual machines.	Applicable
Skill in utilizing virtual networks for testing.	Applicable
Knowledge of Android command line tools (e.g. adb).	Applicable
Knowledge of Authentication methods	Applicable
Knowledge of LINUX Boot Process	Applicable
Knowledge of Mac command line	Applicable
Knowledge of malware persistence methods	Applicable
Knowledge of operating systems (e.g., Windows, Unix/Linux, iOS, Android, etc)	Applicable
Knowledge of operating systems (ex. Windows, Unix/Linux, Mac OS, iOS, Android, etc.) boot process including a through understanding of the execution flow of boot time processes	Updated
Knowledge of Root-Kit design, techniques, and hiding strategies	Applicable
Knowledge of Solaris Boot Process	Applicable
Knowledge of the Android operating system	Applicable
Knowledge of the Apple iOS operating system	Applicable
Knowledge of Windows Boot Process	Applicable
Knowledge of windows process injection techniques	Applicable
Skill in identifying, modifying, and manipulating applicable system components (iOS or Android) (e.g., passwords, user accounts, files)	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Skill in identifying, modifying, and manipulating applicable system components (Windows, Unix/Linux, Mac OS/OS X, iOS and/or Android)	Updated
Knowledge of service catalogues and service management standards (e.g., Information Technology Infrastructure Library, v3 [ITIL]).	Applicable
Skill in talking to others to convey information effectively.	Applicable
Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportable criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	Applicable
Knowledge of the organization's core business/mission processes.	Applicable
Knowledge of the structure and intent of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.	Applicable
Knowledge of Privacy Impact Assessments (PIA).	Applicable
Skill in deconflicting cyber operations and activities.	Applicable
Arrives at sound conclusions and recommendations based on business goals data, and practical constraints.	Applicable
Considers alternatives, implements decisions, and evaluates their effectiveness.	Applicable
Demonstrates urgency and timeliness when dealing with critical issues or people.	Applicable
Identifies efficiency improvements	Applicable
Identifies problems and appreciates the issues required to resolve them	Applicable
Organizes resources effectively to meet demands of projects.	Applicable
Resolves issues quickly and effectively, in a way that mitigates repeat inquiries.	Applicable
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services and CMMI for Acquisitions).	Applicable
Actively identifies new areas for learning and regularly created and takes advantage of learning opportunities	Applicable
Acts courteously and professionally when dealing with customers.	Applicable
Consistently meets expected results within deadlines	Applicable
Follows-up to ensure satisfactory service and complete problem resolution.	Applicable
Gets all things done on a timely basis	Applicable
Is courteous and helpful when responding to requests, even if urgent or unplanned.	Applicable
Maintains composure during pressured/stressful situations.	Applicable
Maintains records as required for the project or service	Applicable
Places a priority on attending to the needs and inquiries from internal and external customers.	Applicable
Remains self-disciplined and prevent irrelevant issues or distractions from interfering with the timely completion of important tasks	Applicable
Takes action that goes beyond job requirements in order to achieve objectives	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Tracks and directs own workflow efficiently.	Applicable
Uses time and energy optimally to ensure delivery of all products and services.	Applicable
Knowledge of information security program management and project management principles and techniques.	Applicable
Knowledge of resource management principles and techniques.	Applicable
Knowledge of operations security.	Applicable
Skill in integrating black box security testing tools into quality assurance process of software releases.	Applicable
Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence.	Applicable
Skill in analyzing memory dumps to extract information.	Applicable
Skill in using scientific rules and methods to solve problems.	Applicable
Knowledge of Electronic Monetary Transaction Processes	Applicable
Ability to apply network programming towards client/server model.	Applicable
Ability to interpret and translate customer requirements into operational cyber actions.	Applicable
Knowledge of applicable business processes and operations of customer organizations.	Applicable
Knowledge of capabilities and requirements analysis.	Applicable
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Applicable
Skill in conducting capabilities and requirements analysis.	Applicable
Business process improvement mindset with a drive for controls, automation and efficiency	Applicable
* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Applicable
Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Applicable
Knowledge of organization's risk tolerance and/or risk management approach.	Applicable
Knowledge of risk threat assessment.	Applicable
Knowledge of supply chain risk management standards, processes, and practices.	Applicable
Knowledge of threat assessment.	Applicable
Skill in building and running working groups to draft Policies and Standards, facilitate and capture feedback and negotiate mutually acceptable results.	Applicable
Skill in Policy & Standards writing (e.g. articulating regulatory/authoritative source and risk based requirements in non-subjective, unambiguous and succinct language.	Applicable
Risk management Governance (I.e. 3 layers of defense, CRO office, RCSA process)	Applicable
Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards.	Applicable
Knowledge of processes for reporting network security related	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
incidents.	
Knowledge of debugging procedures and tools.	Applicable
Knowledge of middleware (e.g., enterprise service bus and message queuing).	Applicable
Knowledge of software debugging principles.	Applicable
Knowledge of software design tools, methods, and techniques.	Applicable
Skill in conducting software debugging.	Applicable
Skill in developing applications that can log errors, exceptions, and application faults.	Applicable
Skill in using code analysis tools to eradicate bugs.	Applicable
Skill in writing kernel level applications.	Applicable
Knowledge of mobile application packaging procedures (e.g. package signatures)	Applicable
Knowledge of debugging procedures and tools	Applicable
Skill in the development and deployment of mobile applications.	Applicable
Knowledge of secure software deployment methodologies, tools, and practices.	Applicable
Knowledge of software development models (e.g., Waterfall Model, Spiral Model, Agile Model).	Applicable
Knowledge of software engineering.	Applicable
Knowledge of software quality assurance process.	Applicable
Skill in configuring and optimizing software.	Applicable
Ability to tailor code analysis for application-specific concerns.	Applicable
Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams.	Applicable
Communicates appropriately with people at various levels and backgrounds, even if they have differing viewpoints.	Applicable
Conveys information that is well organized and analytically sound.	Applicable
Demonstrates an understanding of culturally appropriate communication styles.	Applicable
Recognizes the need for additional information and asks questions to obtain it	Applicable
Tailors communication style for diverse audiences.	Applicable
Utilizes civil discourse techniques to effectively navigate conflict.	Updated
Appropriately delegates and monitors progress of assignments to staff.	Applicable
Contributes to recruitment activities	Applicable
Effectively enhances the development and ongoing performance of subordinates	Applicable
Ensures staff understands expectations and time-lines for assignments.	Applicable
Establishes good interpersonal relationships by helping people feel valued, appreciated , and included in discussions	Applicable
Exhibits strong management skills that are at least commensurate with the role	Updated
Is able to set tasks and direction for the team	Applicable
Is able to work through project plans to completion without continuous oversight or supervision.	Applicable
Maintains oversight and responsibility for staff’s projects.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Provides constructive and timely feedback and coaching to staff.	Applicable
Works within the SLA or project plan	Applicable
Knowledge of hacking methodologies in Windows or Unix/Linux environment.	Applicable
Knowledge of how system components are installed, integrated, and optimized.	Applicable
Knowledge of principles and methods for integrating server components.	Applicable
Knowledge of technology integration processes.	Applicable
Skill in designing the integration of hardware and software solutions.	Applicable
Knowledge of server administration and systems engineering theories, concepts, and methods.	Applicable
Knowledge of system life cycle management principles, including software security and usability.	Applicable
Knowledge of the life cycle process.	Applicable
Knowledge of the operations and processes for diagnosing common or recurring system problems.	Applicable
Knowledge of the systems engineering process.	Applicable
Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly.	Applicable
Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	Applicable
Skill in installing computer and server upgrades.	Applicable
Knowledge of agency evaluation and validation requirements.	Applicable
Knowledge of organization's evaluation and validation requirements.	Applicable
Knowledge of system diagnostic tools and fault identification techniques.	Applicable
Knowledge of systems testing and evaluation methods.	Applicable
Skill in applying organization-specific systems analysis principles and techniques.	Applicable
Skill in conducting test events.	Applicable
Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data).	Applicable
Skill in determining an appropriate level of test rigor for a given system.	Applicable
Skill in developing operations-based testing scenarios.	Applicable
Skill in evaluating test plans for applicability and completeness.	Applicable
Skill in secure test plan design (i.e., unit, integration, system, acceptance).	Applicable
Skill in systems integration testing.	Applicable
Skill in writing test plans.	Applicable
Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	Applicable
Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.	Applicable
Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
to systems security policies and procedures.	
Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.	Applicable
Skill in identifying gaps in technical capabilities.	Applicable
Ability to determine the validity of technology trend data.	Applicable
Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	Applicable
Knowledge of emerging security issues, risks, and vulnerabilities.	Applicable
Knowledge of key industry indicators that are useful for identifying technology trends.	Applicable
Knowledge of new and emerging Information Technology (IT) and cyber security technologies.	Applicable
Knowledge of new technological developments in server administration.	Applicable
Knowledge of products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities.	Applicable
Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs).	Applicable
Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).	Applicable
Skill in applying and incorporating information technologies into proposed solutions.	Applicable
Awareness and use of technology relevant to role and service provided	Applicable
Awareness of at least one vendor solution or security tool relevant to services or solutions in own capability group	Applicable
Awareness of other vendor solutions or tools	Applicable
Awareness of services and solutions in own capability group	Applicable
Can articulate at least one vendor solution or tool relevant to services or solutions in own capability group	Applicable
Competent in the use of own technology area for client and Company benefit	Applicable
Demonstrates an interest in associated technologies	Applicable
Has completed training on at least one vendor solution or tool relevant to services or solutions in own capability group	Applicable
Is aware of company and own area business plans	Applicable
Understands one method associated with services or solutions in own capability group	Not applicable
Knowledge of basic concepts, terminology, and operations of a wide range of communications media (e.g., computer and telephone networks, satellite, fiber, wireless).	Applicable
Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN]).	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Knowledge of Global Systems for Mobile communications (GSM) architecture.	Applicable
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	Applicable
Knowledge of key telecommunication concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	Applicable
Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII]).	Applicable
Knowledge of Voice over Internet Protocol (VoIP).	Applicable
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.	Applicable
Able to communicate a point demonstrating logic, reasoning, and soundness of argument.	Applicable
Demonstrates culturally-inclusive communication.	Applicable
Demonstrates effective active listening skills (paraphrasing, clarifying, perception checking, summarizing).	Applicable
Utilizes non-verbal techniques appropriate to the context of communication.	Applicable
* Knowledge of cyber threats and vulnerabilities.	Applicable
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Applicable
Knowledge of application vulnerabilities.	Applicable
Knowledge of hardware reverse engineering techniques.	Applicable
Knowledge of how different file types can be used for anomalous behavior.	Applicable
Knowledge of packet-level analysis.	Applicable
Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit).	Applicable
Knowledge of reverse engineering concepts.	Applicable
Knowledge of software reverse engineering techniques.	Applicable
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Applicable
Knowledge of system and application security threats and vulnerabilities.	Applicable
Skill in assessing the robustness of security systems and designs.	Applicable
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Applicable
Skill in designing countermeasures to identified security risks.	Applicable
Skill in evaluating the adequacy of security designs.	Applicable
Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Applicable
Skill in the use of penetration testing tools and techniques.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
Skill in using network analysis tools to identify vulnerabilities.	Applicable
Skill in using protocol analyzers.	Applicable
Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (e.g., penetration and testing).	Applicable
Skill in utilizing network analysis tools to identify software communications vulnerabilities.	Applicable
Knowledge of hacking methodologies in Windows or Unix/Linux environment	Applicable
Knowledge of OWASP Security Remediation Framework Projects (ESAPI, AntiSamy, CSRFGuard)	Applicable
Knowledge of OWASP Top 10 and other web and mobile application security taxonomy	Applicable
Skill in CVSS, CVE and related schema and scoring.	Applicable
Skill in establishing and optimizing service models, defining and measuring to SLA/KPIs.	Updated
Skill in implementation programs for supply chain security, vBSIMM and Binary code scanning.	Applicable
Skill in interpreting log output from networking devices, operating systems and infrastructure services	Applicable
Skill in remediation of application vulnerabilities (e.g. OWASP Top 10 application security risks)	Applicable
Skill in reviewing raw log files, data correlation, and analysis (i.e. firewall, network flow, IDS, system logs)	Applicable
Skill in security testing program management and development	Applicable
Skill in the use of penetration testing tools and techniques in regards to Mobile application assessments	Applicable
Skill in Threat Modeling methodologies and approaches such as STRIDE, Attack Trees…	Applicable
Skill in using static code analysis tools principles and practices (i.e. HP Fortify, IBM Appscan Resource, Pylint, RATS, Veracode, The Black Duck Suite).	Applicable
Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	Applicable
Knowledge of web filtering technologies.	Applicable
Knowledge of web services, including service oriented architecture, Simple Object Access Protocol (SOAP), and web service description language.	Applicable
Knowledge of webmail collection, searching/analyzing techniques, tools, and cookies.	Applicable
Adapts writing style and content to fit mode of messaging (sales, email, supervision, or short/long form reporting).	Applicable
Demonstrates a mastery of language structure and syntax through formal and informal writing.	Applicable
Utilizes a strong vocabulary for precise description.	Applicable

Knowledge, Skills, Abilities (KSAs)	**Applicability**
New Communications specific KSAs submitted from Working Group	
Knowledge of cyber incident information sharing protocols such as STIX, TAXII and CybOX	Applicable
General understanding of technology trends and emerging standards in the Cyber Security domain	Applicable
Understands unique Workforce Development for Cyber security professionals	Applicable
Knowledge of various network architectures including near field communications, DAS, LTE, etc.	Applicable
Knowledge of impact to network architectures and management techniques as a result of NFV, SDN, and CDN	Applicable
Skill in installing, configuring and trouble shooting Telco network core components (ENodeB, Gateways, Session Border Controllers, HSS, etc.)	Applicable
Knowledge of NFV, CDN, virtual machines, SDN, and other emerging technologies and their impact to architecture and design	Applicable
Knowledge of legal constraints associated with collection of PII and CPNI data and the release of that data	Applicable
Skill with OSS (Open Source Software), must have extensive experience in understanding OSS agreements and implications of usage	Applicable
Skill with OSS (Open Source Software), must have extensive experience in working with OSS license management tools such as Black Duck software	Applicable
Knowledge of telecommunications specific networking protocols, platforms (e.g., SS7, UMTS, LTE, EPC, eNodeB, etc.) and services (e.g., HLR, HSS, PCRF, etc.) and how they interact to provide network communications.	Applicable
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Signaling System 7, MPLS, LTE, UMTS, etc.) subject to the network type and protocol.	Applicable
Knowledge of the structure and intent of business operation plans, concept operation plans, orders, and policies.	Applicable