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

Appendix 2 – National Cybersecurity Workforce Framework Communications Sector Recommended Categories, Specialties and Competencies

Category	Specialty	Competency
Cybersecurity - Securely Provision	Secure Acquisition	Capacity Management
Cybersecurity - Operate and Maintain	Secure Software Engineering	Communications Security Management
Cybersecurity - Protect and Defend	Systems Security Architecture	Computer Forensics
Cybersecurity - Investigate	Technology Research and Development	Computer Languages
Cybersecurity - Oversee and Govern	Systems Requirements Planning	Computer Network Defense
Cybersecurity - Collect and Operate	Test and Evaluation	Computer Skills
Cybersecurity - Analyze	Systems Development	Computers and Electronics
Essential Skills	Data Administration	Configuration Management
	Customer Service and Technical Support	Contracting/Procurement
	Network Services	Criminal Law
	System Administration	Cryptography
	Systems Security Analysis	Data Management
	Enterprise Network Defense Analysis	Database Administration
	Incident Response	Database Management Systems
	Enterprise Network Defense Infrastructure Support	Distributed Systems
	Vulnerability Assessment and Management	Embedded Computers
	Digital Forensics	Encryption
	Cyber Investigation	Enterprise Architecture
	Legal Advice and Advocacy	External Awareness

Category	Specialty	Competency
	Strategic Planning and Policy Development	Forensics
	Training, Education, and Awareness	Hardware
	Information Systems Security Operations	Hardware Engineering
	Security Program Management	Human Factors
	Risk Management	Identity Management
	Knowledge Management	Incident Management
	Public Safety	Information Assurance
	EMS	Information Management
	Radio Systems	Information Systems Security Certification
	RF Engineering	Information Systems/Network Security
		Information Technology Architecture
		Information Technology Performance Assessment
		Infrastructure Design
		Internal Controls
		Knowledge Management
		Legal, Government, and Jurisprudence
		Logical Systems Design
		Mathematical Reasoning
		Modeling and Simulation
		Multimedia Technologies
		Network Management
		Object Technology
		Operating Systems
		Operations Support
		Oral Communication
		Organizational Awareness
		Personnel Safety and Security

Category	Specialty	Competency
		Political Savvy
		Process Control
		Project Management
		Public Safety and Security
		Quality Assurance
		Reasoning
		Requirements Analysis
		Risk Management
		Security
		Software Development
		Software Engineering
		Software Testing and Evaluation
		Surveillance
		Systems Integration
		Systems Life Cycle
		Systems Testing and Evaluation
		Teaching Others
		Technology Awareness
		Telecommunications
		Vulnerabilities Assessment
		Web Technology
		Collection Operations
		Cyber Operations
		Cyber Operations Planning
		All Source Intelligence
		Exploitation Analysis
		Targets
		Threat Analysis

Category	Specialty	Competency
		Advocacy
		Analytics
		Change Management
		Coalition-Building
		Ethical Decision-Making
		Financial Industry Awareness
		Global Awareness
		Innovation and Creativity
		Problem-Solving
		Professionalism
		Software Development / Engineering
		Strategic Communication
		Supervision
		Verbal Communication
		Written Communication
		Geospatial Information Systems
		- Technician/Cartographer
		- Administrator
		Public Information Relations
		Training Coordinator
		Radio Systems Operation/Technician
		Public Safety Dispatcher/Call Taker
		Senior Technical Coordinator (Public Safety)
		Technical Support Specialist
		Privacy (Statutes/Advocacy)
		Others:
		RF Engineering

cybersecurity education

APPLICATION OF PEDAGOGICAL FUNDAMENTALS FOR THE HOLISTIC DEVELOPMENT OF CYBERSECURITY PROFESSIONALS

Barbara E. Endicott-Popovsky
and Viatcheslav M. Popovsky

Nowhere is the problem of lack of human capital more keenly felt than in the field of cybersecurity where the numbers and quality of well-trained graduates are woefully lacking [10]. In 2005, the National Academy of Sciences indicted the US education system as the culprit contributing to deficiencies in our technical workforce, sounding the alarm that we are at risk of losing our competitive edge [14]. While the government has made cybersecurity education a national priority, seeking to stimulate university and community college production of information assurance (IA) expertise, they still have thousands of IA jobs going unfilled. The big question for the last decade [17] has been 'where will we find the talent we need?' In this article, we describe one university's approach to begin addressing this problem and discuss an innovative curricular model that holistically develops future cybersecurity professionals.

CYBERSECURITY EDUCATION: HOW IT STARTED

Both the National Security Agency (NSA) and the Department of Homeland Security (DHS) have launched programs to increase production of cybersecurity experts. In the late 1990s the National IA Education and Training Program (NIETP) was formed to manage Information Assurance (IA) education and training at the Federal level. NIETP supports the Committee on National Security Systems (CNSS) in the executive branch, which, among other duties, sets national-level IA training standards. NIETP has a number of active programs, among which are:

- **Centers of Academic Excellence in IA Education program (CAE/IAE)** Jointly sponsored by the NSA and DHS, this program promotes university and community college involvement in IA education and research by designating Centers of Academic Excellence that meet certain criteria [15]. Currently, there are 166 CAEs in 42 states, the District of Columbia and the Commonwealth of Puerto Rico.
- **Colloquium for Information Systems Security Education (CISSE)** Formed in 1997, CISSE provides a forum for IA leaders in government, industry and academia to define requirements for IA education and to encourage expansion of IA curriculum at institutions of higher learning.
- **National Information Assurance Training and Education Center (NIATEC)** NIATEC is a consortium of academic, industry and government organizations that detail training standards and maintain a library of IA curriculum materials that map to those standards. Under the leadership of Idaho State University's Dr. Corey Schou, one of the founders of NIETP, NIATEC maintains ties to ISC2, considered the global not-for-profit leader in 'gold standard' IA certifications.

NIETP provides a foundation to dramatically increase the population of prepared cybersecurity experts; however, to date, the production has fallen short of filling the tens of thousands of jobs that are going vacant [3,8]. The need has burgeoned in recent years.

cybersecurity education

Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

INCENTIVE PROGRAMS: ENCOURAGING IA STUDENTS

To encourage students to pursue IA government careers, in 2000, the White House issued the Federal Cyber Services (FCS) training and education initiative. This initiative included the very successful *Cybercorps: Scholarship for Service* (SFS) program that authorizes funding of up to 300 undergrad and graduate students each year through programs awarded by the National Science Foundation (NSF) to a subset of competing CAE/IAE's [26]. Each scholarship recipient signs a contract to work for the government upon graduation—one year for every year of scholarship received. The Department of Defense (DoD) offers a similar program, the Information Assurance Scholarship Program (IASP), designed to attract students into DoD IA careers. Awardees sign agreements to work for DoD agencies upon graduation. IASP funds approximately 200 students at any one time [4].

While incredible incentives, doing the math, these programs combined do not begin to reach the employee numbers government needs, even if the SFS program had been funded for a full complement of 300 students each year—and it has not. Add the needs of industry, and conditions translate into a war for talent [14].

Not only are the numbers insufficient, but, given the evolution of the threat spectrum over the last decade from young people seeking street cred to determined cybercriminals and nation states, the depth of knowledge of current graduates is being questioned by the government agencies and industries hiring them. It is not unusual to hear comments at conferences from government officials and industry leaders like 'we are creating a lot of frequent flyers, but not many pilots,' or we are unhappy with the 'check-list security people' produced by academia—implying that a one-size-fits-all, recipe approach to curriculum dominates these programs. Besides more numbers, we need IA graduates with problem-solving skills and out-of-the-box thinking abilities that many employers aren't seeing.

The Pedagogical Question

While NSA and DHS policies have been successful in 1) generating IA curriculum standards through robust dialogue among industry, government and academia and 2) encouraging universities and community colleges to teach IA curriculum that maps to these standards, producing greater numbers of IA graduates than we would have otherwise. We also need a pedagogical methodology and approach that will generate the creative problem solvers we want. The question is not just 'where do we find them,' but also 'how do we efficiently produce creative, problem-solving IA graduates with the requisite skills and expertise our employers require?' It has become a quality concern.

Over the last decade, this question has intrigued us. At the University of Washington's (UW) Center for Information Assurance and Cybersecurity (CIAC), we have developed conceptual and operational pedagogical models that help us begin to tackle the question of how to produce problem-solving IA experts in the short amount of time we have them as students. This is still an evolving work as we continue to elaborate our approach and share our insights. We are hopeful that our models and examples may be useful to other institutions addressing the same question. We would welcome a dialogue with others who wish to share their perspectives, as well.

The CAE/IAE as a Pedagogical System

From the beginning, we conceived of the CIAC as a pedagogical system designed to produce IA professionals from incoming students—at the meta level, we viewed them as raw material to be processed! A unique blending of Russian and American pedagogical approaches [12,20,27] resulted in the authors creating the KBP (Kuzmina-Bespalko-Popovsky) Pedagogical model (Figure 1)[1] that represents the CIAC pedagogical system taking in raw student talent and producing IA expertise as outcomes. This model was first introduced by the authors in 2008 [18] and is considered a high-level metasystem model that, when applied to developing a specific course, produces a specific instantiation of the model referred to as an Information Assurance Curriculum (IAC) system model, several of which have been outlined in previous publications [5, 6, 7].

[1] This operational pedagogical system is derived from intensive research into two schools of thought regarding the theory of pedagogical systems whose originators are Dr. N.V. Kuzmina and Dr. V.P. Bespalko, respectively. In acknowledgement of the body of work of these two distinguished academics, whose main models we have integrated and modified, we called our model Kuzmina-Bespalko-Popovsky (KBP).

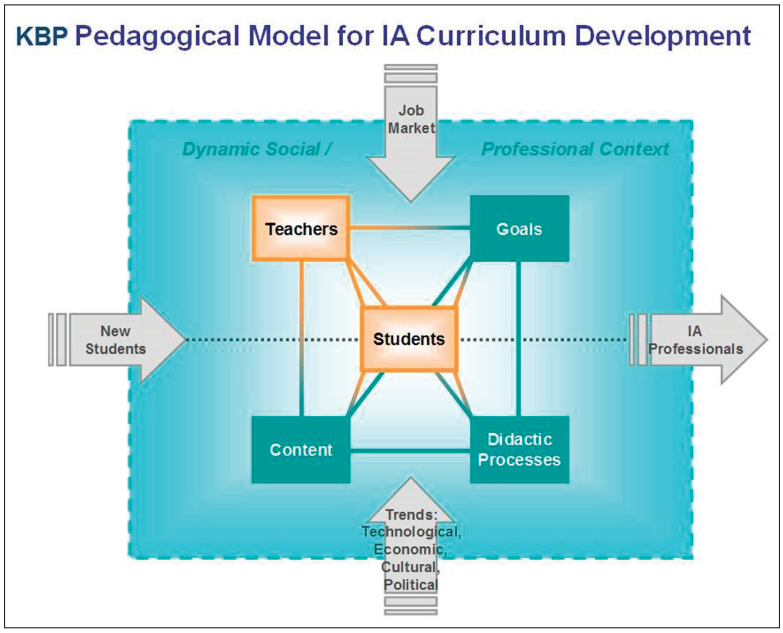


Figure 1: The KBP Pedagogical Model: CIAC as a pedagogical system

The KBP is composed of five model elements—*students, teachers, goals, content* and *didactic processes*—the first two of which are intelligent elements, the *teacher* and the *student*; the remaining three are infrastructure elements—the *goals*, *content*, and *didactic processes* of the curriculum. All elements of the model are dynamic, subject to varying rates of change and adaptation. All of the elements of the model function as an interconnected whole. They operate within a larger dynamic professional and social context that includes economic and political environments, as well as a constantly evolving set of threats, vulnerabilities and operational systems that are affected by influences such as global competition; technological innovation; legal policies; and the creativity of business leaders, entrepreneurs and IA specialists. This context informs the different elements of the model.

In any given context, a specific instructor with his/her own specific slice of IA knowledge and expertise is responsible for developing a specific set of infrastructure components designed to address the needs of a specific type of student.

Students are central to the model—entering the system as potential IA employees; exiting as IA professionals.

By describing each component of the model in relation to learning objectives drawn from the environment and an integration of trends and the condition of the job market, an educational plan is developed iteratively. According to Bespalko and Kuzmina, the more precisely the five components are characterized—along with the connections among them—the more repeatable and predictable the learning results [1,12].

The five elements interact and are changing constantly. Over time, as each of the elements is changed, it affects the other four, requiring each of them to be redefined, and so on, until all five elements are specified in relation to one another. By continuously updating descriptions of these elements, curriculum is kept current ensuring that students remain competitive. We have our curriculum on an annual review cycle, using the model to help us think through curricular changes.

To help envision this process, each of the five elements is elaborated in a later section in relation to one IAC, but first we review the guiding principles that have infused the curriculum development process we use.

Guiding Principles

When we apply the KBP model to developing courses, we operate under the guidance of five key principles that are considered every step of course development.

Guiding Principle 1:
System Activity-based Approach to Learning

According to Michailova [13] and Talizina [24], system activity-based learning is a holistic process that combines learning and productive activities directed toward developing professional abilities and motivation. In this approach, knowledge is not a goal in and of itself, but a remedy for solving practical problems [13,19,21, 24]. The outcome is professional and personal maturity, creativity, the ability to organize one's continuing education as a professional, and student contributions to the community, industry and academia. The center has adopted the system activity-based approach to learning as fundamental to the professional preparation of our students. This approach is characterized by the following five elements:

a) Learning through productive activities

Activities are developed in partnership with an active Northwest cybersecurity community. This includes real world projects and capstones as student assignments. Students present their work to a professional audience and receive honest feedback. *All* participants in these activities—government and industry leaders, university instructors and students, and cybersecurity experts—engage in the learning process, promoting learning from one another.

b) Motivating students to learn on their own

We expect students to become lifelong learners, taking responsibility for their own professional development beyond the classroom, if they wish careers in IA. It is characteristic of a professional that they stay current in their field. This is especially true for the fast moving field of IA where those who succeed develop their own methods of staying current: creating a regimen of daily readings, becoming active in professional organizations, consciously building a network of collaborators that they can draw on. Students are advised to do the same.

Motivating students to learn on their own plays out in the curriculum in assignments that encourage students to

- Develop their own dashboard of RSS-fed, security readings from the internet
- Attend local workshops and conferences held by the regional cybersecurity community that is active and large.

Throughout the course, we tell students that we expect them to become lifelong learners.

c) Knowledge is only a tool, not an end

Gaining knowledge is not the end goal (i.e., learning for a grade), but is a tool to solve practical, complex problems, creatively and independently, unleashing the learner's potential. While we test students to establish a measure of knowledge acquisition, the bigger emphasis is on creative application of what they know to solving unstructured real world problems.

d) Personal and professional development as outcome

Personal and professional development is the end goal. We expect students to exhibit creativity and professionalism in their work and be highly motivated to learn continuously and independently. In many cases, this requires students to transform from being a consumer of whatever the professor provides, to taking an active role in their own personal development. Tools to enable personal growth become part of the curriculum like learning to reflect on their own and others' practical experience to extrapolate generalizations through inductive reasoning.

Character and ethics are discussed in relation to personal and professional growth as students assume responsibility for maintaining currency as an obligation to clients and employers to provide the best possible and most current solutions to their IA problems.

cybersecurity education

Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

e) Real measures of actual production

Criteria for measuring the efficiency of this educational approach are the actual contributions to science and industry made because of cooperative activities. Students are expected to write papers worthy of publication (undergraduates as well as graduates), compose meaningful reports to 'clients,' solve industry problems and effectively present results to business leaders.

This system activity-based approach is adaptive in nature. The five fundamentals mentioned above are a foundation of the educational work of the Center, allowing students to stay current and teachers to move rapidly to adjust curriculum to new learning objectives as the dynamic environment in which we are working changes.

Guiding Principle 2: Mini-max 'brick' Approach to Curriculum

From the beginning, we recognized that there wasn't sufficient time to teach everything that students need to know about IA, nor would that even be feasible. The body of knowledge is forming, expanding, and is not universally agreed upon. It covers a large number of disciplines; students will likely specialize. We know no one who would claim to know everything in IA, and would be suspect of anyone who said they did. The challenge we faced in developing curriculum was to teach enough knowledge on the subject in order for the student to take it from there and succeed on their own professionally.

The solution requires judicious selection of topics from a much larger body of knowledge and decisions about how much time out of the quarter to devote to each topic. Further, in order to ensure students are dedicated enough to assume the initiative to continue to learn on their own, we need to select interesting topics and assignments that we know will engage them. Digital forensics, for example, with all of the attention CSI receives in popular television programs, is a topic that intrigues students. Exercises in identity theft—such as dumpster diving, war walking and google-hacking—also engage student interest, getting them excited about the subject.

Applying the Mini-Max model for teaching IA (Figure 2), we identify the content topics in IA we wish to cover for a particular course, in relation to the other four elements of the pedagogical model, and then identify where those topics fall in the continuum described in Figure 3 (Levels of Learning). The 'brick' (colored block) represents the totality of the IA body of knowledge (BOK); the slice through the 'brick' represents that minimal part of the BOK that must, in our judgment, be taught in the course. Some topics deserve only a mention—in other words, a well-educated IA professional would at least recognize the term or concept. Others are more important to emphasize and are candidates for productive, as opposed to reproductive, learning, that is, lab experiments, participation in research, problem solving in a real-world environment.

Later, we will walk you through the model presented in Figure 3 to show how it is applied in a curriculum development example.

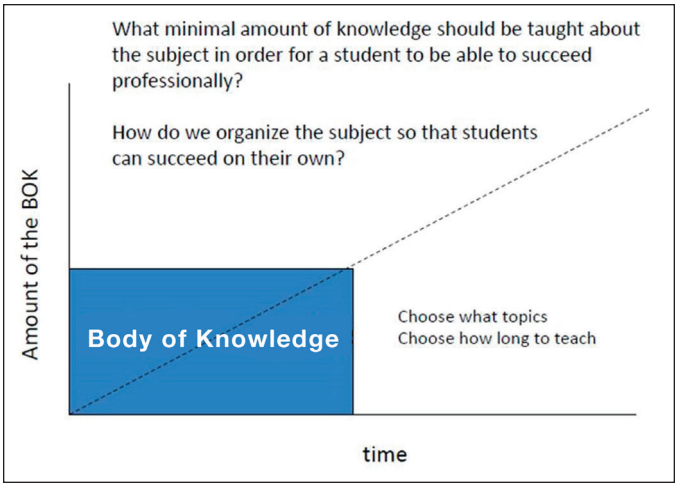


Figure 2: Mini-Max Model for Teaching a Subject

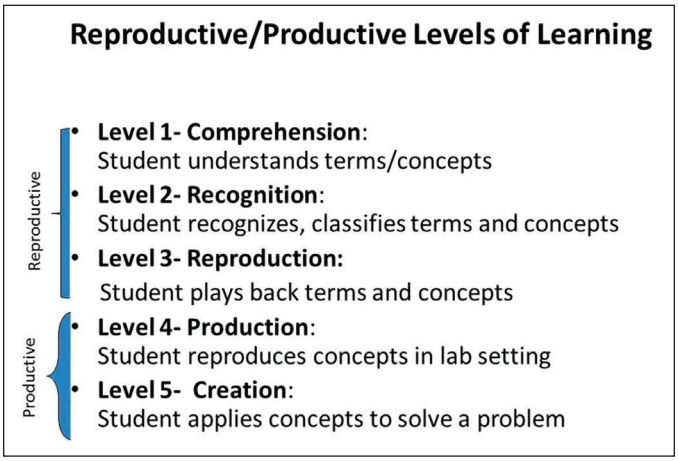


Figure 3: Levels of Learning: Palette of Pedagogical Options (Source: V.P. Bespalko [1])

Guiding Principle 3: IA as a Toolkit, Not a Recipe

We teach IA controls as a set of tools, frameworks and solutions to be mixed and matched to the specifics of an organization, as opposed to focusing on any one particular approach. We did so out of necessity to meet the employment needs of our region (many different approaches are used in practice); fallout from this approach is that students learn there is no one recipe.

In the early years of the Center, unlike many CAE/IAE's, we responded more to local industry demands for graduates than to the Federal government. In a study we found that the majority of graduates ended up working within 30 miles of the university, an area dominated by industry. At the time, Microsoft had launched the Trustworthy Computing initiative [9]; Boeing was actively seeking IA employees; local companies, like IO Active (pen testers), were asking for resumes of students familiar with IA and secure coding. With the impetus coming more from industry, we emphasized using a variety of standards and tools adapted in a variety of ways to suit the different environments and circumstances of local employers, as opposed to focusing on Federal government IA standards—although these are covered. Since compliance regimes

have grown up within industry sectors, they often overlap within organizations that must comply with a variety of standards—such as PCI, HIPAA, GLBA, SOX—producing hybrid models. We prepare our students to be able to create IA plans in such mix and match environments.

This has shaped our approach to curriculum. While using Federal training standards as the baseline, by training our students in a variety of tools, they are quickly disabused of the notion of a single IA 'recipe' being appropriate for all. That makes them uncomfortable at first; but they learn to problem solve. In designing our courses, this principle manifests, for example, in our reliance on actual cases presented by guest lecturers from industry and government, reinforcing the idea of an IA toolkit, as opposed to expecting a formula. We compare IA experts to plumbers who come to the house with a variety of tools—some they will use, some they won't need—depending on the problem they uncover.

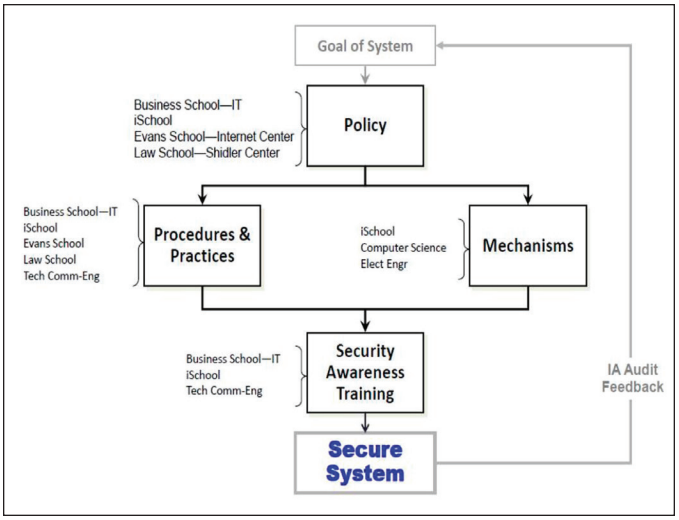


Figure 5: Multi-Disciplinary Approach to Information Assurance

Guiding Principle 4:
Cross Sector and Interdisciplinary Approach

From the beginning, we stressed regional collaboration across sectors (Figure 4), forming Center collaborations with various government, academic and industry organizations. This is expressed in the curriculum in several ways: we make frequent use of guest lecturers from these sources; take on real-world problems as class projects and capstones; and facilitate internships with government and industry, as well as research collaborations with other universities—foreign and domestic—that include our students. Solving complex, real-world problems stretches them to use their IA knowledge in productive, as opposed to reproductive, ways (Figure 3).

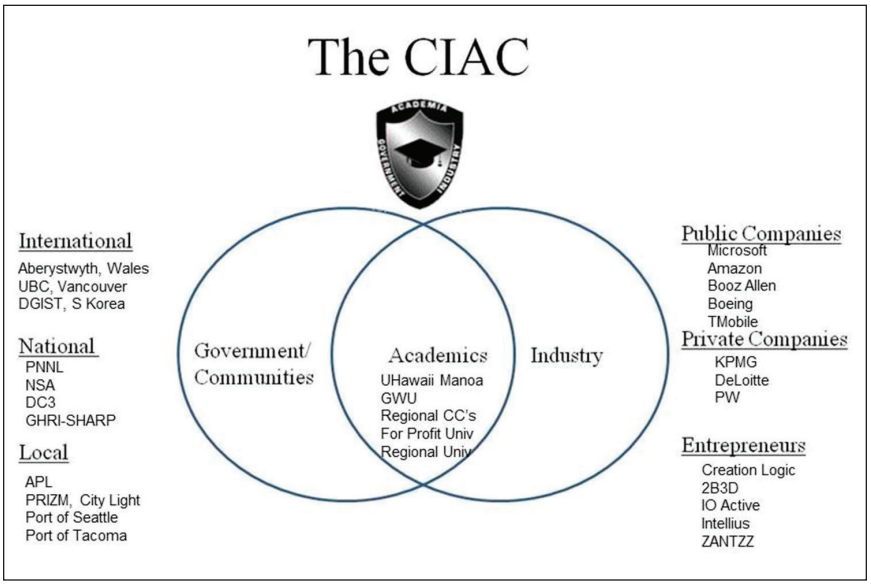


Figure 4: The CIAC: Integrating Community, Industry and Academia in the Pacific Northwest

We also stress a cross disciplinary approach to IA. Taking an organizational view of IA from the Chief Information Security Officer (CISO)'s vantage point, we produced the model in Figure 5 that has guided curriculum development in different academic disciplines at the university. Recognizing that elements ranging from policy to technology keep information secure, we can take a business school slice, for example, through the model, emphasizing the management aspects of IA—policy, compliance procedures, developing an organizational culture of security through awareness training . Using this model, we have developed IA curriculum for business, computer science, information science, library science and urban planning programs—all drawing from the same organizational/operational view of security shown in Figure 5; each taking a relevant slice of this picture that aligns with their particular discipline.

Guiding Principle 5:
Analogy to Developing Elite Athletes

From inception, we analogized the challenge of optimizing development of 'cyber warriors' with the development of Olympic athletes, drawing extensively on the work and experience of one of the authors who was involved with selection and preparation of elite athletes and sport educators for high performance athletic teams [19,25].[2] He applied all of the above approaches while a professor at the prestigious St. Petersburg Lesgaft State University, Russia, the oldest academy of its kind, famous for maturing coaching and athletic talent for Russian national sport and Olympic teams. His work has been disseminated extensively inside and outside Russia in the sports industry and beyond.

We anticipated that by assessing students upon entering our pedagogical system and tai-

[2] Cyber warriors is a term we apply to both industry and government cybersecurity experts. The internet makes no distinctions, in the attackers' view, among the sectors. They are all targets

cybersecurity education

loring curriculum to their specific needs, engagement would increase, as well as interest in IA. This in turn would accelerate learning and ultimately the development of expertise. We have begun to see career results in our graduates that lead us to believe this is supportable. We are in the process of data collection that will allow more discrete analysis of our results.

The meta model in Figure 6 summarizes our pedagogical management approach, beginning with assessment, then making relevant decisions about deficiencies and remedies that translate into execution of resulting plans, and then providing feedback for program correction. When optimizing the development of an elite athlete, the coach (or educator) carefully assesses the skills and capabilities of each athlete, diagnosing strengths and deficiencies, making decisions and executing plans designed to nurture strengths and compensate for deficiencies, then entering into a feedback loop that results in re-assessment. Likewise, in our view, developing elite cyber warriors requires the same approach.

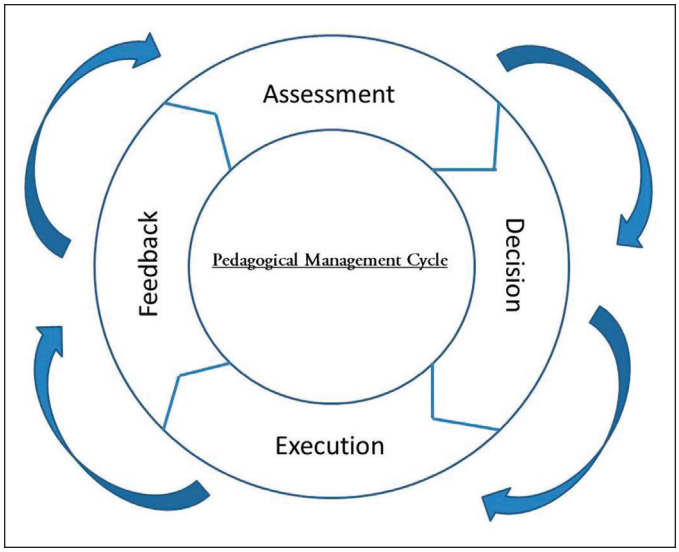


Figure 6: Pedagogical Management Cycle

We use this model to assess and plan for an entire incoming IA class, characterizing the incoming cohort so that we can tailor our offerings to engage them. That means each year, with each new IA cohort, the curriculum varies. Each incoming group is asked the following series of questions:

- In what degree program are you enrolled?
- How close are you to graduation?
- What is your background in IA (knowledge and experience)?
- What do you wish to get from this course (besides a good grade!)?

From our experience, aside from the obvious differences implied by each discipline in which our courses are taught, each new cohort has a distinct character. Answers to these questions at the beginning of the year are used to assess their level of readiness for studying IA and the curiosities that drive the group. This information results in adjustments to the curriculum content to meet the needs of these particular students, keeping in mind our pedagogic goals.

To enhance our management approach, as a systems forming factor, we now employ the NIST/NICE model to encourage students to do their own personal assessment and guide their own growth beyond what they are getting in class.[3] The job tasks associated with each NIST/NICE pathway help students determine the kinds of things they might enjoy doing on the job. The associated skills required for each pathway provide students with a template for understanding what they need to know in order to be qualified for the pathways that interest them. They can compare this list with what they are learning in their formal IA classes and seek remedies outside the program to complete what they need to know. Remedies include professional organization membership, certifications, internships, research projects, reading—things they must do themselves, outside the classroom, in order to complete their preparation as professionals for the track/s they choose to pursue.

This is just the beginning of the student's transformational process and only partially addresses content delivered. The complete pedagogical system we designed provides an efficient path to IA professionalism, from raw recruit to competent practitioner, putting the student at the center of the process. We put these pieces together through an example that follows.

EXAMPLE IAC: SECURE SOFTWARE CODE DEVELOPMENT CURRICULUM (SSCD)

Secure software code development curriculum (SSCD) is one example of an IAC instantiation derived from the KBP pedagogical model. Given the economic and employment environment in the Pacific Northwest in the middle of the last decade when local employers placed new emphasis on the production and deployment of secure software code, we became interested in preparing our students to meet these new demands.

The problem we were presented by industry was compelling. The same programming flaws in code were being created over and over, in spite of raised awareness at the workplace and availability of public tools like the NVD (National Vulnerability Database) and the CWE (Common Weakness Enumeration) that catalogue software flaws. Employers encouraged us to teach secure coding practices as one way to mitigate the problem in our graduates.

Applying our model, we created a pedagogy designed to enhance the professional preparation of software engineers, making them more competitive in the marketplace, and enabling them to carry an inherent sensitivity to the security consequences of the software they build. We have been working with this original IAC system ever since in subsequent iterations, in addition to developing and disseminating curricular artifacts and workshops to assist

[3] The NIST/NICE framework [16] provides useful guidance to government, and now industry, in describing careers in cybersecurity. As educators, we have found it useful guidance in identifying educational outcomes.

other faculty in developing secure coding courses and threaded topics for insertion in existing classes.

Applying the KBP model

Using our approach, we first described each element of the KBP at a high level—Students, Teachers, Goals, Content, and Didactic Processes—and how they interrelate.

The **Students** in the initial instantiation of the SSCD were professional software developers who needed to unlearn their coding habits and re-learn new secure software coding techniques. The in multiple modes—kinesthetically, as well as aurally and visually.

Applying the KBP Pedagogical Model to create the SSCD-IAC (information assurance curriculum) model, the same two generic intelligent elements and three generic infrastructure elements persist and then must be specifically described in terms of secure software code development. The five elements of the KBP function as a system; changes in one element will induce changes in the other four, and so on. Thus instances of the SSCD-IAC model will vary, for example, with changes in the students. What we might teach returning adults with development experience will differ

Within the software engineering community, there is an increasing recognition that secure coding practices are only a subset of the activities needed to create secure information systems.

Teachers were experienced software developers with a background in secure code development who could bring actual cases and examples from their practice into the classroom.

In walking through the remaining infrastructure elements, we have the following.

Goals

The overall goal was to induce learning within a mature set of students, causing a change in behavior. This is different from working with students who are just learning programming. Our students needed to change long-held ways of thinking about coding and adopt new programming habits. Thus, learning objectives incorporated individual personal and professional growth ideas in addition to the new technical skills and knowledge that students were expected to master. Understanding the goals of the class for this specific set of students helped prioritize learning objectives assigned to each lesson, which were based on information assurance and secure coding best practices. These learning objectives included things like: understand and explain IA principles and practices, understand and demonstrate threat-modeling techniques, implement secure coding techniques, produce systems that protect information.

Content

Content for a secure software code class was drawn from a large body of knowledge that integrated standards produced by recognized software development groups and subject matter experts. Specific content was tailored to fit into the available class time and mapped to course goals. Further, a range of learning levels and skills to be acquired were mapped to the class content and sequence of presentation. This will be discussed in more detail later.

Didactic Processes

How we teach is as important in our model as the content. Didactic processes used to deliver content in the secure software curriculum were selected to match learning goals related to the content elements in the course. For example, hands-on case studies were used to emphasize certain topics so that students were stimulated to learn from what and how we might teach undergraduates with no programming experience. During the actual curriculum development process, these five elements were exhaustively discussed among the collaborators. We've just touched on some of the changes that may distinguish one instance of the SSCD from another. As the curriculum is developed through the process discussed next, these elements are revisited and changed iteratively as the curriculum continues to be defined and described.

Conceiving of curriculum as an inter-related system of elements has eased the process of updating IA curriculum to reflect the dynamic changes the field experiences. It has also eased the development of IA curriculum for different disciplines, enabling us to produce new adaptations efficiently.

Methodology for curriculum design

According to Bespalko's methodology for curriculum design [1], the six steps below must be followed in the order presented:

1) Determine the content of the subject in light of general educational goals.
2) Determine specific goals (levels of learning) for each element of the subject taught.
3) Determine in what order each element of the content should be taught.
4) Determine the amount of time to be spent on each subject and optimize the student's progression through the subject, teaching the minimum needed to be able to perform independently.
5) Define methods of control/evaluation based on goals for each subject element.
6) Recommend the didactic processes that teachers can use.

Next, we describe developing the SSCD following the six steps and produce artifacts we developed during the process.

Step 1:
Determine content considering educational goals

We chose the Asset Protection Model as the basis for curriculum content. The authors, co-developers of the APM (Figure 7), view

cybersecurity education

Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

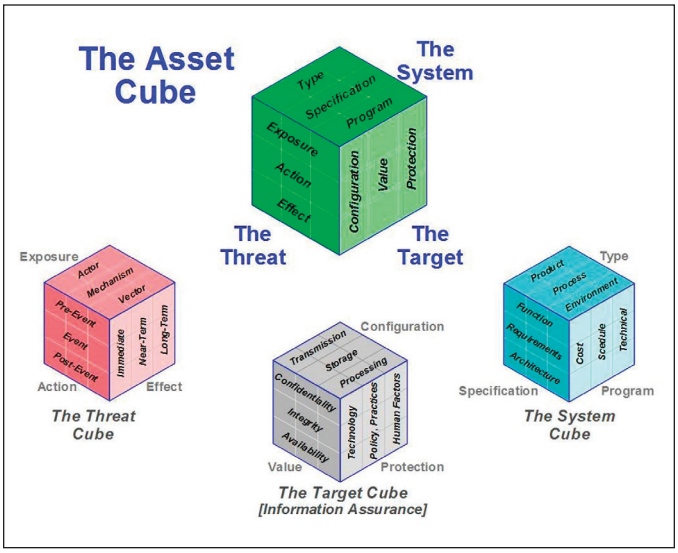


Figure 7: Content Source: Asset Protection Model (APM)

this model as a comprehensive source for secure code curriculum topics [11,23,25]. It provides a common conceptual ontology for secure information system topics; a stable logical framework that is independent of specific organizations, technologies and their associated changes; and a vehicle for structured communication among these groups.

Within the software engineering community, there is an increasing recognition that secure coding practices are only a subset of the activities needed to create secure information systems. Not only the software, but also the hardware, networks and people that contribute to those systems should be considered. The APM accommodates this.

The model acknowledges that the practice of secure information systems design, development, deployment and operation is shared by three professional communities: the justice and intelligence communities, the information assurance community, and the systems engineering (including software engineering) community.[4] Each community is represented in Figure 7, respectively, as: the threat cube, the target cube and the system cube, providing a focus for each community.

Using these three cubes as a reference, topics for secure code curriculum were selected and a graph hierarchy, showing relationships among them, was developed (Figure 8). From the graph, a logical outline of topics was created (Figure 9). Note that the names of the elements evolved as we worked through the process.

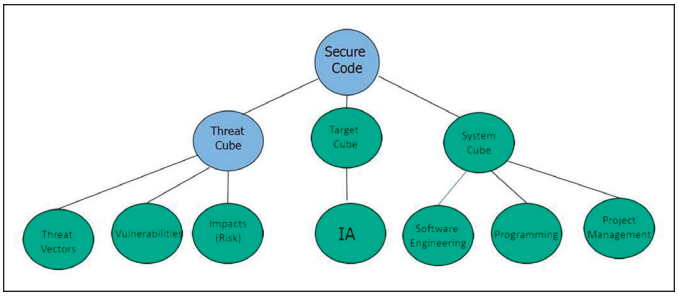


Figure 8: Graph Model of Content

Subsequent steps in the methodology are based on this artifact.

Step 2: Determine specific goals (levels of learning)[5]

Each secure code topic must be assigned a level of learning the instructors believe it deserves in the curriculum in the context of the course goals. As an example, under the *Target Cube, 2.2 Policy and Procedures* may be taught at no greater than a Level 2 or 3. The student either recognizes the term or is able to discuss it in class and perhaps write about it, reflectively. On the other hand, under the *Product Cube, 2.1 Secure Design Patterns and Practices*, since the curriculum goal is to make better software engineers, it makes sense that this topic becomes a focus of more intense learning Levels 4 or 5. To give the reader a sense of what is required at each level, a comparison of *Learning Level III: Reproduction and Learning Level IV: Production* appears in Figures 10. Note the differences in activities required of each.

I. Threat Cube
- 1.1. Threat Vector
  - 1.1.1 Deception
  - 1.1.2. Theft
  - 1.1.3. Manipulation
- 1.2. Vulnerability
- 1.3. Impact

II. Product Cube
1. Development Processes
   - 1.1. Secure Development Lifecycles
   - 1.2. Project Management
   - 1.3. Security in Artifacts
2. Programming
   - 2.1. Secure Design Patterns and Practices
   - 2.2. Language and Compiler Considerations
   - 2.3. Technology Considerations
3. Quality Assurance
   - 3.1. Static Analysis
   - 3.2. Dynamic Testing
   - 3.3. Penetration Testing

III. Target Cube
1. Security Services
   - 1.1. Confidentiality
   - 1.2. Integrity
   - 1.3. Availability
2. Security Countermeasures
   - 2.1. Human Factors
   - 2.2. Policy, Procedures
   - 2.3. Tools
3. Information States
   - 3.1. Transmission
   - 3.2. Processing
   - 3.3. Storage

Figure 9: Logical Outline of Secure Code Curriculum Topics

The output for Step 2 is a table that lists curriculum elements and provides the Level of Learning associated with each. Table 1 provides a sample from the course topic outline above. Levels of Learning can be assigned at whatever level of detail time allows.

[4] The APM integrates several models like: the SSE-CMM (Systems Security Engineering-Capability Maturity Model), the OWASP Software Assurance Maturity Model; output from the NIST/DHW SwA working group; the Microsoft Security Development Lifecycle, the Project Management Body of Knowledge (PMBOK), and the McCumber cube.

[5] Bloom's Taxonomy [2] addresses levels of learning as well, although we rely on Bespalko [1] and Kuzmina [12].

Level III: Reproduction

- **Definition**: simple, straightforward
- **Activities**: Independent reproduction of previously learned material. Student is not generating new information. Every task is based on typical examples the student has memorized.
  - I. II. Constructive tests: No information about the answer given, students must reproduce the answer from memory.
    - Example 1: What kinds of threats do we face today?
      - » (Answer) short essay by student
  - III. Describe Rules, algorithms, formulas: Students given fundamental objectives to accomplish that would require them to reproduce a known rule, algorithm or formula
    - Example 1: How would a programmer eliminate buffer overflow?
      - » (Answer) student would reproduce a block of code or describe step-by-step the approach to elimination
    - Example 2: What are the rules for building a secure website?
      - » (Answer) student would recite rules provided previously by instructor for steps to secure website

Level IV: Production

- **Definition**: Acquiring subjectively new (to the student) information.
- **Activities**: Solving tasks by modifying information already learned/memorized in Level III and applying to new circumstances. Student breaks down/simplifies previous examples into steps that can be applied to addressing new or additional conditions/circumstances. Students are graded on the thoroughness and quality of what they produce. They gain new knowledge about ways/methods they've already learned in the process of addressing new requirements.
  - Practicums: Considering certain new conditions, implement new knowledge.
    - Example 1: Given this policy for computer security, what procedures would you develop for this company to guard against insider threats?
      - » (Answer): Student would adapt what they had learned about preventing insider threats to address the policy described in this particular question.
    - Example 2: Under the following conditions (*instructor enumerates*) what technologies would you apply to mitigate network attacks?
      - » (Answer): Student would assemble network mitigations previously studied into an architecture specific to the conditions described in the question.
    - Example 3: You have been asked to develop an authentication module for a software package that will be implemented in a heavily secured government facility. How would you increase the security of the authentication module studied in class to address these new conditions?
      - » (Answer) Student would add additional code to the module studied in class.

Figure 10: Learning Level III vs. Level IV

TABLE 1:
SAMPLE CURRICULUM ELEMENTS VS. LEVEL OF LEARNING

Threat Cube	Topic	Learning Level
1.1 Threat Vector	1.1.1 Deception	Level 4- Reproduces in lab
	1.1.2 Theft	Level 4- Reproduces in lab
	1.1.3 Manipulation	Level 5- Solves a problem
1.2 Vulnerability		Level 3- Plays back info

Step 3:
Determine order each element of content should be taught
Once levels of learning have been established, topics are organized in the order they should be taught. For our purposes, we were designing not just one course, but a series of topics and courses in secure coding that could be taught across multiple years. We decomposed the elements in further granularity and then distributed them across a four-year program. The first year's activity is given in Figure 11.

Step 4:
Determine the amount of time to be spent on each subject
This step is straightforward. Total classroom hours are distributed across the course topics. Figure 12 is work product that indicates where time will be spent in the first course. Emphasis was on orientation to IA (Target Cube), with more time spent on the Threat Cube.

Each step in the methodology produces dialogue among the instructor/collaborators. This helps enrich the end product and prepare several instructors to teach the material.

Step 5:
Define methods of control/evaluation based on goals for each subject element
At this stage, we identified assignments that would elucidate each topic. Going back to our guiding principles, our preference was for

- **YEAR 1**

[I]. Exposure to Building Software using Programming Language

II. Product Cube
- 2. Programming (R)
  - 2.1. Language (R)
    - 2.2.1. C/C++
    - 2.2.2. Java
    - 2.2.3. C#
  - 2.2. Environment (R)
    - 1.1.1. Stand Alone
    - 1.1.2. Web
    - 1.1.3. Database
  - 2.3. Testing (R)

[II]. Threat Diagnostic (Part A)

I. Thread Cube
- 1.1. Threat Vector (R)
  - 1.1.2. Tampering with data (R)
    - 1.1.2.1. Unsecured access to pages and components
    - 1.1.2.2. HTTP cookies
      - 1.1.2.3. Users are added, removed or modified
      - 1.1.2.3.1. Perform SQL injection attacks
      - 1.1.2.3.2. Perform OS command injection attacks
  - 1.1.5. Denial of Service (R)
    - 1.1.5.1. Perform buffer overflow attacks
      - 1.1.5.1.1. Remove client-side validation
      - 1.1.5.1.2. Perform long string injection attacks
    - 1.1.5.2. Perform DoS attacks
    - 1.1.5.3. Poorly behaved components that can be exploited
    - 1.1.5.4. Disabling a credential store

Figure 11: Part of Year 1 of Secure Code Curriculum Plan

activity-based learning. We identified exercises that could be either demonstrated in the lab or performed as a homework assignment, depending on how we chose to evaluate students. 'Deception' and 'Theft' were categorized as Level IV learning opportunities indicating exercises that could be performed in a lab setting with instructor guidance (Figure 13). 'Manipulation,' not shown here, was identified for exercises in creative problem solving which meant either partnering with 'clients' on a real world problem or perhaps developing a demonstration on their own to share with the class.

cybersecurity education

Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

- **I. Threat Cube**
  - 1.1. Threat Vector
    - 1.1.1 Deception (8)
    - 1.1.2. Theft (14)
    - 1.1.3. Manipulation (13)
  - 1.2. Vulnerability (3)
  - 1.3. Impact (3)
- **II. Product Cube**
  1. Development Processes
     - 1.1. Secure Development Lifecycles
     - 1.2. Project Management
     - 1.3. Security in Artifacts
  2. Programming
     - 2.1. Secure Design Patterns and Practices
     - 2.2. Language and Compiler Considerations
     - 2.3. Technology Considerations
  3. Quality Assurance
     - 3.1. Static Analysis
     - 3.2. Dynamic Testing
     - 3.3. Penetration Testing
- **III. Target Cube**
  1. Security Services (3)
     - 1.1. Confidentiality
     - 1.2. Integrity
     - 1.3. Availability
  2. Security Countermeasures (11)
     - 2.1. Human Factors
     - 2.2. Policy, Procedures
     - 2.3. Tools
  3. Information States (3)
     - 3.1. Transmission
     - 3.2. Processing
     - 3.3. Storage

Figure 12: Topics with Assigned Hours

- **I. Threat Cube**
  - 1.1. Threat Vector
    - 1.1.1 Deception (8)
      - 1.1.1.1. Spoofing identity
        - 1.1.1.1.1. Basic HTTP Authentication sends credentials in the clear
        - 1.1.1.1.2. Credentials of tokens stored in HTTP cookies
        - 1.1.1.1.3. Authentication tokens in the clear on the wire
        - 1.1.1.1.4. Intercepting DNS request – DNS spoofing
      - 1.1.1.2. Repudiation
        - 1.1.1.2.1. User performs illegal operation and there is no trace of what happened
        - 1.1.1.2.2. Attackers get a product ordered w/o paying and there is no audit trail
    - 1.1.2. Theft (14)
      - 1.1.2.1. Information Disclosure
        - 1.1.2.1.1. Reading on the wire
        - 1.1.2.1.2. Error messages at login time divulge too much information
        - 1.1.2.1.3. Unsecured pages and components
      - 1.1.2.2. Elevation of Privilege
        - 1.1.2.2.1. Hijack someone else's session
          - 1.1.2.2.1.1. Perform cross-site scripting attacks
          - 1.1.2.2.1. 1. Sniff the session ID using a network sniffer
        - 1.1.2.2.2. Replay a stolen session
        - 1.1.2.2.3. Log in without the proper credentials
          - 1.1.2.2.3.1. Perform SQL injection
          - 1.1.2.2.3.2. Perform brute-force / dictionary attacks
        - 1.1.2.2.4. Use forceful browsing to access pages with no proper authentication
          - 1.1.2.2.4.1. Use URL tampering techniques

Figure 13: Topics with Assignments

Topics at lower levels (1 – 3) would be subject to evaluation on written tests or quizzes, or perhaps in writing assignments in discussion forums.

Step 6:
Recommend the didactic processes that teachers can use

The final step in the methodology is recommending what didactic processes will be used to convey different elements in the curriculum. Didactic processes are the feedback mechanism that provide students confirmation (or not) of their learning progress. For the instructor, they answer the question: 'how will I teach this material so that students will learn?'

For example, in the stand-and-deliver method of lecturing, the instructor assumes learning is taking place, but may not know until the final exam is given. There are, however, computerized approaches that control the learning process by not allowing students to progress to the next step if they can't pass a quiz on the current one.

Having the material structured through the previous five steps allows the instructor to decide how learning will be assured and the learning process controlled. For our purposes, we discussed various delivery modes as alternatives—guest lectures, conversations with experts. We made decisions about whether to have students break out into discussion groups in class to discuss topics among themselves, or use asynchronous discussion forums monitored online and commented upon by the TA or professor. Alternatively, we decided whether to show videos demonstrating certain hacking concepts or to lead students into a hands-on hacking experience in a guided, air-gapped lab. Didactic processes determine how quickly students learn, how engaged they are and their level of excitement for the subject.

RESULTS

In the past nine years, applying the KBP model, along with our guiding principles, has resulted in development of 23 individual courses in IA taught in five different disciplines at the University of Washington and the Center's partner schools. In addition several IA certificate programs, degree concentrations and complete degrees either have been launched, or are under construction, with the authors either taking a direct hand in development or acting in an advisory capacity.

Further, one of these programs, the yearlong Information Security and Risk Management (ISRM) Certificate, educated its

To strengthen our program, we have built an informal alumni organization; many of our graduates come back to lecture and teach in our programs, as well as recruit employees for their respective firms.

9th cohort in AY2012-13 (Table 2). Growth in the program has been significant. Beginning with 11 students in 2005, last year we graduated 62 successfully. We now conduct two complete cohorts simultaneously—one composed of graduate students, the other of returning adults in continuing education. Of these students, approximately 30% have been women and 13 have been military/veterans from a special outreach program with the Washington National Guard. This program was one of the university's initial offerings through Coursera, with over 24,000 students in the first class. It has been repeated each quarter since. Our retention rates are higher than average and we estimate a total of 50,000 students have completed our series.

The growth of our program may be partially attributable to the reputation of our graduates. Several local firms annually seek opportunities to interview and hire our students. Anecdotally, we know we have had many go into IA careers with industry and government and progress to higher ranks. They are malware and risk analysts, IA auditors, and IA executives and managers. Chief among them are (1) the NCC Deputy Manager, National Communications System, Cybersecurity and Communications within the US Department of Homeland Security, (2) a Technical Director with the National Security Agency, (3) a Chief Information Security Officer with a university in Southern California, (4) CEO and Founder of an IA consulting firm, now in its 4th year, and (5) a senior malware consultant in Washington, DC.

TABLE 2: ISRM CERTIFICATE GRADUATES 2005-2013

Cohort	Academic Year	Total Certificate Students (No. of female)	Total Matriculated Students (No. of female) *[No. of Washington National Guard]*
I	2005	11	
II	2005-6	16 (5)	
III	2006-7	18	
IV	2007-8	19 (4)	16 (4)
V	2008-9	17 (5)	8 (3)
VI	2009-10	12 (4)	14 (4)
VII	2010-11	22 (5)	30 (8) [5]
VIII	2011-12	27 (5)	33 (12) [6]
IX	2012-13	28 (6)	34 (18) [2]
Total		**170 (34)**	**135 (49) [13]**

To strengthen our program, we have built an informal alumni organization; many of our graduates come back to lecture and teach in our programs, as well as recruit employees for their respective firms. We are in the process of formalizing this group and hope to collect additional data regarding career progression of those who have graduated. This will give us more insight into any progress we have made in better preparing students to become IA professionals. Our future work involves continuing to improve our pedagogical processes and assessing our programs against our stated goals.

While the first instantiation of any IAC model requires an investment of time, it has been our experience that it pays off by providing materials that can be leveraged easily to create different instantiations and updated curriculum that keeps pace with change. **Ir**

References

[1] Bespalko, V. *Fundamentals of Theory of Pedagogical Systems.* (Vorenege, RU: Voronege State University Press, 1977).

[2] Bloom, B., Mesia, B. and Krathwohl, D. *Taxonomy of Educational Objectives.* (New York: David McKay Company, 1964).

[3] Chabrow, E. "Placing in Context the Infosec Skills Gap: NASCIO's Chad Grant Analyzes Challenges." *GovInfoSecurity.com*, Princeton, NJ. http://www.govinfosecurity.com/interviews/placing-in-context-infosec-skills-gap-i-986. Accessed 2013 June 30.

[4] Chief Information Officer, US Department of Defense. "Information Assurance Scholarship Program: Are You Ready?" *US Department of Defense*, Washington, D.C. http://dodcio.defense.gov/Home/Initiatives/InformationAssuranceScholarshipProgram(IASP).aspx. Accessed 2013 June 30.

[5] Endicott-Popovsky, B., Frincke, D., Popovsky, V. "Designing a Computer Forensics Course for an Information Assurance Track." in *Proceedings of the Eighth Colloquium for Information Systems Security Education.* (West Point, NY: Colloquium for Information Systems Security Education, 2004): 59-64.

[6] Endicott-Popovsky, B., Frincke, D., Popovsky, V. "Secure Code: The Capstone Class in an IA Track." in *Proceedings of the Ninth Colloquium for Information Systems Security Education.* (Atlanta, GA: Colloquium for Information Systems Security Education, 2005).The Printing House, Inc., Stoughton, WI.: 100-108.

[7] Endicott-Popovsky, B., Seifert, C. Frincke, D. "Adopting Extreme Programming on a Graduate Student Project." in *Proceedings of the Sixth IEEE Systems, Man and Cybernetics Information Assurance and Security Workshop.* (West Point, NY: 2005) IEEE Publishing, Los Alamitos, CA. ©2005: 454-455.

[8] Fitzpatrick, A. "For Job Security, Try Cybersecurity, Experts Say." *Mashable.com*, Mashable, Inc., New York. http://mashable.com/2012/05/29/cybersecurity-career/ . Accessed 2013 June 30.

[9] Gates, W. "Trustworthy Computing." *January 15, 2002 Memo.* Microsoft Corporation, Seattle, WA.

[10] Goldman, A. (2009). "Feds Need 10,000 Cyber Security Experts." *Internet News.com*, Quin-Street Enterprise, Louisville, KY. http://www.internetnews.com/security/article.php/3823806. Accessed 2013 June 30.

[11] Hansel, L., Chung, S. and Endicott-Popovsky, B. "Software Reengineering Approach to Teaching Secure Coding Practices. in *Proceedings of the Fifteenth Colloquium for Information Systems Security Education.* (Fairborn, OH: Colloquium for Information Systems Security Education, 2011). The Printing House, Inc., Stoughton, WI: 29-36.

[12] Kuzmina, U. *Fundamentals of Pedagogy of Higher Education.* (Leningrad, RU: Lenizdat, 1972).

[13] Michailova, A. "Establishing a System of Professional–Practical Activity." *Messenger of Higher Education*, Moscow, RU, 11, (1985): 31-33.

[14] National Academies of Science. *Rising above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future.* (Washington, D.C.: The National Academies Press, 2005).

[15] National Security Agency Central Security Service. "National Centers of Academic Excellence." National Security Agency, Washington, D.C. http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. Accessed 2013 June 30.

[16] NIST/NICE framework. http://csrc.nist.gov/nice/framework/. Accessed 2014 January 6.

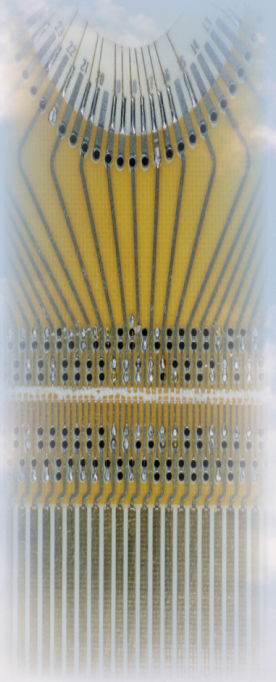
[17] Pecinovsky, E. "A Human Capital Crisis in Cybersecurity." *ClearanceJobs.com.* Dice, Inc., Urbandale, IA; http://www.clearancejobs.com/cleared-news/152/a-human-capital-crisis-in-cybersecurity. Accessed 2013 June 30.

[18] Popovsky, V. and Endicott-Popovsky, B. "Integrating Academics, the Community and Industry." in *Proceedings of the Physical Culture and Sports: Analysis of Social Processes '08.* (St. Petersburg, RU: 2008), Lesgaft National State University Press, St. Petersburg, RU: 239-243.

[19] Popovsky, V. "Coaching Volleyball with Unleashing Personal Potential in Mind." in *Proceedings of the Int'l Conference Honoring 70th Anniversary Sports Games Dept. Lesgaft State Academy of Physical Education '04*, (St. Petersburg, RU 2004), Lesgaft National State University Press, St. Petersburg, RU: 136-140.

[20] Popovsky, V., Endicott-Popovsky, B., "Physical Culture Pedagogy: Coaching by Design." in *Methods for Modernizing Physical Culture: Selection of Scientific and Methodological Works*, edited by V.E. Grigoriev, (St. Petersburg, Russia, 2005): 176-187.

Curriculum Assessment Pedagogy Space.org



The ACM Committee for Computing Education in Community Colleges

Serving Computing Education Communities since 1991

CAPSpace.org

cybersecurity education

Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

[21] Roginsky, V. *Alphabet of Pedagogical Work*. (Moscow, RU: Higher Education, 1990).
[22] Simpson, J. and Endicott-Popovsky, B. "A Systematic Approach to Information Systems Security Education." in *Proceedings of the Fourteenth Colloquium for Information Systems Security Education*, (Baltimore, MD: Colloquium for Information Systems Security Education, 2010). The Printing House Inc., Stoughton, WI: 173-179.
[23] Simpson, J., et al. Secure software education: A contextual model-based approach. *International Journal of Secure Software Engineering*, (2010). 1(4). pp. 35-61.
[24] Talizina, N. Activity approach to the development of the model specialist. Messenger of Higher Education, Moscow, RU, 11, (1986): 10-13.
[25] Talizina, N. *Management of the Learning Process*. (Moscow, RU. Higher Education, 1975).
[26] US Office of Personnel Management. "Cybercorps: Scholarship for Service." https://www.sfs.opm.gov/. Accessed 2013 June 30.
[27] Wiggins, G. and McTighe, J. *Understanding by Design*, 2nd ed. (Alexandria, VA: Association for Supervision and Curriculum Development, 2005).

BARBARA E. ENDICOTT-POPOVSKY
University of Washington
Information School
4311 11th Avenue NE, Suite 400
Seattle, Washington 98105 USA
endicott@uvv.edu

VIATCHESLAV M. POPOVSKY
University of Idaho
HERD
709 South Deakin Street
Moscow, Idaho 83844 USA
dr_popovsky@hotmail.com

Categories and Subject Descriptors: K.3.2
General Terms: Security
Keywords: cybersecurity, education and workforce development, pedagogy

DOI: 10.1145/2568195.2568214 © 2014 ACM 2153-2184/14/03 $15.00

CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT

How to Build a Strong Cybersecurity Workforce

WHAT IS CYBERSECURITY?

Cybersecurity refers to the technologies and techniques used to protect information and systems from being stolen, compromised or attacked. This includes unauthorized or criminal use of electronic data, attacks on networks and computers, and viruses and malicious codes. Cybersecurity is a national priority and critical to the well-being of all organizations. Start building your cybersecurity workforce today. Together, we can build a skilled and cyber-capable workforce to meet the cybersecurity challenges of the future.

ABOUT PLANNING YOUR CYBERSECURITY WORKFORCE

Cybersecurity professionals have unique skills, are in short supply, and are vital to our nation's security. As a result, competition for talent is fierce and establishing a strong team is essential. This requires organizations to tailor how they plan for their cybersecurity workforce so they have the right people in the right positions. The Department of Homeland Security (DHS) is committed to strengthening the workforce to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders.

This kit will help you strengthen your organization through tools to help you understand your organization's cybersecurity workforce risks and take inventory of your workforce, templates to create your own cybersecurity career paths, and resources to recruit and retain top cybersecurity talent. Before getting started, familiarize yourself with key cybersecurity workforce design concepts and best practices:

Cybersecurity Workforce Planning Diagnostic

Cybersecurity Capability Maturity Model

Best Practices for Planning a Cybersecurity Workforce

National Cybersecurity Workforce Framework

Cybersecurity Training Catalog

HOW TO USE THE TOOLKIT

This kit has the resources and information you need to plan, build, and advance your cybersecurity workforce. How you use this toolkit is up to you: use the kit to start conversations with managers about building their cybersecurity teams, talk with employees about professional development, and/or integrate the concepts found in this toolkit into strategic planning efforts for future staffing needs. This kit is meant for Leaders and Program/Function Managers in large government and private organizations, including Human Resources, Information Security, Risk Management, Information Technology and Cybersecurity. For more information email niccs@hq.dhs.gov.

WHAT'S INSIDE?

This kit has a number of tools to help you build your cybersecurity workforce. All of the content can be found online at https://niccs.us-cert.gov/. Adapt the content for your organization's specific cybersecurity needs.

PREPARE

Assess Your Organization's Cybersecurity Workforce Planning Readiness

Self-assessment to determine the readiness of your organization to conduct cybersecurity workforce planning.

PLAN

How to Plan for your Cybersecurity Team

Tools to evaluate your current and future cybersecurity workforce needs; explore your cybersecurity risks; and suggestions to close workforce gaps.

BUILD

What Should a Cybersecurity Team Look Like?

Roles that make up a great cybersecurity team; cybersecurity talent profiles to help make informed hiring decisions; and tips for recruiting cybersecurity staff.

ADVANCE

Develop Your People

Templates to create custom cybersecurity career paths; links to training, certifications and professional events; and ideas for retaining staff at every level.

P R E P A R E

ASSESS YOUR ORGANIZATION'S CYBERSECURITY WORKFORCE PLANNING READINESS

A first step in preparing to build your cybersecurity workforce is having a shared vision for organizing your cybersecurity workforce against cybersecurity work. Having a common understanding supports leaders in responding to changing environments – giving you data to better adjust resources, see patterns of work, and highlight areas of potential risk. This is especially important in the ever-changing environment of cybersecurity.

To understand your organization's readiness to begin assessing your cybersecurity workforce, explore the **Cybersecurity Workforce Planning Capability Maturity Model (CMM).** The CMM is a self-assessment tool to help organizations evaluate the maturity of their cybersecurity workforce planning capability.

DOWNLOAD

How Mature is Your Cybersecurity Workforce Planning Capability?

Each organization is unique. Some may not need their workforce planning capability to reach the *optimizing* state. The CMM helps you identify with one of these levels, and determine where to best apply your organization's planning resources:

Workforce Planning Maturity Levels

LIMITED

The most basic level, with a cybersecurity workforce planning capability in its infancy. For example, this organization may have limited established processes, lack of clear planning guidance, and limited data and analysis methods.

PROGRESSING

This level indicates some aspects of cybersecurity workforce planning throughout the organization that have started to perform and establish some infrastructure to support planning efforts.

OPTIMIZING

The highest level of maturity, indicates workforce planning capabilities that are fully developed, are integrated with other business processes, and can support different levels of workforce and workload analysis.

P

L

A

N

HOW TO PLAN FOR YOUR CYBERSECURITY TEAM

Your organization must ensure protection against threats to information systems. Unchecked risk puts any organization in jeopardy. Security breaches are often caused not by breakdown in technology, but by breakdown in organizational structure or workforce. To plan for protection, you need a good understanding of your current cybersecurity workforce as well as a strategy for the structure and management of that workforce for the future.

Below are the first five (5) steps to start planning for your cybersecurity team, including developing an inventory of your current cybersecurity workforce, understanding workload and staffing levels, and beginning to address any gaps.

1. **Explore Your Cybersecurity Risks:** Gain foundational knowledge about your cybersecurity workforce risk and the extent to which your organization can tolerate the potential outcomes. Increased risk places greater demands on your workforce and drives much of your future cybersecurity workforce needs.

   To help identify your general cybersecurity risk exposure and risk tolerance, and tailor your cybersecurity workforce planning to better predict future need, use the **Cybersecurity Workforce Planning Diagnostic**. While the Diagnostic will help identify general cybersecurity risk exposure and risk tolerance (i.e. your risk profile), it is not a substitute for in-depth, organization-specific risk assessment and analysis in collaboration with leadership, human capital experts and cybersecurity managers. (Separate sections for government and private organizations are included as well).

   DOWNLOAD

2. **Inventory Your Cybersecurity Workforce:** Work with your cybersecurity managers to quantify the size of your cybersecurity team, number of vacancies, identify the team's skills, and capture the activities they perform.

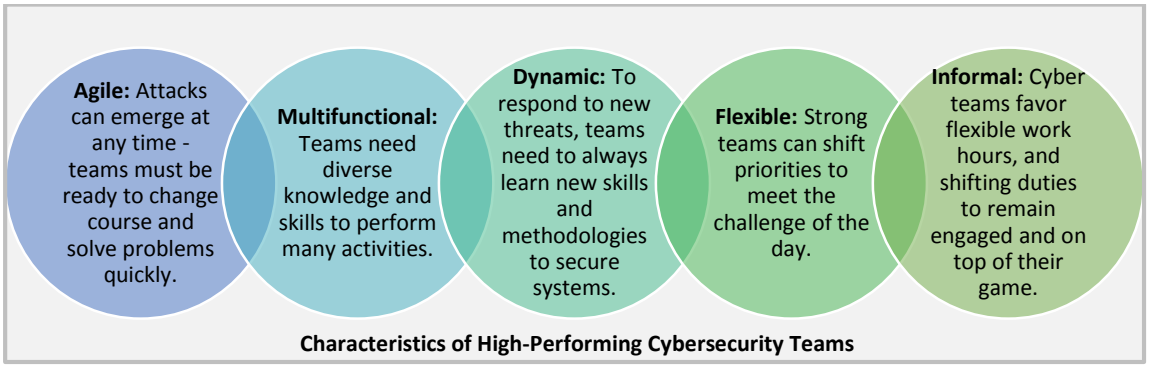
   Government organizations – Access the Office of Personnel Management's (OPM) Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report to see a count of staff performing cybersecurity work, as well as training needs and workforce demographics (e.g., proficiency levels, background).

   Private organizations – A tool to help inventory your cybersecurity workforce is forthcoming. This toolkit will be updated to provide this tool.

P L A N

Use the results as a baseline to understand the current state of your organization's cybersecurity workforce. Refresh your workforce analysis on an annual basis.

As you take inventory of your cybersecurity staff skills, also consider the following recommended characteristics of high-performing cybersecurity teams. Use these characteristics as an additional guide to determine current and future staffing needs.



Characteristics of High-Performing Cybersecurity Teams

3. **Determine Any Gaps:** Evaluate your organization's risk profile and workforce planning recommendations from step 1 (Workforce Planning Diagnostic) *against* your workforce inventory in step 2 to begin to determine future needs and close gaps. For example:
   - ✓ List the skills needed to meet your team's workload and the types/number of professionals you need to develop internally or recruit externally
   - ✓ Determine hiring targets for vacancies and initiate recruiting (see *Build* section for cybersecurity-specific tips)
4. **Address the Gaps:** Below are examples of steps you can take to address the gaps identified in your organization's cybersecurity workforce inventory.
   - ✓ Consider adjusting the mix of positions and skills that make up your cybersecurity workforce
   - ✓ Search the **NICCS Training Catalog** to identify training for your workforce:

     GO
   - ✓ Determine if you can assign additional job duties to existing staff
   - ✓ Develop a program to create future cybersecurity leaders
   - ✓ Convene an internal panel of decision makers. Consider including:
     - Senior leaders
     - Financial and budgetary representatives
     - Human capital experts
     - Cybersecurity managers
   - ✓ Consider aligning the workforce planning process to your organization's budgetary process to ensure funding for cybersecurity positions
5. **Review and Update:** Once you have completed the first four steps, revisit the CMM in the *Prepare* section to determine additional ways to further your planning capability.

BUILD

WHAT SHOULD A CYBERSECURITY TEAM LOOK LIKE?

One way to ensure you have the right cybersecurity team is to align to current national standards. The National Cybersecurity Workforce Framework (Workforce Framework) is the standard for defining your cybersecurity workforce. Align position descriptions, job duties, and competencies to the Workforce Framework to operate successfully. For example, you can use Specialty Area definitions, as well as Tasks and knowledge, skills and abilities (KSAs), to develop position descriptions and establish competency models.

1. **Explore the Workforce Framework.**

   GO

2. **Align your Cybersecurity Workforce to National Standards:** Understand how each position aligns to the Workforce Framework to uncover potential skill gaps.
   - **Choose from a list of Specialty Areas** (found in the Workforce Framework) for each position that includes cybersecurity work
   - **Compare current tasks performed to additional tasks recommended** for each Specialty Area

What is the National Cybersecurity Workforce Framework?

The Workforce Framework is the foundation for all cyber workforce development activities and was created to increase the size and capability of the U.S. cybersecurity workforce.

- Organizes cybersecurity work into 7 Categories and 32 Specialty Areas
- Identifies the tasks and knowledge, skills, and abilities (KSAs) required to complete cyber work

3. **Use the following template to create custom cyber-specific positions for your organization.** Populate the highlighted fields with information that meets the needs of your organization (you can find Specialty Areas and Task Examples in the Workforce Framework).

Position Title	*[Fill in Position Title]*
Primary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Secondary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Current Tasks Performed (i.e., specific job duties) – see general role examples in Workforce Framework Employer User Guide for sample wording	
Additional Tasks recommended by Specialty Area	

B U I L D

What to Look for in High-Performing Cybersecurity Professionals

Another important part of building a cybersecurity team is knowing the unique characteristics you want to add to your team. Whether your organization is looking to hire one cybersecurity worker or build a whole team, understanding what makes a cybersecurity professional tick is important to attracting - and keeping - the right team. The table below features many of the traits of top cybersecurity professionals. (Also refer to the list of page five of this kit for high-performing *team* characteristics).

Review this table and consider if individuals on your team with skills from the Workforce Framework also have these traits; how might they expand their skills to fill your need?

Also, think about how you might change your approach to attracting cybersecurity professionals to better identify individuals with these attributes.

For example, **use the questions to interview candidates for your cybersecurity team.**

	Passionate	Systems Thinker	Problem Solver	Abstract Thinker
TRAITS	• Intrinsic interest in cyber work • Early adopter of technology • Displays excitement when discussing technology	• Understands how parts of a system interact and operate as a whole • Comfortable with complexity	• Oriented toward finding solutions to complex challenges • Takes unique approaches depending on the problem	• Tends to think 'outside the box' • Evaluates challenges from many different perspectives before acting
QUESTIONS	**Describe your career interests and goals.** - Where do you see yourself in a few years? - Describe a time you had to display courage or persistence to achieve a goal.	**Describe a time you had to analyze a problem by understanding the parts.** - What were the parts? - What was the outcome?	**Describe a time you solved a complex problem.** - What data did you gather? - How did you decide on a solution? - What was the outcome?	**Describe a time you had to come up with a novel solution to a challenge.** - What was the problem? - How was your solution novel?

BUILD

How to Recruit Top Cybersecurity Talent

Use the Cybersecurity Recruitment Activity Checklist to build a cybersecurity workforce that meets the needs of your organization.

Cybersecurity Recruitment Activity Checklist

Use the checklist to recruit top cybersecurity talent.

IDENTIFY VACANT POSITION(S)

- ❑ Work with hiring managers and workforce planners to determine cybersecurity recruiting needs
- ❑ Identify cybersecurity-specific hiring flexibilities (e.g., hiring bonuses)
- ❑ Use the workforce planning tools and cybersecurity traits profiles included in this toolkit to identify target population characteristics, work preferences, technical background, and current cybersecurity trends to increase job interest

EVALUATE POTENTIAL SOURCES FOR THE TALENT PIPELINE

- ❑ Create a comprehensive list of current and potential recruiting alliances that align with organizational goals and resources (e.g., Centers for Academic Excellence (CAEs)), colleges, universities, cybersecurity competitions, and Veteran's transition programs)
- ❑ Prioritize where and how to recruit cybersecurity professionals (e.g. online job search engines, hackathon, cyber competitions, personal referrals, social media)
- ❑ Identify current cybersecurity employees who can engage with potential candidates at recruiting events (e.g., job fairs, campus recruiting events)
- ❑ Establish an employee referral program to recruit talented and trusted cybersecurity professionals from your cybersecurity employees' personal networks (e.g., colleges/universities, alma maters, professional associations)

DEVELOP MARKETING STRATEGY & MATERIALS

- ❑ Develop a list of advantages and benefits of the position(s) and your organization (i.e., selling points) to incorporate into outreach efforts and materials. Think about the trait profiles on the previous page to appeal to the best talent
- ❑ Highlight key technology, tools, and IT capabilities to attract the right cybersecurity talent for your organization's specific risk profile from page four of this kit
- ❑ Develop materials (e.g., slick sheets, job announcements, social media messages)
- ❑ Consider using interactive communication tools, such as social media (e.g., Twitter), that live where cybersecurity professionals do – the internet – to recruit Schedule and announce interaction opportunities (e.g. webinars, live Tweeting)

SELECT AND HIRE

- ❑ Use the cybersecurity trait profiles and interview questions provided in this toolkit to evaluate non-technical characteristics of cybersecurity professionals
- ❑ If a decision to hire candidate is made, create a competitive offer package to attract top cybersecurity talent, considering the development items in the next section

Develop Your People

Retain Staff at Every Level

Whether entry level, mid-career or seasoned cybersecurity professionals, here are some simple steps you can take to recognize, develop and retain staff at every level. Use the profiles below as a guide to understand which of the steps outlined in the Advance section will best support the specific type of cybersecurity professional your organization is looking to recruit and retain.

Entry-Level Cyber Professional	Mid-Career Cyber Professional	Seasoned or Executive Cyber Professional
• College, graduate, post-graduate, and career changers. New to cybersecurity. • Focused on learning cyber technical skillset and job requisites, acclimating to organizational environment, establishing support network, and gaining work experience.	• Professionals with previous cyber related experience and skills. • Focused on shaping career path and advancing technical skillset through job rotations, certifications, developing technology, and supervisory opportunities.	• Demonstrated cyber expertise and progressive leadership experience. • Focused on expanding technical expertise, making contributions to technical domain and broader cyber security community, and leadership development.
Tips to Retain Entry-Level Staff ❖ Foster an environment where diverse perspectives are welcome ❖ Encourage two-way dialogue for open communication ❖ Provide frequent feedback on job performance ❖ Ensure that cyber professionals have quality supervision and mentorship ❖ Provide opportunities to acquire new skills through established training, challenging job assignments, and career pathing ❖ Recognize staff for strong work performance	**Tips to Retain Mid-Career Staff** ❖ Emphasize work-life balance; encourage taking time to pursue activities and interests ❖ Provide opportunities to obtain advanced training and certifications ❖ Allow information sharing within the organization and professional forums ❖ Offer challenging job assignments ❖ Include employees in decision making and innovation ❖ Implement reward programs	**Tips to Retain Executive Staff** ❖ Provide advanced training and development opportunities ❖ Create tailored development plans that identify leadership competencies and areas for development ❖ Recognize leaders for their successes and accomplishments ❖ Consider performance and loyalty-based bonuses to retain staff ❖ Promote cyber executives to develop intellectual capital and create information sharing mechanisms

Help Your Staff Navigate Cybersecurity Careers

Once you have the cybersecurity team you need inside your organization, taking measures to grow and keep that staff is equally important. According to the 2015 (ISC)[2] Global Information Workforce study, approximately 20% of cybersecurity professionals changed employers in the past year. It's important HR professionals and cybersecurity managers work together to retain cybersecurity professionals, and help them develop career paths inside your organization. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Here are three (3) steps you can take to start building your organization's cybersecurity career path.

Step 1 – Familiarize yourself with proficiency levels and review sample career paths.

Sample Proficiency Levels

BEGINNER	INTERMEDIATE	SENIOR/EXPERT
Ability to apply basic knowledge and skills in simple work situations with specific instructions and/or guidance	Ability to apply knowledge and skills in straightforward, routine work situations with limited need for direction	Ability to apply advanced knowledge and skills in complex, difficult, or novel work situations; is an acknowledged authority, advisor, or key resource in a given topic

Sample Career Paths

CAREER PATH: BEGINNER LEVEL		
Suggested Experience & Credentials	Competencies and Sample Skills / KSAs	Suggested Training & Development Activities

Bachelor's Degree from an accredited program in a Computer Science-related
OR
2 years relevant work experience
	Technical Competencies & Sample KSAs
	• **Vulnerabilities Assessment**
	  ○ Skill in the use of penetration testing tools and techniques
	• **Information Security/Assurance**
	  ○ Skill in performing damage assessments
	General Competencies
	  ○ Critical Thinking & Analytical Skills
	  ○ Written & Oral Communication
		Sample Development Activities
		• University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon)
		• Government agency courses (e.g., IRM-NDU, NSA, DoD, Dept. of State DSTC, DHS certifications)

SAMPLE

A
D
V
A
N
C
E

CAREER PATH: INTERMEDIATE LEVEL		
Suggested Experience & Credentials	Competencies and Sample Skills / KSAs	Suggested Training & Development Activities

Bachelor's Degree from an accredited program in a Computer Science-related field plus 3 years of relevant work experience;
OR
6 years relevant work experience
Possession and demonstrated application of relevant certifications (as determined by the department/agency):
 	
Information systems security certifications (e.g., (ISC)^2 CSSLP and CISSP, various SANS certs, EnCase Cybersecurity suite, GIAC Security Essentials Certification (GSEC), and relevant programming languages
	Technical Competencies & Sample KSAs
	
	• **Vulnerabilities Assessment**
	  ○ Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
	  ○ Skill in the use of penetration testing tools and techniques
	• **Information Security/Assurance**
	  ○ Skill in performing damage assessments
	• **Computer Network Defense**
	  ○ Skill in detecting host and network-based intrusions
	
	General Competencies
	  ○ Critical Thinking & Analytical Skills
	  ○ Written & Oral Communication
		*None of the UMUC or SANS courses considered map to this specialty area at the Full Performance level
		
		Sample Development Activities
		• University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon)
		• Formal training programs/seminars (e.g., GIAC-Auditing Networks, Perimeters & Systems)
		• Government agency courses (e.g., IRM-NDU, NSA, DoD, Dept. of State DSTC, DHS certifications)
		• Joint Duty Assignments

SAMPLE

ADVANCE

CAREER PATH: SENIOR/EXPERT LEVEL		
Suggested Experience & Credentials	Competencies and Sample Skills / KSAs	Suggested Training & Development Activities

Master's Degree from an accredited program in a Computer Science-related field plus 5 years of relevant work experience;
OR
Bachelor's degree plus 10 years relevant work experience and project management experience
 	
Possession and demonstrated application of relevant certifications (as determined by the department/agency):
 	
PMP, Information systems security certifications (e.g., (ISC)² CSSLP and CISSP, various SANS certs, EnCase Cybersecurity suite, GIAC Security Essentials Certification (GSEC), ISACA Certified Information Security Manager Certification (CISM), SCNP), IT/Business Systems Audit certifications (e.g., CISA, GSNA), and relevant programming languages
	Technical Competencies & Sample KSAs
	
	• **Vulnerabilities Assessment**
	  ○ Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
	  ○ Knowledge of application vulnerabilities
	  ○ Skill in the use of penetration testing tools and techniques
	• **Information Security/Assurance**
	  ○ Skill in performing damage assessments
	• **Computer Network Defense**
	  ○ Skill in mimicking threat behaviors
	  ○ Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)
	
	General Competencies
	  ○ Critical Thinking & Analytical Skills
	  ○ Attention to Detail
	  ○ Creative Problem Solving
	  ○ Written & Oral Communication
	  ○ Project/Program Management
	  ○ Leadership & People Management
	  ○ Influencing/Negotiating
		Training – UMUC
		  ○ INFA660 Security Policy, Ethics and the Legal Environment
		
		Sample Development Activities
		  ○ University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon)
		  ○ Formal training programs/seminars (e.g., GIAC-Auditing Networks, Perimeters & Systems)
		  ○ Participation in community organizations and working groups (e.g., Federal Information Systems Security Educators Association (FISSEA), Information Systems Security Association (ISSA))
		  ○ Joint Duty Assignments
		  ○ Participation in professional associations, communities, practice or network groups in the field to share best practices, trends
		  ○ Developing white papers and policies
		  ○ Participating in professional coaching sessions, particularly for general competencies
		  ○ Participation in security and cyber relevant conferences (i.e. BlackHat, Defcon, Shmoocon, RSA, CANSEC West, others)

SAMPLE

Step 2 – Use the following template to create custom cybersecurity-specific career paths for your organization. Populate the **highlighted** fields with information that meets the needs of your organization (Competencies and KSAs can be found in the Workforce Framework)

CAREER PATH: *[LEVEL]*		
Suggested Experience & Credentials	Competencies and Sample Skills / KSAs	Suggested Training & Development Activities

[DEGREE] **from** ***[PROGRAM TYPE]*** **(plus)** ***[YEARS]*** **relevant work experience;**
OR
[YEARS] **relevant work experience**
Possession and demonstrated application of relevant certifications (as determined by the department/agency):
 	
[CERTIFICATIONS] **and/or relevant programming languages**
	Technical Competencies & Sample KSAs
	
	• ***[COMPETENCY]****
	  ○ *[RELATED KSAs]*
	• ***[COMPETENCY]***
	  ○ *[RELATED KSAs]*
	• ***[COMPETENCY]***
	  ○ *[RELATED KSAs]*
	
	General Competencies
	  ○ *[GENERAL COMPETENCY]*
	  ○ *[GENERAL COMPETENCY]*
		Training
		  ○ *[COURSE]*
		
		Sample Development Activities
		• *[UNIVERSITY PROGRAMS]*
		• *[FORMAL TRAINING PROGRAMS/SEMINARS]*
		• *[GOVERNMENT AGENCY COURSES]*
		• *[ACTIVITY]*
		• *[ACTIVITY]*

***Competency: The knowledge, skills, and abilities required to successfully perform a role or job function** **Example Competencies can be found in the Workforce Framework**		

Step 3 – Share career paths with cybersecurity managers and staff. Communications channels might include:

- Internal websites
- Employee communications
- Annual reviews

Professional Growth Opportunities for Your Cybersecurity Staff

In addition to career paths, your organization can provide a variety of professional growth opportunities to attract, engage, and retain cybersecurity professionals. Offering staff opportunities to think outside-the-box, solve complex cybersecurity challenges, and learn new cybersecurity skills may increase job satisfaction and improve retention. These opportunities also enable your staff to develop their skills for the quickly-evolving field of cybersecurity.

ADVANCE

TRAINING	• Direct all cybersecurity staff to more than 2,000 cyber training courses on the National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog Government cybersecurity staff and veterans also have access to free courses through the Federal Virtual Training Environment (FedVTE) - Post the following FedVTE Flyer in your workplace

CERTIFICATIONS	• Earning certifications enables staff to stay current on in-demand skills and become leaders in the cybersecurity field
	• Example Certifications:
	  ○ CompTIA SECURITY+
	  ○ Certified Information Systems Security Professional
	  ○ GIAC Security Essentials (GSEC)
	• Visit NICCS for more information on certifications

SHADOWING	• Staff gain on-the-job experience for a desired position • Encourage staff to connect with cybersecurity colleagues; shadowing is a great way to network and learn first-hand from others
MENTORING	• Encourage cybersecurity staff to establish mentoring relationships to learn from seasoned cybersecurity professionals

CONFERENCES & PROFESSIONAL ORGANIZATIONS	• Employees can stay up-to-date with developments in the field and network with fellow cybersecurity professionals
	• Example Conferences:
	  ○ NICE Conference & Expo
	  ○ RSA Security Conference
	  ○ NSA Information Assurance Symposium
	• Example Professional Organization:
	  ○ Information Systems Security Association

CYBERSECURITY AWARENESS	Stop.Think.Connect.™ • National public awareness campaign aimed at increasing the understanding of cybersecurity threats and empowering all Americans to be safer and more secure online. Resources are available at www.dhs.gov/stopthinkconnect • October is National Cyber Security Awareness Month. Learn more at www.dhs.gov/national-cyber-security-awareness-month
TOP CYBERSECURITY SCHOOLS	• Centers for Academic Excellence (CAE) in Information Assurance/Cyber Defense: DHS/NSA designated over 190 institutions where employees can pursue degrees • For more information visit the CAE Site or email askCAEIAE@nsa.gov • The Scholarship for Service (SFS) provides funding to full-time students in exchange for government service. Learn more here

TELL US WHAT YOU THINK

The field of cybersecurity is ever-changing. If you have ideas on additional resources that will help you plan for, build, and advance your cybersecurity workforce, please email us at niccs@hq.dhs.gov.

Homeland Security

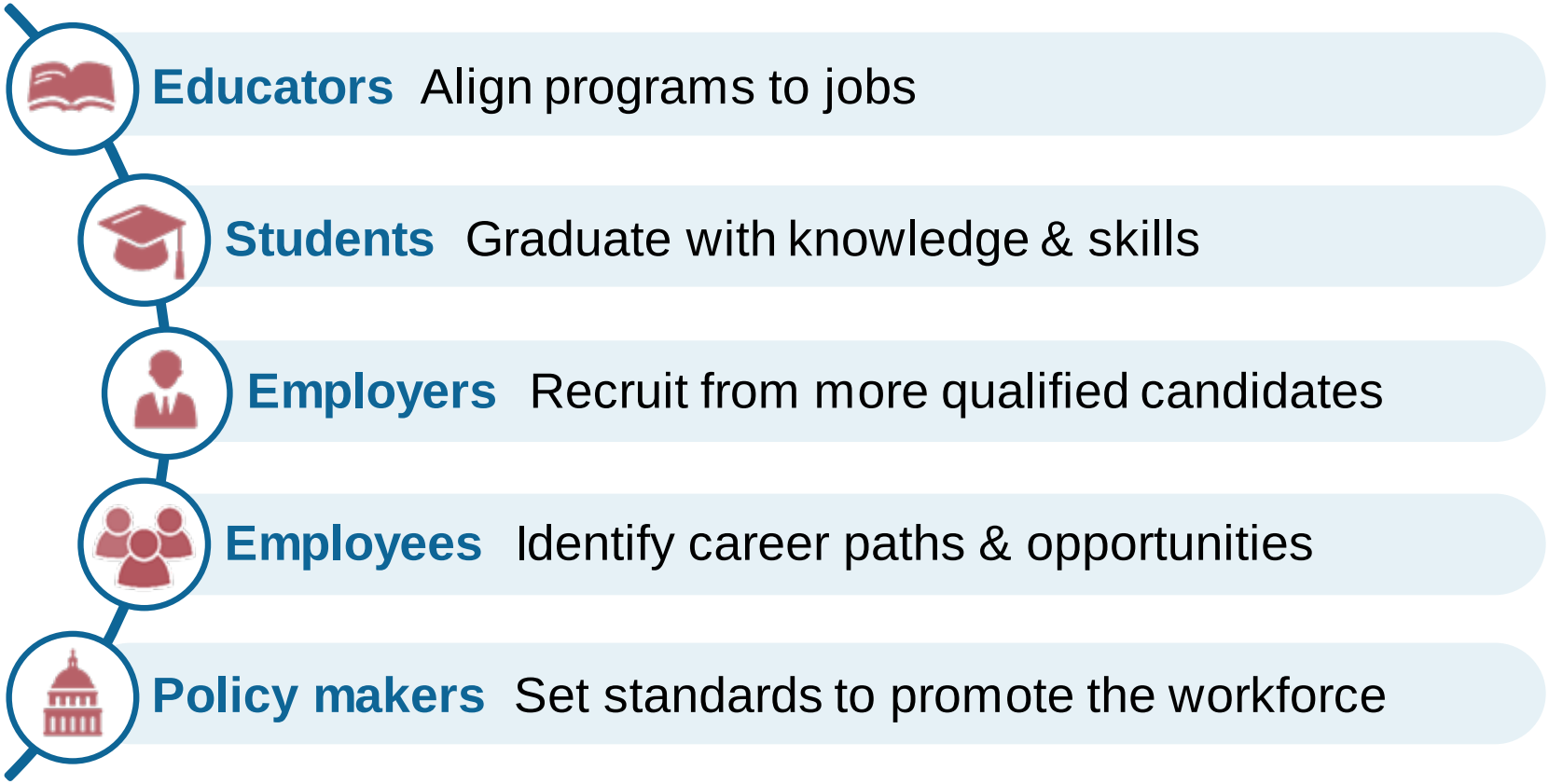
Cyber Workforce Development Best Practices

Benjamin Scribner
Department of Homeland Security (DHS)
National Cybersecurity Education & Awareness Branch (CE&A)

March 2016
CSRIC FCC Cybersecurity Workforce Working Group

Cybersecurity: Why it Matters

Vision for the Nation's Cyber Workforce



The Foundation for our Nation's Cyber Workforce

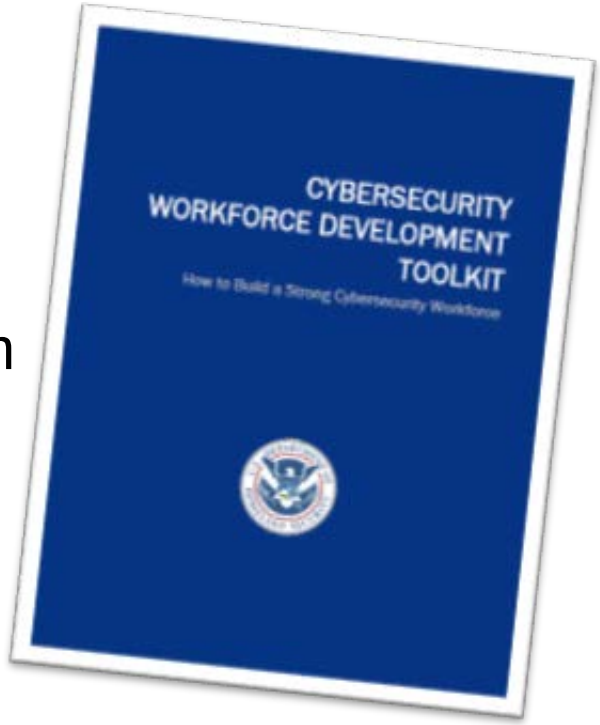
The National Cybersecurity Workforce Framework

- 7 Categories, 30+ Specialty Areas
- Baselines knowledge, skills, and abilities & tasks
- Support for strategic workforce development

Creating a Strong Cybersecurity Team

The Cybersecurity Workforce Development Toolkit equips you with resources to:

- ✓ **PREPARE** for workforce development
- ✓ **PLAN** your cybersecurity workforce
- ✓ **BUILD** a high-performing cybersecurity team
- ✓ **ADVANCE** cybersecurity staff with career development opportunities



Available online at niccs.us-cert.gov/

Prepare for Workforce Planning

Assess Your Workforce Planning Readiness

- ✓ Establish a vision for your cybersecurity workforce
- ✓ Use the Cybersecurity Workforce Planning Capability Maturity Model (CMM) to assess your organization's workforce planning readiness

3 Workforce Planning Maturity Levels

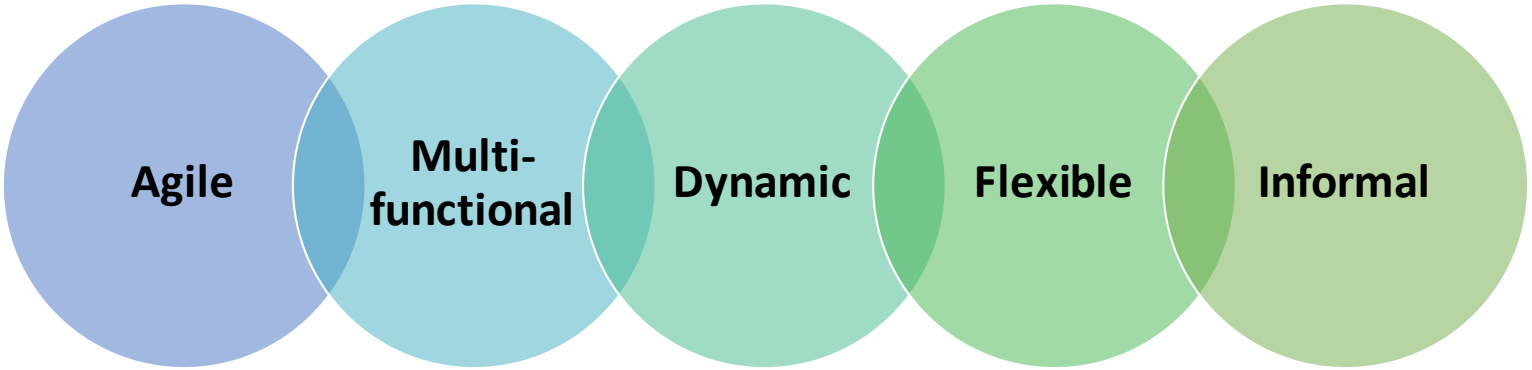
LIMITED PROGRESSING OPTIMIZING

Plan for Your Cybersecurity Team

How to Plan for Your Team

- ✓ Understand your cybersecurity risk exposure and tolerance using the Cybersecurity Workforce Planning Diagnostic
- ✓ Inventory your cybersecurity workforce
- ✓ Determine and address gaps

Characteristics of High-Performing Cybersecurity Teams



Build a High-Performing Cybersecurity Team

What Should a Cybersecurity Team Look Like?

- ✓ Align positions to the Workforce Framework
- ✓ Learn non-technical traits of cybersecurity professionals
- ✓ Use the recruitment checklist to hire top talent

Template – Align Positions to Workforce Framework

Position Title	*[Fill in Position Title]*
Primary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Secondary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Current Tasks Performed (i.e., specific job duties) – see general role examples in Workforce Framework Employer User Guide for sample wording	
Additional Tasks recommended by Specialty Area	

Advance Your Staff

Develop Your People

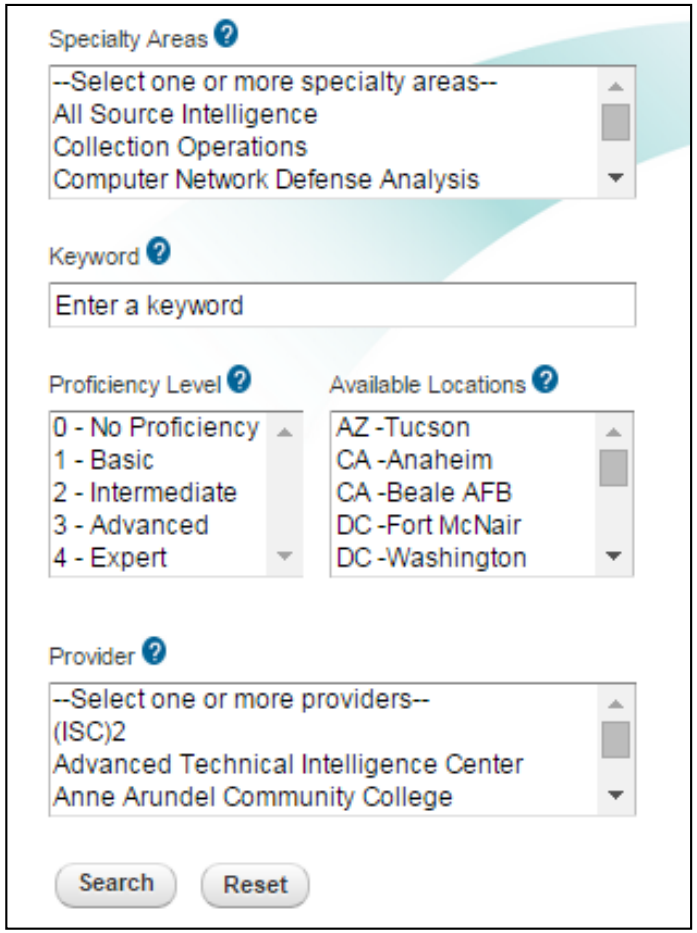
- ✓ Take steps to retain staff at every level
- ✓ Develop career paths to help your staff navigate their careers
- ✓ Discover continuous development opportunities

Customize Sample Career Paths Based on Level
(e.g., Beginner, Intermediate, Expert)

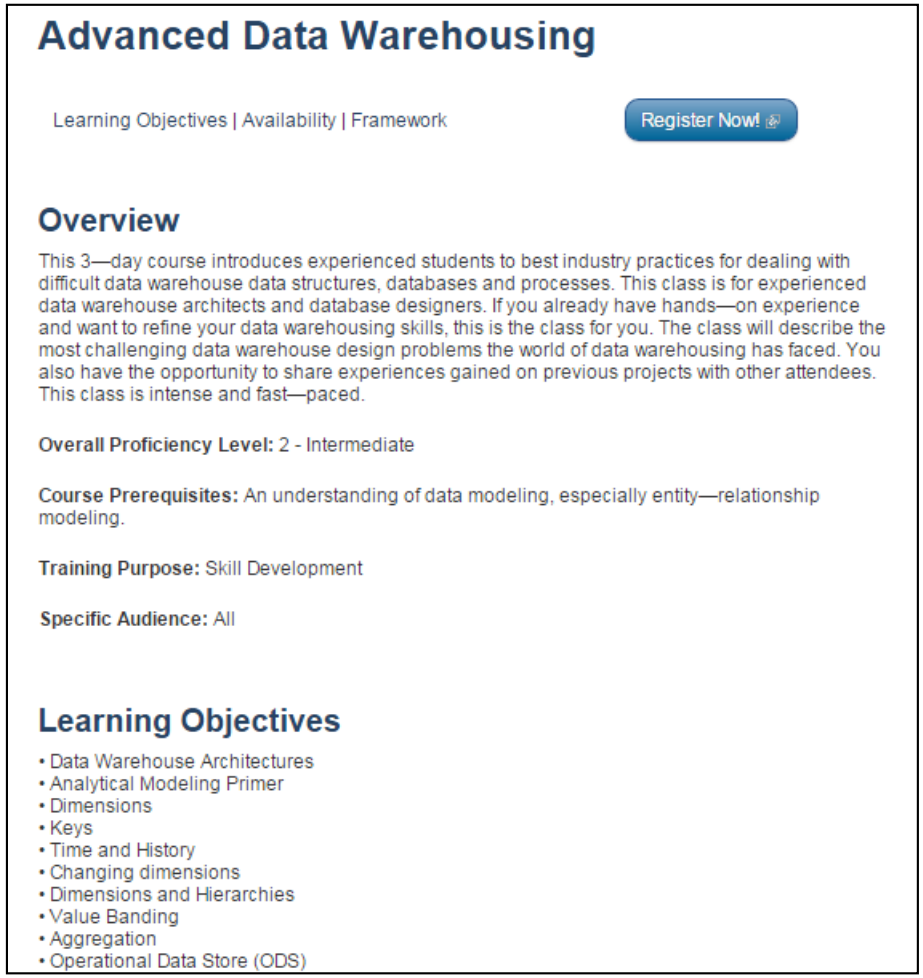
CAREER PATH: BEGINNER LEVEL		
Suggested Experience & Credentials	Competencies and Sample Skills / KSAs	Suggested Training & Development Activities
Bachelor's Degree from an accredited program in a Computer Science-related OR 2 years relevant work experience	**Technical Competencies & Sample KSAs** • **Vulnerabilities Assessment** o Skill in the use of penetration testing tools and techniques • **Information Security/Assurance** o Skill in performing damage assessments **General Competencies** o Critical Thinking & Analytical Skills o Written & Oral Communication	**Sample Development Activities** • University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon) • Government agency courses (e.g., IRM-NDU, NSA, DoD, Dept. of State DSTC, DHS certifications)

Training for Cyber Professionals

Search Courses



View Course Information



Advanced Data Warehousing

Learning Objectives | Availability | Framework

Register Now!

Overview

This 3—day course introduces experienced students to best industry practices for dealing with difficult data warehouse data structures, databases and processes. This class is for experienced data warehouse architects and database designers. If you already have hands—on experience and want to refine your data warehousing skills, this is the class for you. The class will describe the most challenging data warehouse design problems the world of data warehousing has faced. You also have the opportunity to share experiences gained on previous projects with other attendees. This class is intense and fast—paced.

Overall Proficiency Level: 2 - Intermediate

Course Prerequisites: An understanding of data modeling, especially entity—relationship modeling.

Training Purpose: Skill Development

Specific Audience: All

Learning Objectives

- Data Warehouse Architectures
- Analytical Modeling Primer
- Dimensions
- Keys
- Time and History
- Changing dimensions
- Dimensions and Hierarchies
- Value Banding
- Aggregation
- Operational Data Store (ODS)

FedVTE

DHS offers free cybersecurity training for U.S. government and veterans!

- ✓ Available to Federal, State, Local, Tribal, and Territorial government and US veterans!
- ✓ Courses ranging from beginner to advanced levels
- ✓ 55,000+ active users
- ✓ 42 courses and growing. Popular courses include certification preparation for the following exams:
  - Network +
  - Security +
  - Certified Information Systems
  - Security Professional
  - Certified Ethical Hacker

Fedvte.usalearning.gov

NICCS™ Website

The Nation's One Stop Shop for Cybersecurity Careers and Studies!

- ✓ 28,000+ visitors per month
- ✓ 2,000+ courses in the NICCS Training Catalog mapped to the National Cybersecurity Workforce Framework
- ✓ 100+ links to cybersecurity resources
- ✓ 15+ tools for managers, including a Cybersecurity Workforce Development Toolkit
- ✓ 10+ monthly events
- ✓ 10+ links to customized job searches

…and more coming soon!

niccs.us-cert.gov

How to Reach Us

Kristina Dorville

Branch Chief, Cybersecurity Education & Awareness (CE&A)

Phone: (703) 235-5281

Email: kristina.dorville@hq.dhs.gov

Benjamin Scribner

Director, CE&A Professionalization & Workforce Development Program

Phone: (703) 235-5293

Email: benjamin.scribner@hq.dhs.gov

National Cryptologic School
NSA/CSS Learning

Building the Cyber Workforce Pipeline: Preparing for Tomorrow and the Day After Tomorrow

GenCyber and the Centers of Academic Excellence in Cybersecurity

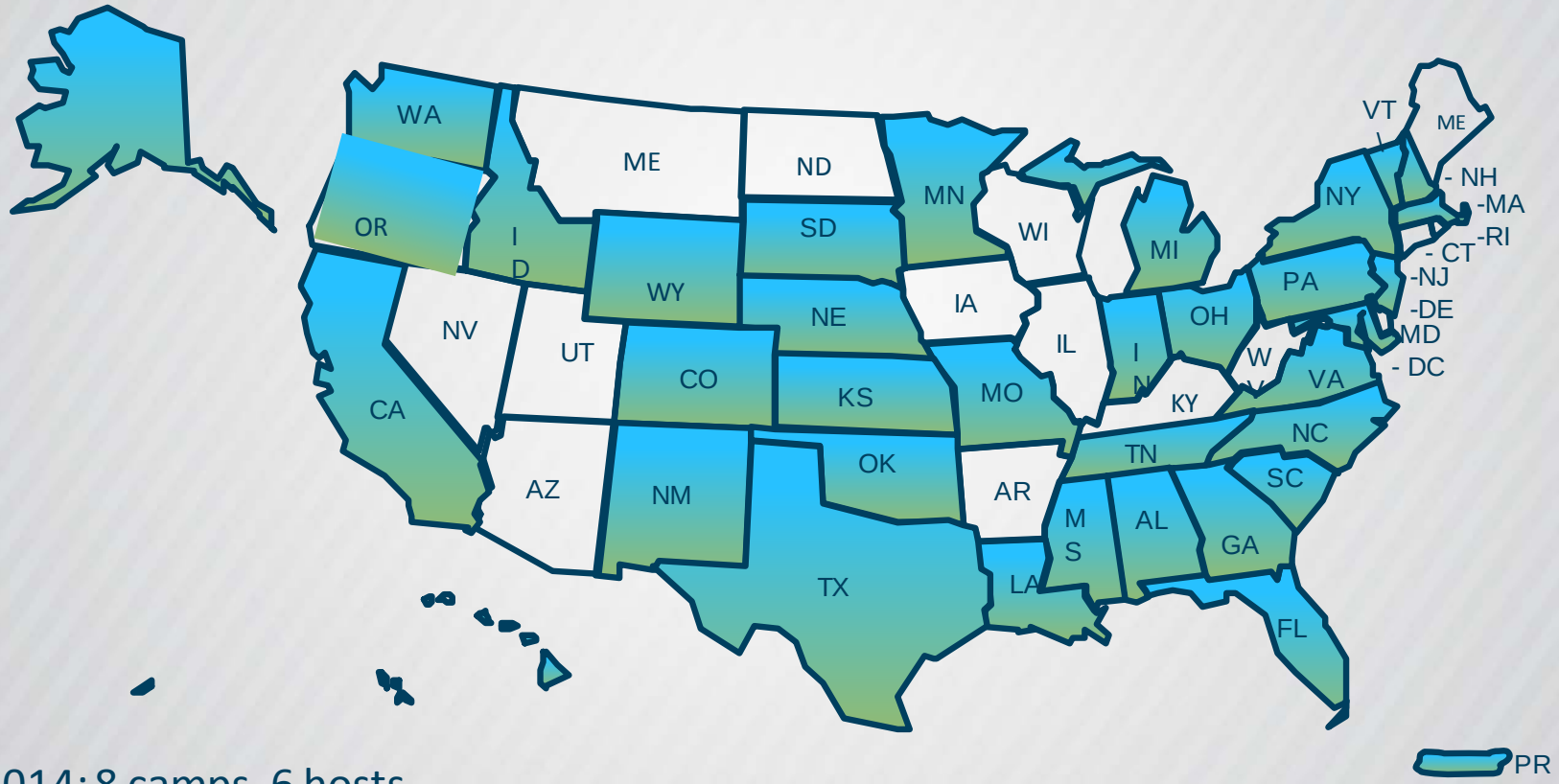
Emphasis on Workforce

- Burning Glass study on Cybersecurity Workforce
  - 84% of job postings require at least a BA or BS
  - Only 17% accept less than 2 years experience
  - 10% require a security clearance
  - Volume of listings increased 91% from 2010 to 2014
- CAE-CD placing emphasis on educating students as preparation for careers
- Mapping to DHS/NICE Cybersecurity Workforce Framework

GenCyber

- Summer Camps for K-12 students and teachers
- 1-2 weeks, residential/non-residential
- Computer background not required
- Provided at no cost to the participants
- Awareness
- Increase interest in cybersecurity
- Improve teaching methods

2016 GenCyber Camps



2014: 8 camps, 6 hosts

2016: 133 Camps, 68 hosts,

In three years, 6000+ Students/Teachers

www.gen-cyber.info

Centers of Academic Excellence (CAE) *Purpose*

CAE IN CYBER DEFENSE (CAE-CD)

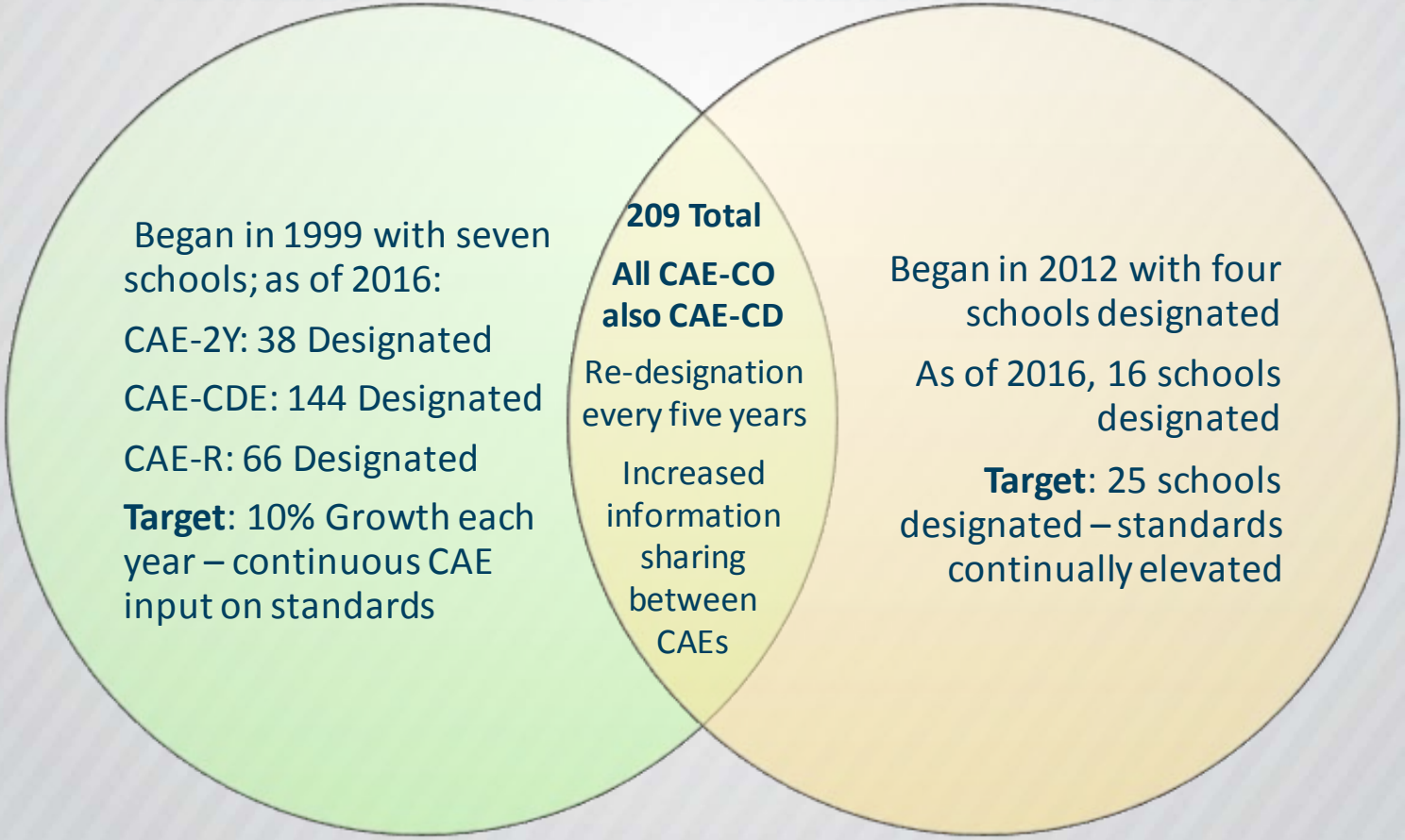
- Meet National workforce needs
- Reduce vulnerability in our national information infrastructure
- Promote higher education and research in IA/CD
- Produce a growing number of professionals with cybersecurity expertise for the Nation

CAE IN CYBER OPERATIONS (CAE-CO)

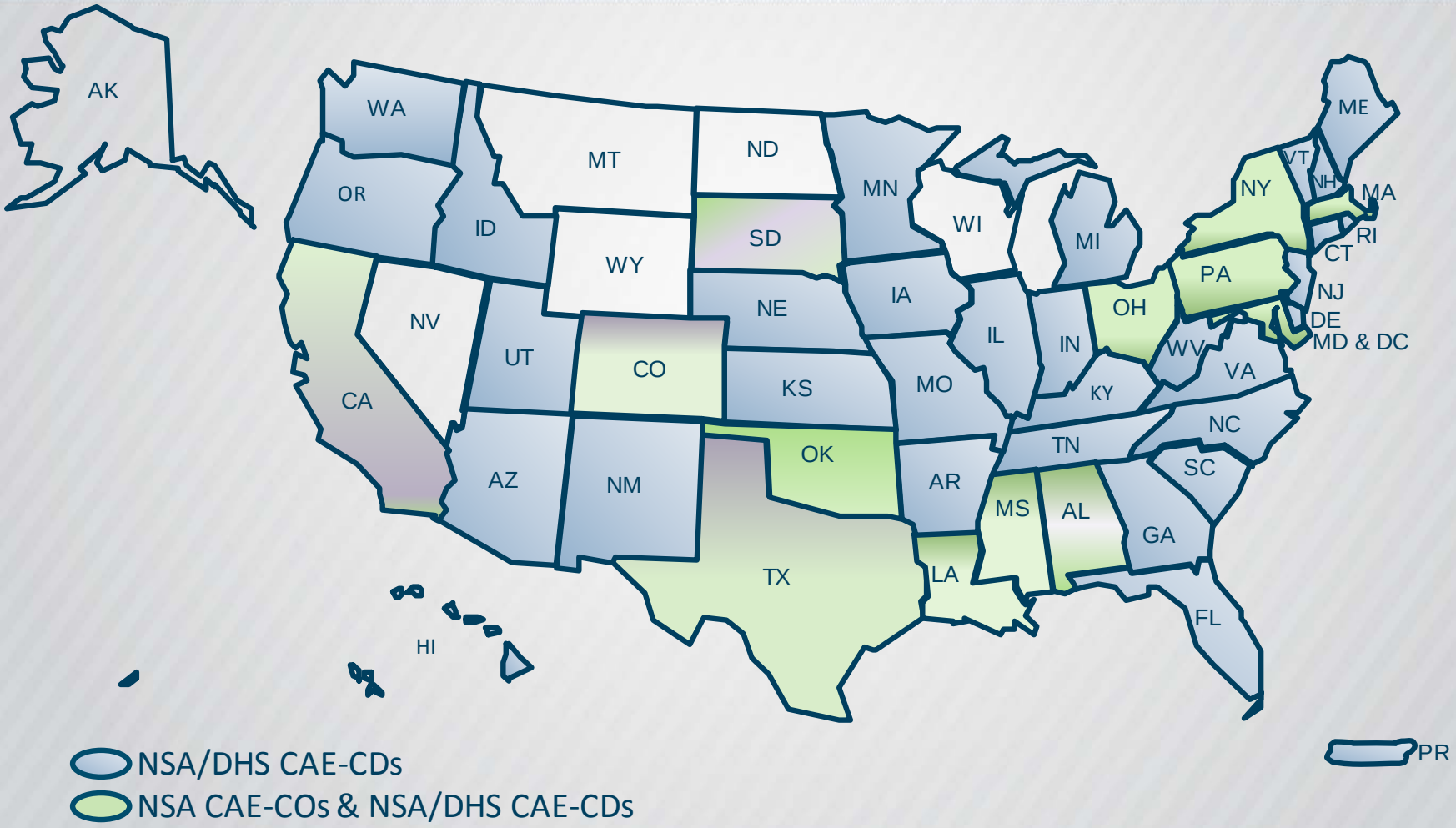
Creating the workforce NSA and DoD need

- Deeply technical, inter-disciplinary, BS/MS level
- Grow workforce pipeline for NSA and DoD
- Enhance the national security posture of our Nation
- CAE-CO offers a 12 week summer internship

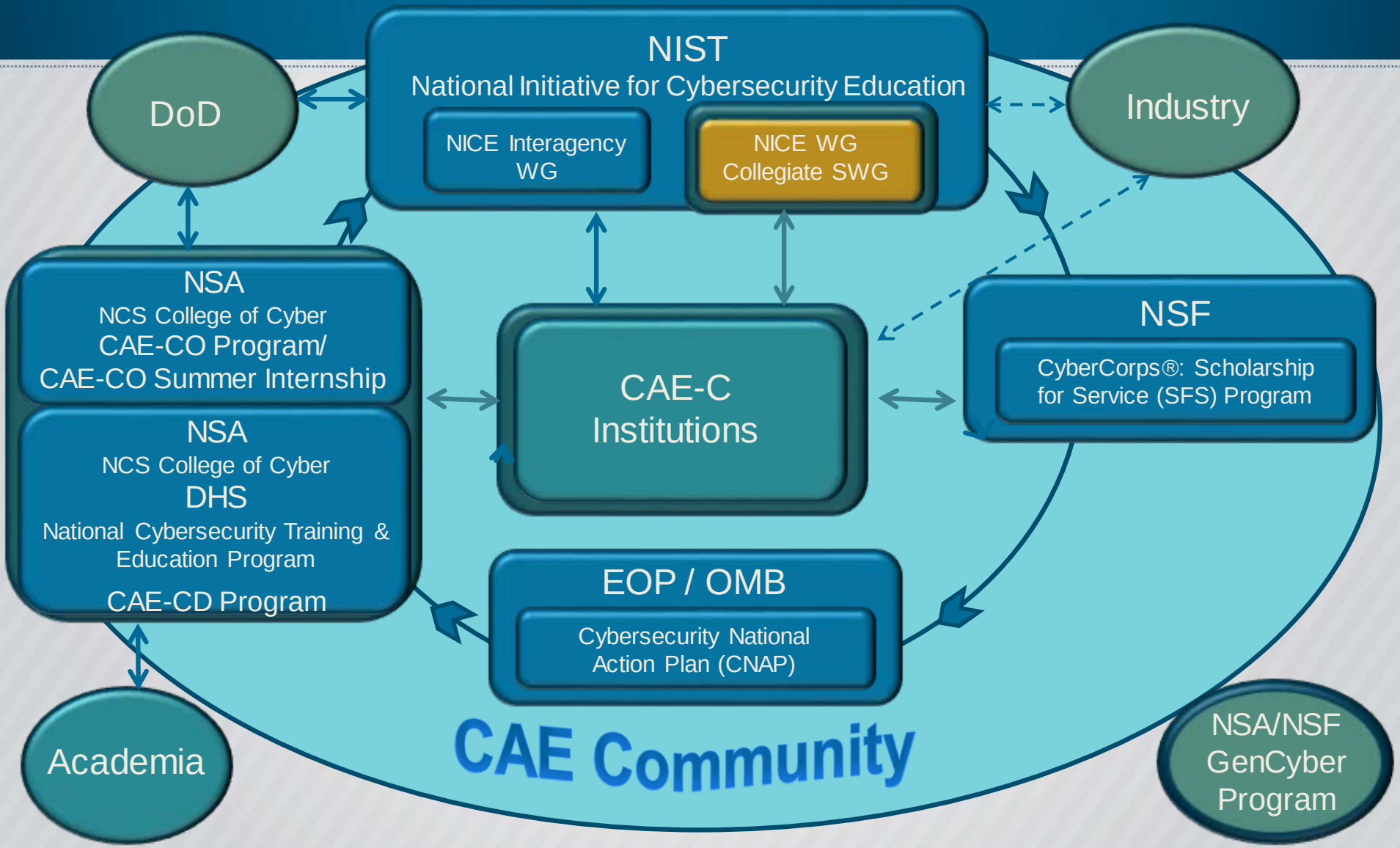
Creating Tomorrow's Workforce



CAE-C Designated Institutions



CAE-C Program Partnerships



CAE Impact

"300% enrollment increase"

"Stopped State Funding Cuts"

"Increased opportunities for NSF grants"

"Influencing regional collegiate programs and outreach activities"

"Increased contact from government and industry seeking partnerships"

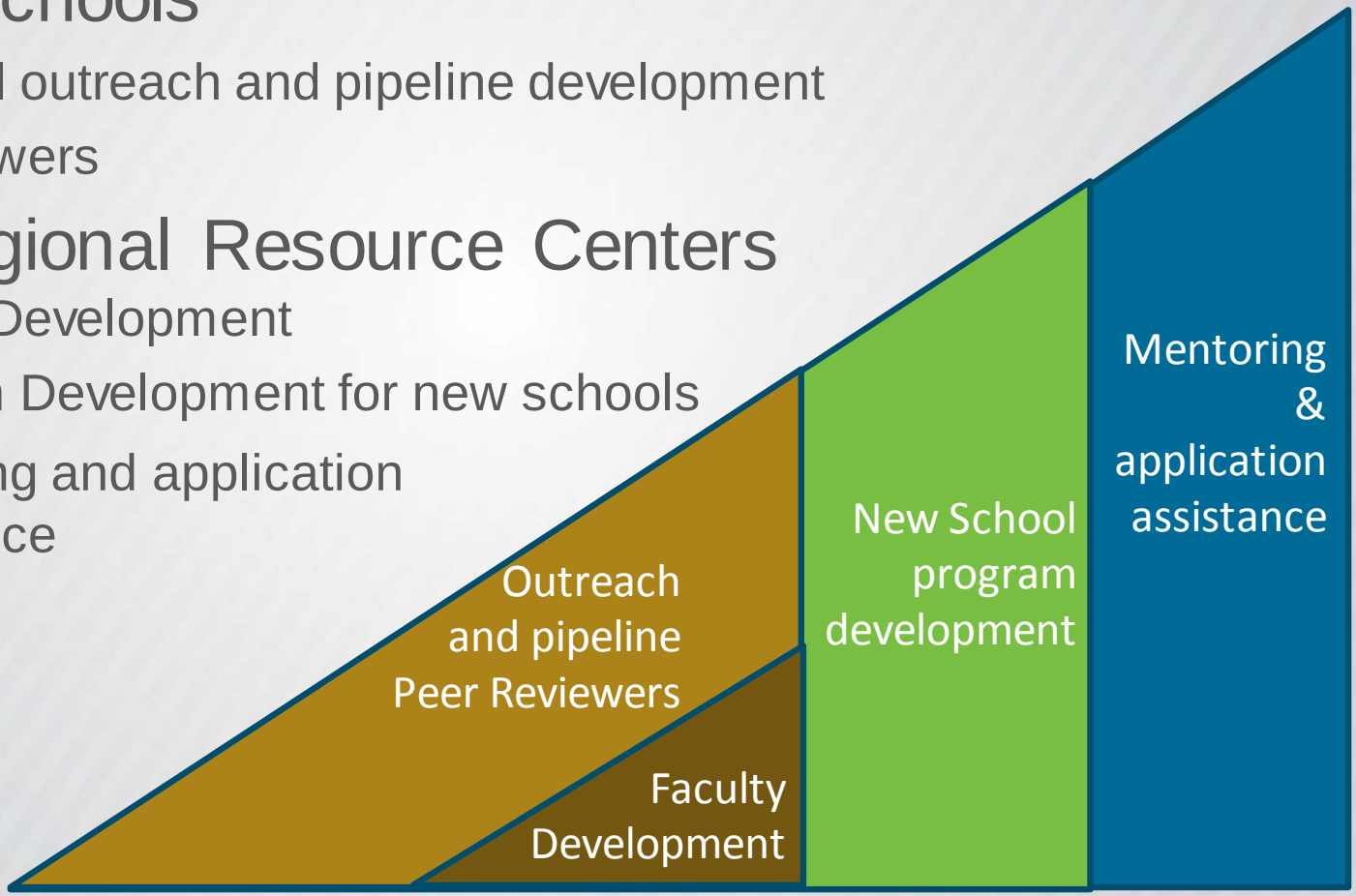
"Collegiate level Red Team vs. Blue Team exercises between CAE-CO schools"

"Administration support to increase faculty and programs for Cyber Operations curriculum"

"Chosen by State government to consult on Cyber Security Councils "

CAE-CD Program Expansion

- CAE-CD Schools
  - High school outreach and pipeline development
  - Peer Reviewers
- CAE Regional Resource Centers
  - Faculty Development
  - Program Development for new schools
  - Mentoring and application assistance



Additional Information

CAE in Cyber Operations Program Office

- https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/
  - AskCAECyberOps@NSA.gov 410-854-6535

CAE in Cyber Defense Program Office

- https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
  - askCAEIAE@NSA.gov 410-854-6206

Cybersecurity

Defending our Information Assets from an Ever Increasing Threat

---

Authored by

Burning Glass Technologies

BATEC National Center of Excellence in Computing and Information Technologies

Published

January 2016

This report was prepared with support from the National Science Foundation under grant DUE-110415 to the University of Massachusetts. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the editor and the principal investigators of the BATEC ATE Center. They do not necessarily reflect the views of the National Science Foundation.

© Copyright 2016

FORWARD

There is a natural partnership between business and academia when it comes to workforce development.

- Corporate entities depend on a robust supply of qualified and capable workforce talent in order to grow their business and achieve their strategic objectives.

- Educational institutions have an implied contract with their students, promising them meaningful employment upon attainment of their degree credentials.

This partnership, though critically important, is particularly challenging in fields where the discipline is an emerging, tools, paradigms and best practices are still in development, and experience is relatively limited.

CyberSecurity is a new and emerging discipline that exhibits all of these characteristics. Moreover, it is a discipline which is critically important as the integrity and availability of our information infrastructure depends on it. Our computers, our databases and our networking platforms are under constant attack, and the stakes are quite high.

We've all been "hacked" at one time or another, and received some junk email, spam content, or annoying virus. We might categorize this experience as simply inconvenient and annoying. Corporate Cybercrime is, however, another matter. Strategic, intentional, and harmful attacks on corporate information resources can be costly, paralyzing and significant. World renowned experts forecast, without hesitation, that our next global conflict, "World War III", will be fought in Cyberspace.

This report, and the analysis contained herein, is both timely and valuable in its ability to enhance discussion, dialogue and collaboration between industry and academia about the emerging and pervasive discipline of CyberSecurity. This report analyzes the dimensions of the career pathway (number of jobs, average compensation, and geographical distribution of jobs) and the requirements of the employment opportunity (job responsibilities, technical and soft skill proficiencies).

It is our hope that this report will aid in the development of dynamic, innovative academic programs and a pipeline of workforce talent that support the industry needs for trained professionals. CyberSecurity is the hottest and most important discipline to take center stage in the next decade.

Lou Piazza

Lou Piazza
Director, BATEC

Contents

FORWARD
INTRODUCTION 1
THE TOP EIGHT THINGS YOU NEED TO KNOW 2
APPROACH AND METHODOLOGY 3
DETAILED FINDINGS 4
Occupational Categories and Representative Job Titles 5
Summary Statistics 6
Educational Requirements 7
Experience Requirements 8
Career Pathways and Transitions 8
Opportunities for Veterans 10
IMPLICATIONS AND RECOMMENDATIONS 12
SPECIFIC PROFILES 13
Engineer 13
Manager 20
Analyst 26
Specialist 33
Architect 40
Auditor 47
Consultant 54
REGIONAL ANALYSIS 61
Bay Area 61
Boston 61
Chicago 62
Miami 62
New York 63
Southern Ohio 63
Washington, D.C 64
ACKNOWLEDGEMNTS 65

INTRODUCTION

The economic, privacy, and national security concerns stemming from rising cybersecurity threats are among the most critical issues facing the United States today. Cyber-related attacks have risen 38%[1], and all indicators suggest that the workforce needs in cybersecurity are a growing challenge for most employers as CyberSecurity job postings remain unfilled 21% longer than the most other jobs.

A workforce shortage in CyberSecurity talent has far reaching implications for our national, economic, and personal security. Mitigating this shortage will require coordination between a multitude of stakeholders, including employers, educators, and policymakers.

Some important initiatives are already underway – perhaps most notably, the National Initiative for Cybersecurity Education (NICE) has developed a framework to describe and profile the CyberSecurity workforce and improve Cyber literacy[2]. The Center for Academic Excellence (CAE) Initiative, jointly sponsored by the National Security Administration (NSA) and the Department of Homeland Security (DHS), is aimed at increasing access to the academic pathway in CyberSecurity.

This report, produced by Burning Glass Technologies and Broadening Advanced Technological Education Connections (BATEC), aims to facilitate dialog among the aforementioned stakeholders providing a data-driven analysis of employment opportunities across the cybersecurity jobs landscape. It documents the workforce need and maps it into a set of cybersecurity academic pathway, describing the opportunities for workers to enter and advance within the field.

The field of CyberSecurity features both great promise and significant challenge. It promises high-demand, high-growth, and high-paying careers for skilled professionals, while threatening grave consequences if the workforce needs are not rapidly and effectively addressed.

The field of CyberSecurity is pervasive, and our national, economic and personal security is only as strong as the weakest link, the most vulnerable component. The principles of secure programming, network administration, digital forensics and information assurance will, and should, find their way into every computer-related academic pathway, and every IT-related job description.

We know that the status quo is not adequate to address the future needs of our nation. We hope that you find the information contained within this report informative and actionable, and encourage you to review it, discuss it, and debate it with stakeholders in your local geographical area. The integrity and privacy of our digital assets depends upon in.

[1] The Global State of Information Security Survey 2016. PwC.

[2] National Cybersecurity Workforce Framework.

THE TOP TEN THINGS YOU NEED TO KNOW…

1. The field of CyberSecurity is pervasive. Cyber-related skills are finding their way into every job in Information Technology, Digital Networking, and Computer Programming.
2. The cybersecurity job landscape is large and growing, and offers strong employment opportunities across the economy. There were 238,158 online job postings, in 2014, for cybersecurity job postings in the United States. This represents a 91% increase in the four year period 2010 to 2014.
3. CyberSecurity job postings remain open longer (8% longer than IT jobs overall) suggesting that these jobs are harder to fill than IT jobs in general.
4. CyberSecurity jobs pay well. The average advertised salary for these jobs is almost $84,000 – well above the average for all IT roles.
5. Cybersecurity jobs break into seven key broad categories (listed in order of employer demand): Engineers, Managers, Analysts, Specialists, Architects, Auditors, and Consultants.
6. The strongest growth in job postings is for the entry level roles of Specialist, Analyst and Auditor. These positions work in operations and defend information resources on a day-by-day basis.
7. Workforce opportunities in cybersecurity exist for job seekers of all educational levels. Candidates, with appropriate skills but not a bachelor's degree, can enter the workforce in the Specialist category where 37% of the positions do not require a four-year degree. A career in CyberSecurity does, however, require a commitment to continued education as the majority of positions require a Bachelor's Degree and many high paying positions require a Master's Degree.
8. The career pathway in CyberSecurity has reasonable definition. The job categories of Specialist and Analyst provide entry level opportunities for candidates with modest skills. The job category of Engineer provides economic incentive for continued educational achievement and skill development. The job categories of Manager, Architect and/or Consultant are the highest paying opportunities and require advanced training, experience, and/or certification.
9. There is a career transition opportunity for returning veterans. Many corporate CyberSecurity roles require similar competencies to those required in the military, and require security clearances which veterans either have in their possession or have experience qualifying for.
10. The workforce challenge can be best addressed when employers, educators, and policymakers work together in close collaboration. A shared vision and mutual understanding of the requisite skills, academic credentials and industry certifications required of a qualified candidate can empower educators to properly prepare an entry level workforce.

APPROACH AND METHODOLOGY

Burning Glass drew from its detailed database of online employer demand, which includes over 90 million current and historical job postings, to conduct this analysis. Burning Glass surveys postings from approximately 40,000 online job sites, extracting from each posting top-line information such as title, employer and industry. Duplicate postings are systematically eliminated; unique job postings are further analyzed. An artificial intelligence engine then reads each job description identifying job titles, skills, qualifications, and certifications.

Job postings requesting core cybersecurity job titles (e.g. information security analyst), skills (e.g. cryptography), or certifications (e.g. CISSP), were extracted from this database of online employment demand. These postings form the basis of the cybersecurity definition used throughout the report, and are heretofore referred to as "the CyberSecurity jobs".

The Cybersecurity jobs were grouped into categories based upon functional similarities. These categories were analyzed and compared across multiple factors, including magnitude of demand, skill and certification requirements, required education and suggested experience to understand the key dynamics shaping the employment ecosystem. The average length of time that job postings remained open was also calculated in an attempt to assess the relative difficulty that employers experience in filling these positions.

The dimensions (number of jobs, 4 year growth, average salary, duration of posting, and workforce density) was measured, and reported, both nationally, and regionally (in each of the following Metropolitan Statistical Areas (MSAs):

Bay Area[3]	Miami	Southern Ohio[4]
Boston	New York City	Washington D.C.
Chicago		

Burning Glass also surveyed the contents of its resume database analyzing almost 60 million career transitions. This results of this survey were used to document how, and when, workers move from one job category to another, and which skills and credentials trigger the opportunity for career advancement.

An internal catalog of mappings between military and civilian occupations was used to assess the opportunity for returning veterans to enter cybersecurity workforce. These mappings use skill requirements and on-the-job duties to define functional equivalency between military and civilian occupations.

Unless otherwise noted, all data in this analysis pertains to the calendar year 2014.

[3] Bay Area includes the Metropolitan Statistical Areas (MSAs) of San Francisco and San Jose

[4] Southern Ohio includes the MSAs of Springfield, Dayton, Cincinnati and Columbus

DETAILED FINDINGS

The CyberSecurity job landscape is large and growing, and offers strong employment opportunities across the economy. There were 238,158 online job postings in 2014, representing an increase of 91% since 2010. This robust growth has helped to make cybersecurity jobs are harder to fill than the industry norm. On average, cybersecurity jobs remained open for 40 days in 2014 – 8% longer than IT jobs overall.

CyberSecurity jobs are among the highest paying IT-related jobs. The average advertised salary is almost $84,000 – well above the average for comparable non-Cyber related jobs.

The resulting pressure on employers to attract and retain top cyber talent has driven average advertised salaries up to almost $84,000 – well above the average for all IT roles.

Our analysis of the CyberSecurity online postings suggests a segmentation of seven job categories, which account for 90% of the cybersecurity job openings and form a career pathway that employers, educators and job seekers can follow in their discussion about and focus their efforts in development of the cybersecurity workforce.

The table on the following page lists these categories (sorted by employer demand) with a description and set of representative titles.

There has been strong growth for entry-level roles, specifically in the two categories of Specialist and Analyst. These individuals work on operational teams involved in the day-to-day defense of information assets. Job postings, in each of these categories grew by more than 95% growth during the four year period, 2010 to 2014.

The largest job category, in terms of overall demand, was in the category Engineer. These individuals build and maintain the IT infrastructure (computers, networks, storage systems). The four year growth in this category was robust at 55%, but much less than the 91% growth rate experienced broadly across all cybersecurity jobs.

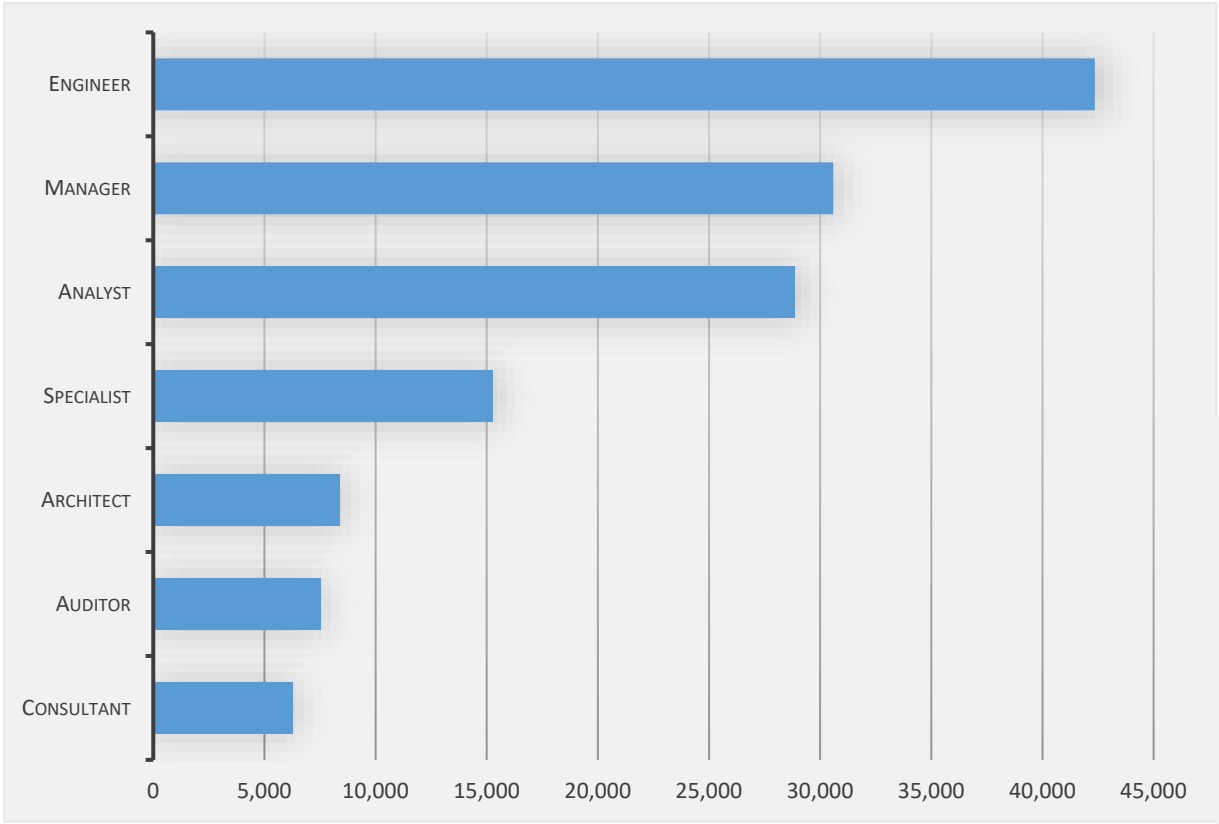
The greatest growth has been in the category Auditor. These individuals evaluate the preparedness of the information security systems. The growth rate (132% during the four year period 2010 to 2014) is a challenge for employers as they try to recruit from a constrained pool of talent. Job postings for this category remained open the longest of any CyberSecurity job category (43 days on average)

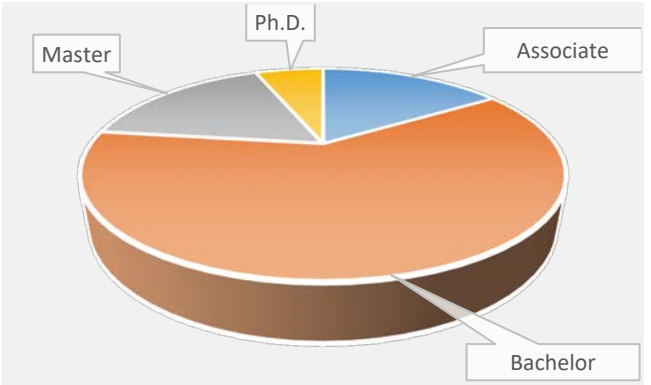
The most advanced roles are in the categories of Consultant, Engineer and Architect. The educational and certification requirements are significant for these roles, and they command the highest salaries of $95,311, $97,620, and $112,659, respectively.

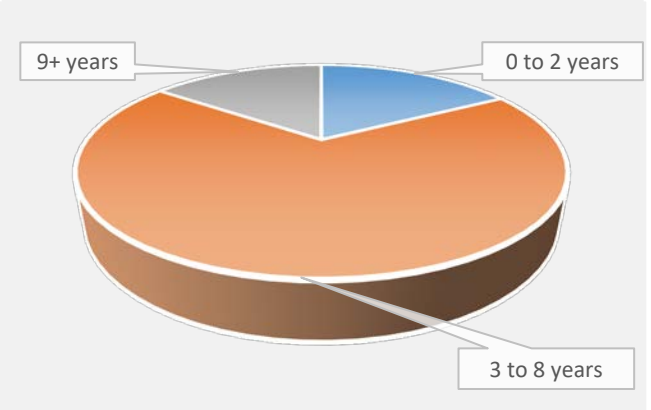
Occupational Categories and Representative Job Titles

Category & Description	Sample Job Titles
Engineer *Builds and maintains information security solutions for an organization's IT infrastructure.*	*Security Engineer* *Network Engineer* *Systems Engineer* *Software Development Engineer* *Network Security Engineer*
Manager *Develops and manages an organization's information security operations and infrastructure.*	*Systems Administrator* *Security Manager* *Network Administrator* *Security Administrator* *Information Security Manager*
Analyst *Detects and prevents cybersecurity threats by identifying weaknesses in an organization's information security.*	*Security Analyst* *Information Security Analyst* *Information Technology Security Analyst* *Compliance Analyst* *Operations Analyst*
Specialist *Implements, tests, and monitors an organization's information security systems.*	*Security Specialist* *Information Technology Specialist* *Information Security Specialist* *Network Specialist* *Cyber Security Specialist*
Architect *Oversees the design and implementation of an organization's information security systems.*	*Security Architect* *Solutions Architect* *Network Architect* *Enterprise Architect* *Information Security Architect*
Auditor *Conducts security audits to assess the effectiveness of an organization's information security protocols and infrastructure.*	*Information Technology Auditor* *Internal Auditor* *Staff Auditor* *Internal It Auditor* *It Auditor*
Consultant *Provides advice to inform the design and implementation of an organization's information security solutions.*	*Security Consultant* *Information Security Consultant* *Information Technology Consultant* *Technical Consultant* *Technology Consultant*

CyberSecurity Job Postings (238,158 Total)







Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**238,158**	**91%**	**$83,934**	**40 Days**
Engineer	42,355	55%	$97,620	42 Days
Manager	30,586	80%	$90,262	41 Days
Analyst	28,853	100%	$78,898	38 Days
Specialist	15,289	97%	$80,847	35 Days
Architect	8,409	95%	$112,659	37 Days
Auditor	7,533	132%	$80,750	43 Days
Consultant	6,294	44%	$95,311	31 Days

Professionals can enter the CyberSecurity workforce most easily in the job category of Specialist where there is a minimal educational requirement (37% of the postings are eligible to professionals with only 2 years of college education) and a minimal experience requirement (44% of the postings are eligible to candidates with less than 2 years of work experience.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Overall	**38,073 (16%)**	**145,243 (61%)**	**40,918 (17%)**	**13,938 (6%)**
Engineer	7,082 (17%)	27,879 (66%)	5,591 (13%)	1,803 (4%)
Manager	4,245 (14%)	19,913 (65%)	5,251 (17%)	1,177 (4%)
Analyst	3,316 (11%)	21,514 (75%)	3,223 (11%)	799 (3%)
Specialist	5,639 (37%)	6,717 (44%)	1,364 (9%)	1,569 (10%)
Architect	1,617 (19%)	4,422 (53%)	1,981 (24%)	389 (5%)
Auditor	74 (1%)	4,907 (65%)	2,055 (27%)	496 (7%)
Consultant	671 (11%)	4,388 (70%)	1,076 (17%)	158 (3%)

Beyond the role of Specialist, entry into, and advancement within, the CyberSecurity workforce requires a commitment to both education and experience. Overall, more than 80% of the job postings required a bachelor degree; more than 20% require with a more advanced degree. Just as challenging, more than 80% of the job postings require at least 3 years of prior experience; 15% require more than 8 years of prior experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Overall	**40,334 (17%)**	**161,556 (68%)**	**36,282 (15%)**
Engineer	3,476 (8%)	31,882 (75%)	6,997 (17%)
Manager	3,179 (10%)	22,891 (75%)	4,516 (15%)
Analyst	5,608 (19%)	20,861 (72%)	2,384 (8%)
Specialist	6,661 (44%)	7,246 (47%)	1,382 (9%)
Architect	302 (4%)	5,356 (64%)	2,751 (33%)
Auditor	2,361 (31%)	5,017 (67%)	155 (2%)
Consultant	1,222 (19%)	4,345 (69%)	728 (12%)

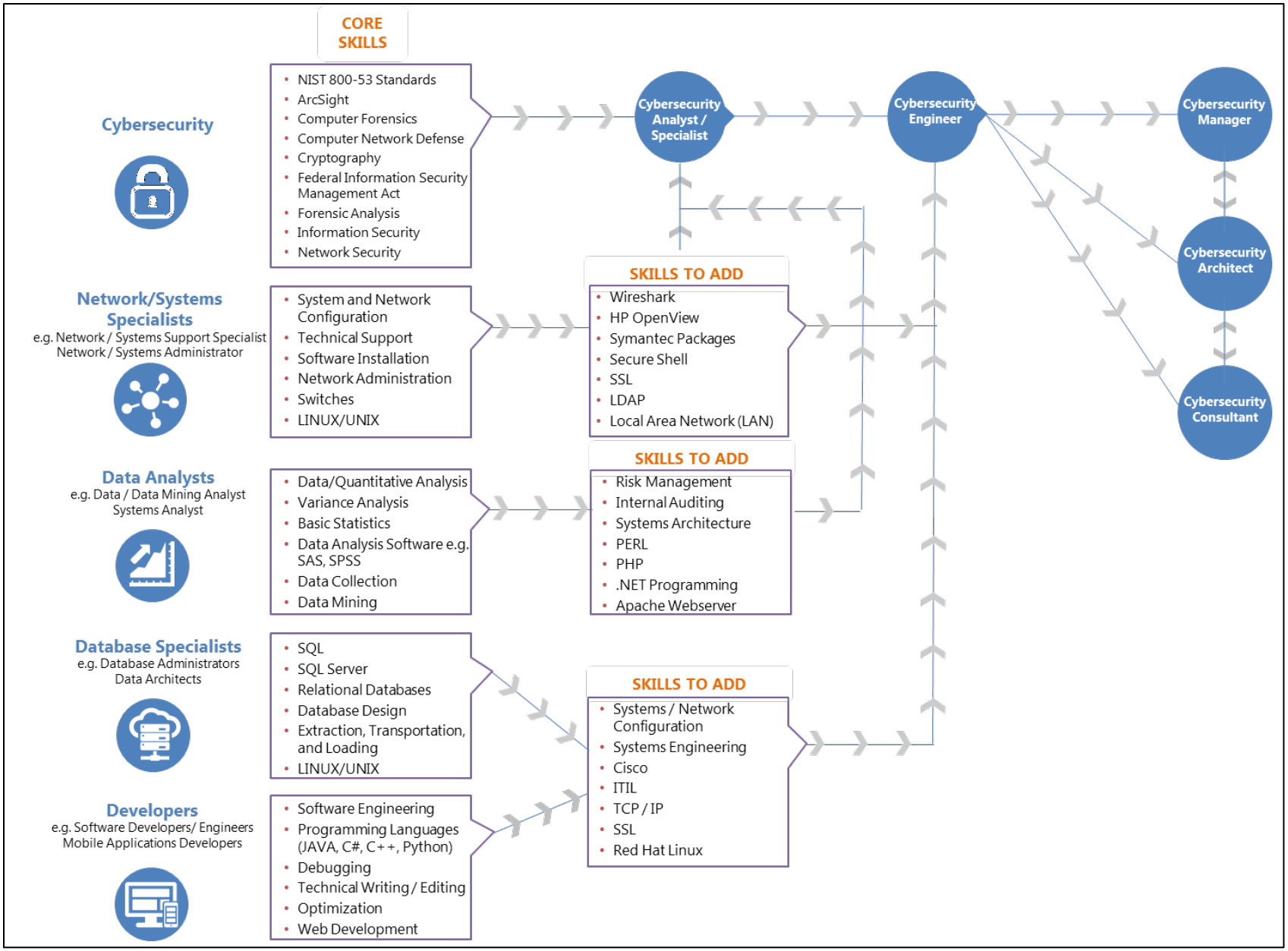
Career Pathways and Transitions

CyberSecurity is an emerging discipline that builds upon the skills of data analytics, data management, software development, digital networking and IT administration. Candidates, with these skills, have the opportunity to transition into the CyberSecurity workforce with additional training, education and certification.

The normative career pathway begins with the role of Specialist, as this role requires the least amount of education and experience. This role is a natural entry-point for workers with experience in digital networking, administration and/or technical support.

The role of Analyst can also be an entry point for workers with experience in data analytics.

For workers advancing in the career pathway, the role of Network Engineer is a frequent, and almost universal, stop along the way. Advancing in the career pathway, to a lesser IT administration. It can also be an entry-point for workers skilled and experienced in Database Management and/or Software Developmen


CORE SKILLS
Cybersecurity
NIST 800-53 Standards
ArcSight
Computer Forensics
Computer Network Defense
Cryptography
Federal Information Security Management Act
Forensic Analysis
Information Security
Network Security
Cybersecurity Analyst / Specialist
Cybersecurity Engineer
Cybersecurity Manager
Cybersecurity Architect
Cybersecurity Consultant
Network/Systems Specialists
e.g. Network / Systems Support Specialist
Network / Systems Administrator
System and Network Configuration
Technical Support
Software Installation
Network Administration
Switches
LINUX/UNIX
SKILLS TO ADD
Wireshark
HP OpenView
Symantec Packages
Secure Shell
SSL
LDAP
Local Area Network (LAN)
Data Analysts
e.g. Data / Data Mining Analyst
Systems Analyst
Data/Quantitative Analysis
Variance Analysis
Basic Statistics
Data Analysis Software e.g. SAS, SPSS
Data Collection
Data Mining
SKILLS TO ADD
Risk Management
Internal Auditing
Systems Architecture
PERL
PHP
.NET Programming
Apache Webserver
Database Specialists
e.g. Database Administrators
Data Architects
SQL
SQL Server
Relational Databases
Database Design
Extraction, Transportation, and Loading
LINUX/UNIX
SKILLS TO ADD
Systems / Network Configuration
Systems Engineering
Cisco
ITIL
TCP / IP
SSL
Red Hat Linux
Developers
e.g. Software Developers/ Engineers
Mobile Applications Developers
Software Engineering
Programming Languages (JAVA, C#, C++, Python)
Debugging
Technical Writing / Editing
Optimization
Web Development

Career transitions, in CyberSecurity, is not casual nor easy to make. Each advancement requires additional skills (often specific to CyberSecurity) and a rigorous set of industry certifications.

The most senior positions in the career pathway are the roles of Manager, Architect, Consultant, or Chief Security Officer. Many of these positions report to the organization's most senior management and are responsible for either operations or strategy as it applies to a large department or the entire organization.

Opportunities for Veterans

The field of CyberSecurity can be a logical career pathway for returning veterans. The security clearance credentials, possessed by many veterans, imply a clearance eligibility that many civilian workers may, or may not, possess.

Approximately 11% of CyberSecurity job posting require some kind of security clearance, and these jobs take employers longer to fill (10% longer than CyberSecurity jobs that do not have a security clearance requirement).

The following table lists the job titles of military occupations which require skills found in a high percentage of civilian CyberSecurity job postings. This information can be used to identify military personnel most likely make successful transitions into civilian cybersecurity roles.

MOC	MOC Title	Service	Career
275	Information Systems Technician	Coast Guard	Enlisted
6049	NALCOMIS Application Administrator/Analyst	Marine Corps	Enlisted
9556	Security Specialist	Navy	Enlisted
17C0	Cyberspace Operations Commander	Air Force	Officer
17D1x, 17D3x, 17D4x	Cyberspace Operations	Air Force	Officer
140A	Command and Control Systems Integrator	Army	Officer
24A	Telecommunications Systems Engineer	Army	Officer
24X	Designated Telecommunications Systems Engineer	Army	Officer
250A	Telecommunications Technician	Army	Officer
254A	Signal Systems Support Technician	Army	Officer
255S	Information Protection Technician	Army	Officer
25A	Signal, General	Army	Officer
290A	Electronic Warfare Technician	Army	Officer
29A	Electronic Warfare Officer	Army	Officer
352N	Signals Intelligence Analysis Technician	Army	Officer
352S	Signals Collection Technician	Army	Officer
35G	Signal Intelligence/Electronic Warfare	Army	Officer
0206	Signal Intelligence/Ground Electronic Warfare Officer	Marine Corps	Officer
0602	Communications Officer	Marine Corps	Officer
0603	Command, Control, Communications, Computers and Intelligence (C4I) Planner Officer	Marine Corps	Officer
0610	Telecommunication Systems Engineering Officer	Marine Corps	Officer
0620	Tactical Communications Planning and Engineer Officer	Marine Corps	Officer
0640	Spectrum Management Officer	Marine Corps	Officer
2602	Signals Intelligence/Electronics Warfare Officer	Marine Corps	Officer
2802	Electronics Maintenance Officer (Ground)	Marine Corps	Officer
8858	Command, Control, Communications, Computers and Intelligence (C4I) Officer	Marine Corps	Officer
9650	Electronic Intelligence Officer	Marine Corps	Officer
9658	Command, Control, Communications, Computers and Intelligence (C4I) Officer	Marine Corps	Officer
2748	Security Manager, Information Security Program	Navy	Officer
9046	Staff Electronic Warfare Officer	Navy	Officer
9282	Ship's Electronic Warfare Officer	Navy	Officer
9404	Tactical Deception Plans Officer	Navy	Officer
9510	Communications System Center Director	Navy	Officer
9512	Communications System Current Ops Manager	Navy	Officer
9515	Communications Plans & Operations Officer	Navy	Officer
9517	Communication Security Officer	Navy	Officer
9523	Joint Interface Control Officer	Navy	Officer
9525	Communication Watch Officer	Navy	Officer
9530	Cryptoboard Officer	Navy	Officer
9543	Director of Communications	Navy	Officer
9560	Satellite Communications Officer	Navy	Officer
9575	Circuit Control Officer	Navy	Officer
9582	Information Systems Officer	Navy	Officer
9590	Staff Communications Officer	Navy	Officer
9595	Communications Traffic Officer	Navy	Officer
9690	Intelligence Support to CNO/CYBER	Navy	Officer
9781	ADP Systems Security Officer	Navy	Officer
2748	Security Manager, Information Security Program	Navy	Officer

IMPLICATIONS AND RECOMMENDATIONS

The CyberSecurity career pathway offers strong opportunity for both first time and recurring job seekers. It features high demand, significant growth and high levels of compensation.

The workforce issues in CyberSecurity are significant for most companies and organizations. Several factors, including higher than normal growth rates, limited CyberSecurity talent, and a lengthy process of education and certification, combine to make it difficult to find qualified talent and extend the time required to fill open positions.

The workforce issues are best addressed by coordinated effort of educators, employers, and policymakers. To that end, this analysis suggests that the following concrete steps are all steps in "the right direction":

- **Transition existing workers into a CyberSecurity pathway:** Many of the roles in CyberSecurity require skills and competencies which have traditionally been required of network administrators, data management specialists and system engineers. The employees in these positions can, with additional training, skill development and certification, be transitioned into a career pathway in CyberSecurity.
- **Resist the temptation to "OverSpec" the job description:** Employers pride themselves on their ability to find and recruit the best talent. And while specifying more than "what is needed" may appear to be one way to do this, it has proven to backfire in this field where talent is in short supply. The CISSP certification, by example, is difficult to obtain and individuals who possess it are in high demand. Employers who include this as either a required or desired credential must be prepared to offer elevated strategies and senior level job titles or else risk finding that their recruitment efforts are both prolonged and unsatisfied.
- **Upgrade educational programs improving their relevancy and authenticity:** Employers prefer to hire candidates who possess critical thinking skills, are able to work on team projects and have some level of work experience. Quality educational programs address all of these attributes challenging and exposing their students to each of these areas aided by industry advisors and their companies. The very best educational programs require and facilitate placement in Cyber-related internship as part of the program and degree requirement.
- **Promote the value of a career in CyberSecurity:** Students and job seekers need to better understand the magnitude and value of the opportunity in cybersecurity. Employers and educators are competing with rival fields for students and employees, and students would benefit from more information about the rewards and responsibilities of a career protecting the nation's digital information.

SPECIFIC PROFILES

Engineer

Engineers build and maintain the security architecture for the IT infrastructure. This is the largest job category in CyberSecurity (42,355 job postings). It grew 55% in the four year period 2010 to 2014, and while robust, this growth rate was significantly lower than almost any other category. Job postings, in this category, remained open an average of 42 days, and the average salary was nearly $14,000 higher than the average salaries across the CyberSecurity spectrum.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Engineer	42,355	55%	$97,620	42 Days

Most job postings (more than 80%) for CyberSecurity Engineers require a four year degree; 17% require a graduate level degree. A modest opportunity (less than 20% of the job postings) exists for candidates with an associate degree.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Engineer	7,082 (17%)	27,879 (66%)	5,591 (13%)	1,803 (4%)

The vast majority of job postings (more than 90%) for CyberSecurity Engineers require at least 3 years of prior experience; 17% require at least 8 years of prior experience. There is a modest opportunity (3,476 job postings) for few entry-level positions in this category, but these positions can be difficult to find (as they are less than 10% of the total).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Engineer	3,476 (8%)	31,882 (75%)	6,997 (17%)

Industry certifications are a valued credential and can significantly affect an employer's level of interest in a specific candidate. It can be a competitive advantage differentiating two candidates who are comparable in experience and education; or it can disqualify a candidate for certain positions that require it. Job Postings are increasingly explicit about the need for specific certifications, and in the case of the one certification, the vendor neutral Certified Information Systems Security Professional (CISSP) certification, more than 20% of the job postings for the role of Engineer, specified this certification as a requirement.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	9,524	22%
Cisco Certified Network Associate	5,320	13%
Cisco Certified Network Professional (CCNP)	5,080	12%
Security+	2,849	7%
Cisco Certified Internetwork Expert (CCIE)	2,548	6%
Microsoft Certified Systems Engineer (MCSE)	2,011	5%
Certified Information Security Manager (CISM)	1,893	4%
Certified Information Systems Auditor (CISA)	1,761	4%
Cisco Certified Security Professional	1,030	2%
GIAC Security Essentials	996	2%

The role of Engineer requires a set of skills unique to CyberSecurity, including an in-depth understanding of firewalls, network and information security, and cryptography. It also relies on more generic software and programming skills and a familiarity with device and software configuration, systems engineering, and network administration. The Cisco Networking Academy is a popular curriculum, adopted by many schools and universities, as a platform of learning modules in this area.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Firewalls	Cisco
Troubleshooting	Network Security	LINUX
Writing	Network Engineering	TCP-IP Protocol
Planning	Information Security	UNIX
Organizational Skills	Cryptography	Virtual Private Networking (VPN)
Problem Solving	System and Network Configuration	Domain Name System (DNS)
Research	Systems Engineering	JAVA
Project Management	Wide Area Network (WAN)	PERL
Customer Service	Software Engineering	Python
Detail-Oriented	Technical Support	SQL
Quality Assurance and Control	Network Administration	OSPF
Microsoft Office	Information Assurance	SSL
Presentation Skills	System Administration	C++
Multi-Tasking	VoIP	Oracle
Microsoft Visio	Telecommunications	Dynamic Host Configuration Protocol (DHCP)
Change Management	Technical Writing - Editing	ITIL
Leadership	Software Installation	CISA
Microsoft Excel	Disaster Recovery Planning	Cisco Routers
Time Management	EIGRP	JavaScript
Analytical Skills	Configuration Management	Extensible Markup Language (XML)

There is a large demand for Engineers in all of the major cities (the nation's capital more than any other) however the hubs of Colorado Springs, and San Jose have a particularly high concentration of jobs (more than 6 times the national average).

Top Metropolitan Areas

Location Analysis

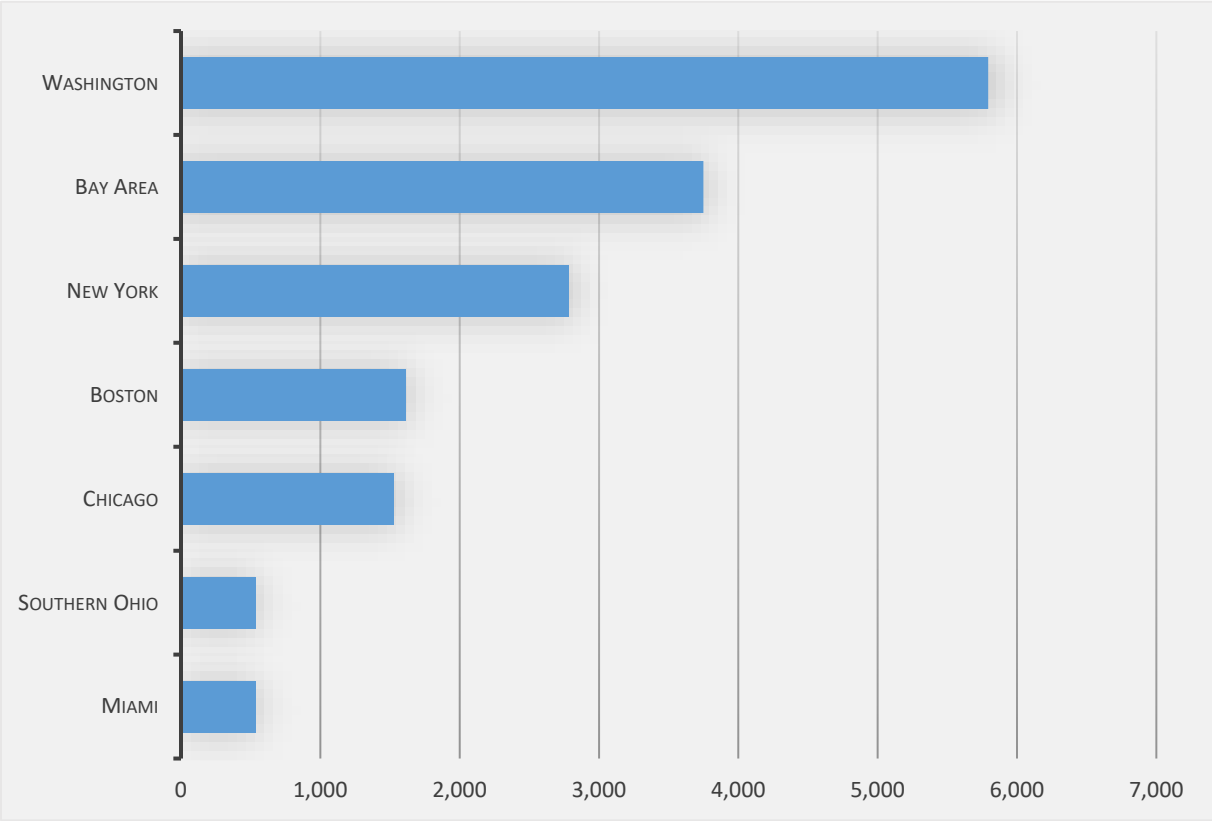
Metro Area	Postings
Washington, D.C	5,793
New York	2,778
San Jose	1,900
San Francisco	1,849
Dallas	1,686
Boston	1,608
Chicago	1,527
Los Angeles	1,373
Atlanta	1,310
Baltimore	1,135

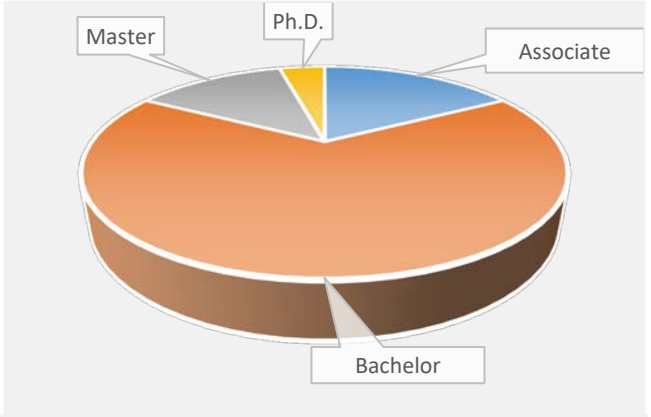
Metro Area	Location Quotient
Colorado Springs	6.7
Washington, D.C.	6.3
San Jose	6.2
Huntsville, AL	3.4
Baltimore	2.8
San Francisco	2.8
Boulder	2.7
Durham	2.7
Denver	2.3
Raleigh	2.1

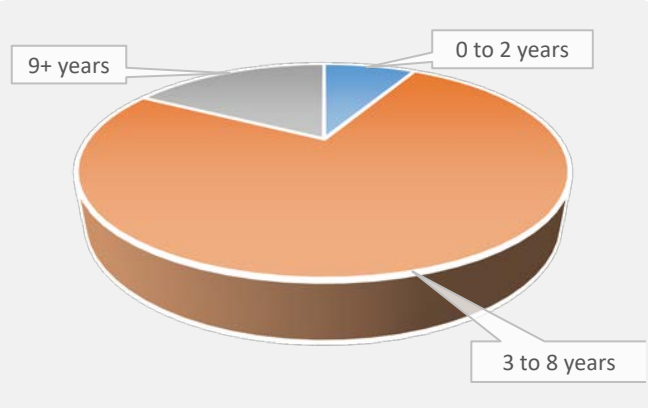
The employment market is maturing at different rates in different regions. Two regions (Washington D.C. and the Bay Area of San Jose) have large numbers of job postings and significant concentration density. Other regions (Miami and Chicago) have smaller numbers but higher growth rates.

It is worth noting that the concentration of job postings is higher than the national average in all of the markets analyzed for this study. It is also worth noting that the posting duration, in these same urban areas is lower than the national average, and only slightly higher than the posting duration for IT jobs overall. The only exception to this trend is Boston, which has a higher than average (45 days) posting duration for Engineers.

Job Postings for Engineers (42,355 Nationally)







	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**42,355**	**55%**	**$97,620**	**42 Days**	**1.0**
Bay Area	3,749	61%	$115,418	39 Days	3.9
Boston	1,608	97%	$102,920	45 Days	2.0
Chicago	1,527	143%	$103,993	39 Days	1.1
Miami	532	173%	$87,975	34 Days	0.7
New York	2,778	89%	$107,440	34 Days	1.0
Southern Ohio	533	118%	$91,393	29 Days	0.7
Washington, D.C.	5,793	13%	$101,233	37 Days	6.3

The majority of job postings (75%) for Engineers require a Bachelor's Degree, but opportunities do exist for candidates with an Associate's Degree. Opportunities exist for candidates with Associate Degrees in modest number (Washington, New York and the Bay Area having the largest number of postings). The Bay Area has the notable distinction of requiring Graduate Degrees for more job postings (36% of all postings, more than twice the national average) than any other region.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**7,082 (17%)**	**27,879 (66%)**	**5,591 (13%)**	**1,803 (4%)**
Bay Area	466 (12%)	1,906 (51%)	1,060 (28%)	316 (8%)
Boston	207 (13%)	993 (62%)	283 (18%)	125 (8%)
Chicago	339 (22%)	1,013 (66%)	145 (9%)	31 (2%)
Miami	84 (16%)	310 (58%)	130 (24%)	9 (2%)
New York	500 (18%)	1,878 (68%)	312 (11%)	87 (3%)
Southern Ohio	103 (19%)	364 (68%)	51 (10%)	14 (3%)
Washington, D.C.	736 (13%)	4,013 (69%)	750 (13%)	295 (5%)

This category has limited opportunity for entry-level professionals as postings consistently require a modest work experience (75% to 80% calling for more than 3 years of experience). Washington D.C. is no exception (72% of postings require more than 3 years of experience), however a high number (25% of postings) require more than 9 years of work experience. This statistic is 50% higher than the national norm and may be a consequence of the region's high concentration of defense contractors and federal government workers.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**3,476 (8%)**	**31,882 (75%)**	**6,997 (17%)**
Bay Area	309 (8%)	3,000 (80%)	441 (12%)
Boston	124 (8%)	1,255 (78%)	229 (14%)
Chicago	111 (7%)	1,212 (79%)	204 (13%)
Miami	44 (8%)	423 (80%)	65 (12%)
New York	223 (8%)	2,256 (81%)	299 (11%)
Southern Ohio	41 (8%)	406 (76%)	86 (16%)
Washington, D.C.	462 (8%)	3,833 (66%)	1,498 (26%)

Manager

Managers are responsible for both the information security infrastructure and the personnel who design and administer the operation of it. This is the second largest cybersecurity category (more than 30,000 postings). The opportunity for Managers grew significantly (80% growth) in the four year period 2010 to 2014. This job category pays well (average salary is $90,262), and new positions can be challenging to fill (41 days average duration for job postings).

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Manager	30,586	80%	$90,262	41 Days

The educational requirements for this category do not differ from those of the other categories (86% require a bachelor degree, 25% a more advanced degree).

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Manager	4,245 (14%)	19,913 (65%)	5,251 (17%)	1,177 (4%)

However the experience requirement is much more rigorous (90% of job openings require at least 3 years of experience, 15% require at least 9 years of experience).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Manager	3,179 (10%)	22,891 (75%)	4,516 (15%)

Managers are required to have a strong mix of systems and networking skills (e.g. systems administration and network security) and a demonstrated proficiency in both organizational and interpersonal skills (project management, planning, and communications).

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	LINUX
Organizational Skills	Network Security	UNIX
Planning	Systems Administration	Oracle
Troubleshooting	Firewalls	Cisco
Writing	System and Network Configuration	SQL
Project Management	Technical Support	Domain Name System (DNS)
Problem Solving	Software Installation	Transmission Control Protocol - Internet Protocol (TCP - IP)
Research	Cryptography	ITIL
Customer Service	Network Administration	Virtual Private Networking (VPN)
Microsoft Office	Disaster Recovery Planning	Dynamic Host Configuration Protocol (DHCP)
Building Effective Relationships	Risk Management	Microsoft SharePoint
Microsoft Excel	Internal Auditing	SAP
Detail-Oriented	Wide Area Network (WAN)	Microsoft Exchange
Presentation Skills	Windows Server	Red Hat Linux
Change Management	Database Administration	SQL Server
Budgeting	Business Process	PERL
Supervisory Skills	Risk Assessment	JAVA
Project Planning and Development Skills	Telecommunications	Microsoft SQL
Leadership	Optimization	Solaris
Quality Assurance and Control	Hardware and Software Configuration	Symantec Packages

The certification requirements for this category are not unique when compared to other jobs categories, however certain job postings (15 to 20%) will require either a CISSP or CISA.

These certifications are noteworthy because they require documentation demonstrating at least five years of work experience.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	5,690	19%
Certified Information Systems Auditor (CISA)	5,224	17%
Security+	3,204	10%
Certified Information Security Manager (CISM)	2,411	8%
Microsoft Certified Systems Engineer (MCSE)	2,122	7%
Project Management Certification (E.G. PMP)	1,620	5%
Cisco Certified Network Associate	1,511	5%
Cisco Certified Network Professional (CCNP)	1,468	5%
GIAC Security Essentials	1,180	4%

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	3,094
New York	2,468
Chicago	1,210
Dallas	1,173
Los Angeles	1,159
San Francisco	922
Boston	872
Atlanta	837
San Jose	744

Metro Area	Location Quotient
Washington, D.C.	4.6
San Jose	3.4
Denver	2.1
San Francisco	1.9
Charlotte	1.9
Baltimore	1.7
Portland	1.7
Dallas	1.6
Virginia Beach	1.6

The strongest demand for Managers is in the defense and technology hubs of Washington, D.C. and San Francisco. There is also a strong concentration of job openings in the metro areas of Denver, Charlotte, and Portland.

Location Analysis

The areas of Miami and Chicago have experienced the highest level of job growth in this category (145% and 152%, respectively since 2010). They also have high average posting durations (41 and 43 days, respectively). This suggests that the supply of qualified workers is struggling to keep up with demand in these locations.

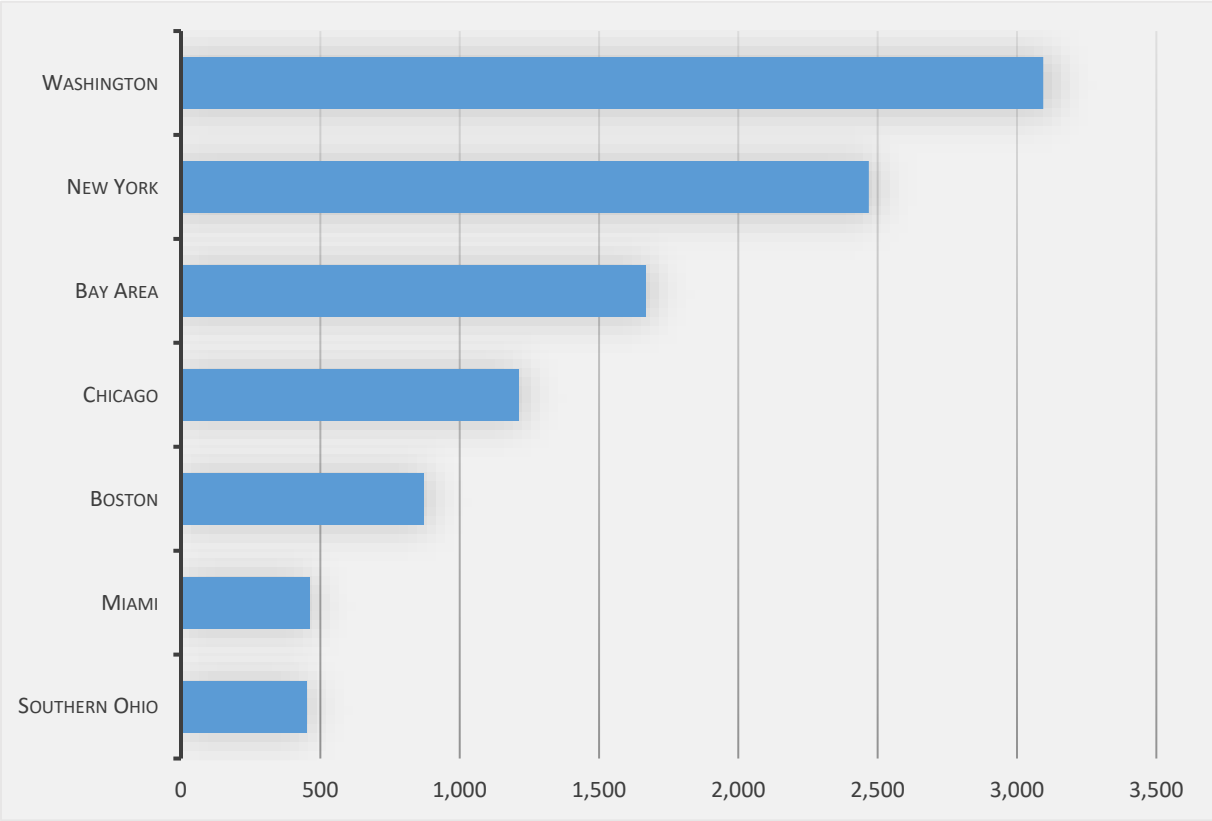
The metro areas of Washington and New York have the largest number of postings, and Washington has an extremely high location quotient (over 4 times the national average).

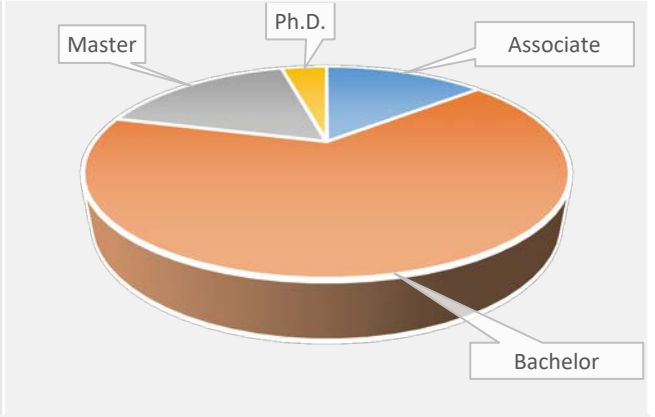
Managers, in CyberSecurity are well paid, and the managers in the selected metro areas are, with the exception of Southern Ohio, paid 10% to 15% more than the national average of $90,262.

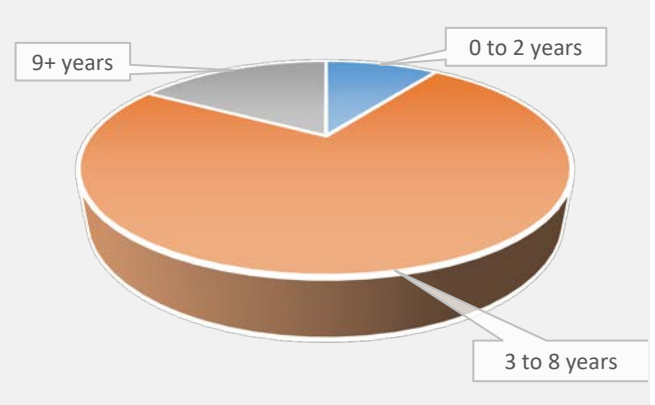
	Total Postings	Growth (2010 to 2014)	Average Salary	Average of Days Open	Location Quotient
Nationally	**30,586**	**80%**	**$90,262**	**41 Days**	**1.0**
Bay Area	1,666	65%	$100,304	40 Days	2.4
Boston	872	67%	$103,302	37 Days	1.5
Chicago	1,210	145%	$106,640	41 Days	1.2
Miami	461	152%	$96,239	43 Days	0.9
New York	2,468	81%	$108,481	37 Days	1.3
Southern Ohio	449	94%	$79,183	27 Days	0.8
Washington, D.C.	3,094	47%	$98,282	37 Days	4.6

A bachelor's degree is, generally, an important credential (both in CyberSecurity and in the Manager category) but in Boston, Miami, New York, and the Bay Area employers place even greater emphasis (more than 90% of all openings) on a four-year degree for Manager candidates.

Job Postings for Managers (30,586 Nationally)







	A.S.	B.S.	M.S.	Ph.D.
Nationally	**4,245 (14%)**	**19,913 (65%)**	**5,251 (17%)**	**1,177 (4%)**
Bay Area	133 (8%)	1,026 (62%)	409 (25%)	98 (6%)
Boston	60 (7%)	574 (66%)	187 (21%)	51 (6%)
Chicago	145 (12%)	755 (62%)	256 (21%)	54 (4%)
Miami	35 (8%)	337 (73%)	89 (19%)	0 (0%)
New York	147 (6%)	1,647 (67%)	537 (22%)	137 (6%)
Southern Ohio	69 (15%)	283 (63%)	86 (19%)	11 (3%)
Washington, D.C.	388 (13%)	2,224 (72%)	393 (13%)	89 (3%)

Job openings, nationally, specify a minimum of 3 years of experience for most (90%) manager positions. The metro areas, analyzed for this report, were, as a general rule, slightly more rigorous (with more than 90% specify a minimum of 3 years of experience).

	0 to 2 years	3 to 8 years	9+ years
Nationally	**3,179 (10%)**	**22,891 (75%)**	**4,516 (15%)**
Bay Area	106 (6%)	1,293 (78%)	266 (16%)
Boston	66 (8%)	718 (82%)	88 (10%)
Chicago	76 (6%)	942 (78%)	192 (16%)
Miami	30 (7%)	374 (81%)	57 (12%)
New York	184 (7%)	1,947 (79%)	336 (14%)
Southern Ohio	34 (8%)	364 (81%)	50 (11%)
Washington, D.C.	310 (10%)	2,177 (70%)	607 (20%)

Washington D.C., although consistent with the national trend for job postings requiring more than three years of experience, led both the nation and the other metro areas requiring more than 9 years of experience for 20% of the open Manager positions.

Analyst

Analysts detect and prevent cybersecurity threats by identifying vulnerabilities in the infrastructure. This is the third largest cybersecurity category (almost 29,000 postings) The opportunity for Analysts grew significantly (100% growth) in the four year period 2010 to 2014. This job category has an average salary of $78,898 and job postings remain open for 38 days on average.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Analyst	28,853	100%	$78,898	38 Days

Most job postings, in this category, specify the the requirement for a bachelor's degree (75% of all job postings), while only a modest number (14% require a more advanced degree).

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Analyst	3,316 (11%)	21,514 (75%)	3,223 (11%)	799 (3%)

However, the experience requirement is much more rigorous (90% of job openings require at least 3 years of experience, 15% require at least 9 years of experience).

The Analyst position is a strong candidate for entry level professionals (almost 20% of the Analyst postings specify 0 to 3 years of prior experience).

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Analyst	5,608 (19%)	20,861 (72%)	2,384 (8%)

Analysts are required to have specialized skills in information security, firewalls, network security, and cryptography and a demonstrated proficiency in the baseline skills of communication, writing, organization and problem solving. They are expected to have programming experience in SQL and Python, and a background in data mining and manipulation.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	LINUX
Writing	Firewalls	UNIX
Organizational Skills	Network Security	SQL
Problem Solving	Cryptography	Transmission Control Protocol - Internet Protocol (TCP - IP)
Research	Technical Support	Cisco
Project Management	System and Network Configuration	Oracle
Troubleshooting	Information Assurance	ITIL
Planning	Systems Analysis	Virtual Private Networking (VPN)
Microsoft Excel	Business Process	JAVA
Microsoft Office	HIPAA	PERL
Customer Service	Risk Management	Microsoft SharePoint
Detail-Oriented	Business Analysis	Domain Name System (DNS)
Microsoft PowerPoint	System Administration	Python
Multi-Tasking	Risk Assessment	SAP
Analytical Skills	Network Engineering	Symantec Packages
Building Effective Relationships	Technical Writing - Editing	ArcSight
Quality Assurance and Control	Disaster Recovery Planning	McAfee
Time Management	Wide Area Network (WAN)	Microsoft Operating Systems
Presentation Skills	Telecommunications	SSL
Change Management	Data Analysis	C++

Candidates, who are certified as CISSPs, will have an advantage when applying for positions in this category.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	7,050	24%
Certified Information Systems Auditor (CISA)	3,491	12%
Certified Information Security Manager (CISM)	2,289	8%
Security+	1,513	5%
Cisco Certified Network Associate	1,068	4%
GIAC Certified Incident Handler	882	3%
GIAC Security Essentials	747	3%
Certified In Risk And Information Systems Control	723	3%
GIAC Certified Intrusion Analyst	667	2%
Microsoft Certified Systems Engineer (MCSE)	577	2%

The greatest demand, for this job category, in in the metro areas of Washington D.C. and New York. There is a high concentration of postings in the metro areas Charlotte, Denver, Baltimore, Austin, and San Jose (almost twice the national average).

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	2,817
New York	1,853
Chicago	1,068
Dallas	1,040
Atlanta	794
San Francisco	686
Philadelphia	664
Los Angeles	662
Boston	658
Denver	642

Metro Area	Location Quotient
Washington, D.C.	4.5
Charlotte	2.6
Denver	2.3
Baltimore	2.2
Austin	1.9
San Jose	1.9
St. Louis	1.8
Portland, OR	1.8
Atlanta	1.6
Dallas	1.5

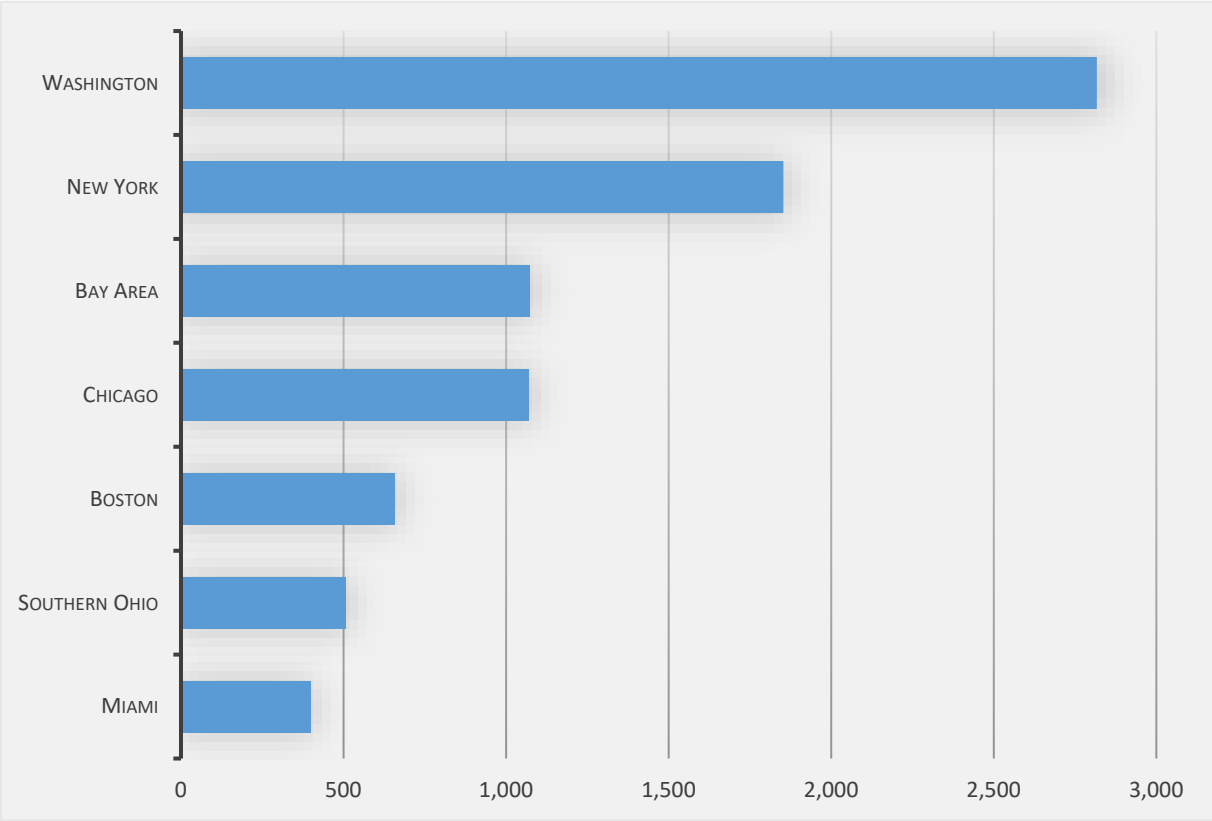
Location Analysis

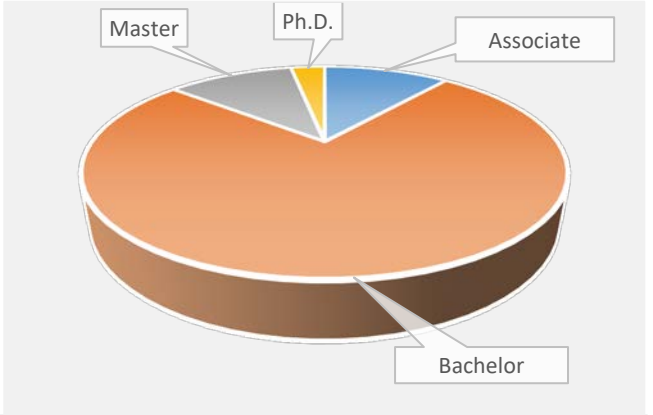
The areas of Chicago, Boston and Miami have experienced the highest level of job growth in this category (286%, 147% and 146%, respectively since 2010).

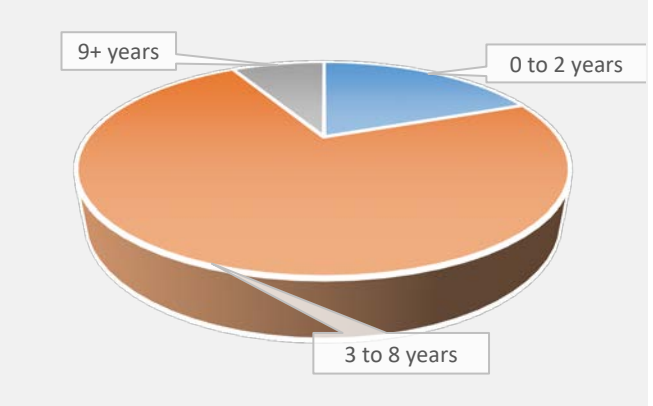
The metro areas of Washington and New York have the largest number of postings, and Washington has an extremely high location quotient (over 4 times the national average).

Analysts in the selected metro areas are, with the exception of Southern Ohio, paid 15% to 25% higher than the national average of $78,.898.

Job Postings for Analysts (28,853 Nationally)







	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**28,853**	**100%**	**$78,898**	**38 Days**	**1.0**
Bay Area	1,073	126%	$94,886	42 Days	1.6
Boston	658	147%	$89,381	35 Days	1.2
Chicago	1,068	286%	$86,885	39 Days	1.1
Miami	399	146%	$67,732	37 Days	0.8
New York	1,853	72%	$101,241	36 Days	1.0
Southern Ohio	507	137%	$67,900	33 Days	1.0
Washington, D.C.	2,817	7%	$94,387	37 Days	4.5

The metro areas of Employers are predominantly looking to fill analyst openings with bachelor's-level candidates across geographies. In all locations, over 85% of openings request at least four-year degree, and in the Bay Area, Boston, New York, and Washington, D.C. this requirement is demanded in over 90% of openings. Only Miami and Southern Ohio show slightly greater opportunities for sub-baccalaureate workers, but the opportunities are still scarce compared to many other cybersecurity roles. In the Bay Area and New York, over 20% of postings request candidates with at least a master's degree

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**3,316 (11%)**	**21,514 (75%)**	**3,223 (11%)**	**799 (3%)**
Bay Area	70 (7%)	753 (70%)	182 (17%)	67 (6%)
Boston	46 (7%)	503 (76%)	86 (13%)	23 (4%)
Chicago	117 (11%)	807 (76%)	115 (11%)	30 (3%)
Miami	48 (12%)	315 (79%)	32 (8%)	3 (1%)
New York	93 (5%)	1,323 (71%)	372 (20%)	65 (4%)
Southern Ohio	65 (13%)	384 (76%)	50 (10%)	8 (2%)
Washington, D.C.	137 (5%)	2,238 (79%)	355 (13%)	87 (3%)

Despite the lack of opportunities for workers without a bachelor's degree, entry-level opportunities are consistently more plentiful for Analysts. In Chicago and Southern Ohio the entry-level opportunities for Analysts are especially strong, with over 25% of openings requesting two or fewer years of experience in each location. In contrast, Washington, D.C. employers is the only geography where over 10% of Analyst openings request more than eight years of experience – in fact, Analyst openings in D.C. are over twice as likely to request workers with such heightened levels of experience than they are nationally.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**5,608 (19%)**	**20,861 (72%)**	**2,384 (8%)**
Bay Area	195 (18%)	850 (79%)	28 (3%)
Boston	113 (17%)	509 (77%)	36 (5%)
Chicago	274 (26%)	742 (69%)	52 (5%)
Miami	46 (12%)	320 (80%)	33 (8%)
New York	280 (15%)	1,432 (77%)	140 (8%)
Southern Ohio	136 (27%)	351 (69%)	20 (4%)
Washington, D.C.	504 (18%)	1,837 (65%)	476 (17%)

Specialist

Specialists implement, test, and monitor an organization's information security systems. Specialist openings generally represent the strongest opportunities for workers to begin a career in cybersecurity due to strong opportunities for sub-baccalaureate and entry-level workers. In 2014 there were 15,289 openings for Specialists, representing 97% growth in demand since 2010. Because many Specialist openings represent entry-level opportunities, the average salary for Specialists is slightly below the average for all cybersecurity jobs. Nonetheless, it is still robust at just over $80,000. Specialists are also remaining open for 35 days – 13% shorter than the average for all cybersecurity roles. This suggests that the reduced education and experience requirements for these roles make them easier to fill than many of their counterparts in cybersecurity.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Specialist	15,289	97%	$80,847	35 Days

Although a majority of postings for cybersecurity Specialists request at least a bachelor's, cybersecurity Specialists offer robust opportunities for workers without a four-year degree. In total, 37% of Specialist job postings were open to workers without a bachelor's degree – the highest among all cybersecurity job categories.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Specialist	5,639 (37%)	6,717 (44%)	1,364 (9%)	1,569 (10%)

Just as Specialists offer strong opportunities for sub-baccalaureate workers, they also offer excellent opportunities for entry-level candidates. Almost half of all Specialist openings – 44%, specifically – were open to workers with two years or less experience. This establishes Specialists as the strongest option for inexperienced workers aiming to begin a career in cybersecurity.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Specialist	6,661 (44%)	7,246 (47%)	1,382 (9%)

Specialist job openings request a strong set of technical support and basic networking skills and tools, such as software installation, help desk support, Cisco, and Hardware and Software Configuration.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	Cisco
Troubleshooting	Network Security	LINUX
Organizational Skills	Technical Support	UNIX
Writing	Information Assurance	Transmission Control Protocol - Internet Protocol (TCP - IP)
Problem Solving	Firewalls	Virtual Private Networking (VPN)
Planning	Software Installation	ITIL
Detail-Oriented	System and Network Configuration	SQL
Research	Repair	Oracle
Customer Service	Cryptography	Domain Name System (DNS)
Project Management	Help Desk Support	JAVA
Microsoft Office	Wide Area Network (WAN)	Microsoft Operating Systems
Building Effective Relationships	Telecommunications	Microsoft SharePoint
Microsoft Excel	System Administration	Dynamic Host Configuration Protocol (DHCP)
Supervisory Skills	Hardware and Software Configuration	PERL
Analytical Skills	Knowledge of Personal Computers	SAP
Computer Skills	Network Hardware-Software Maintenance	McAfee
Multi-Tasking	Mathematics	Symantec Packages
Quality Assurance and Control	Printers	Microsoft Exchange
Leadership	Local Area Network (LAN)	Python
Typing	Network Engineering	Solaris

Certifications are in-demand for Specialists, and CISSP is still the most-demanded certification as with other cybersecurity job categories, but most of the in-demand certifications for Specialists are entry-level security or networking credentials such as Security+, Network+, and Cisco Certified Network Associate.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	2,425	16%
Security+	1,941	13%
Network+ Certified	1,271	8%
Cisco Certified Network Associate	942	6%
Certified Information Systems Auditor (CISA)	923	6%
Systems Security Certified Practitioner	869	6%
Certified Information Security Manager (CISM)	743	5%
Microsoft Certified Technology Specialist (MCTS)	609	4%
Microsoft Certified Professional (MCP)	505	3%
GIAC Security Essentials	483	3%

Demand for cybersecurity Specialists is strongest in Washington, D.C., as is the case for cybersecurity roles overall. However, some smaller markets have some of the strongest concentration of Specialist openings – including Colorado Springs, Honolulu, and St. Louis.

Top Metropolitan Areas

Metro Area	Postings
Washington, D.C.	2,570
New York	558
Dallas	378
Los Angeles	369
San Francisco	366
Chicago	338
Baltimore	336
Virginia Beach	278
St. Louis	267
San Diego	266

Metro Area	Location Quotient
Washington, D.C.	7.7
Colorado Springs	5.1
Honolulu	5
Virginia Beach	3.4
Baltimore	2.3
St. Louis	1.8
San Diego	1.8
Denver	1.7
San Antonio	1.7
San Francisco	1.5

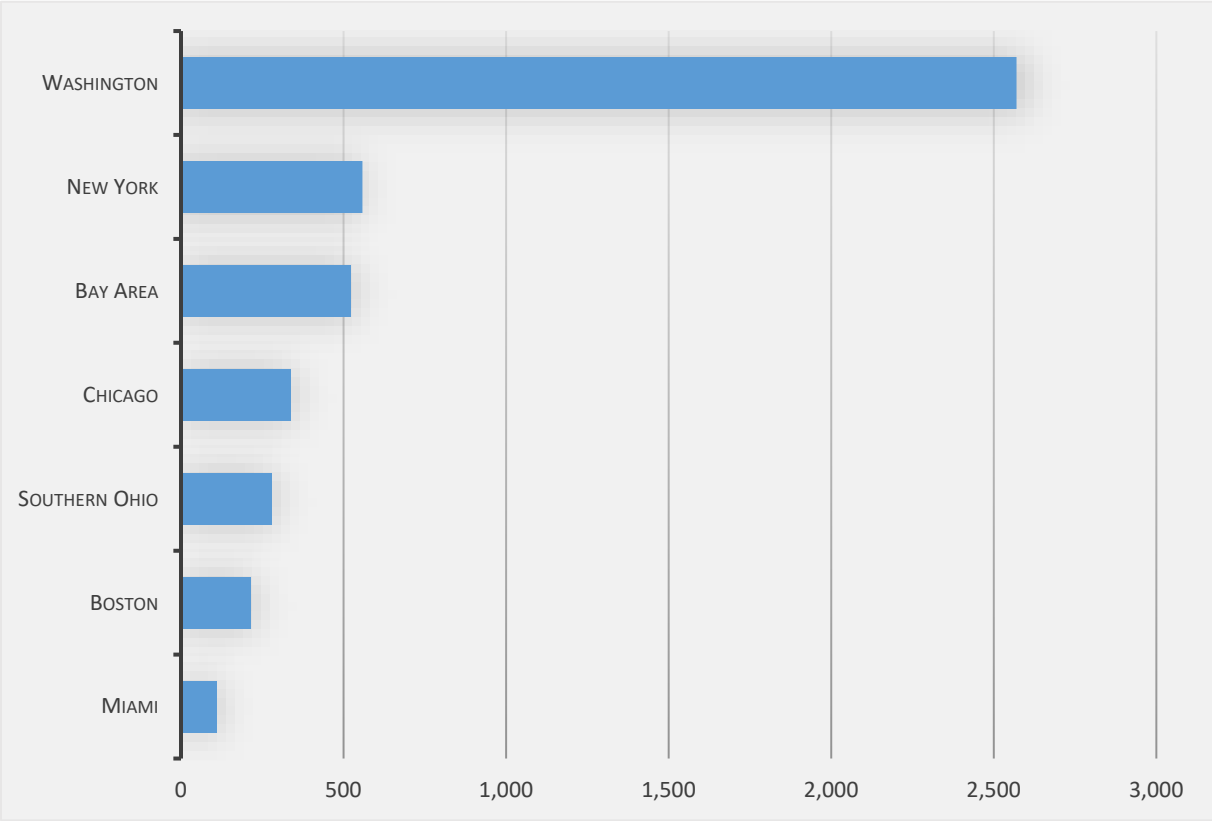
Location Analysis

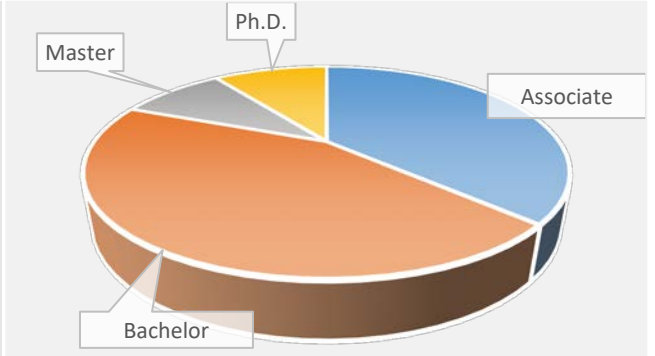
Demand dynamics for Cybersecurity Specialists differ significantly across geographies. Although demand growth for Specialists since 2010 has been strong across geographies, it ranges from 42% in Miami and New York all the way to 167% in the Bay area. Salaries also differ across geographies, from a low of $60,386 in Miami to over $100,000 in Washington, D.C. and New York. Even in the locations with heightened salaries and growth, however, Specialist jobs are remaining open for comparable or shorter lengths of time compared to the national average. This may be due, at least in part, to the combination of high salaries and low barriers to entry for cybersecurity Specialists.

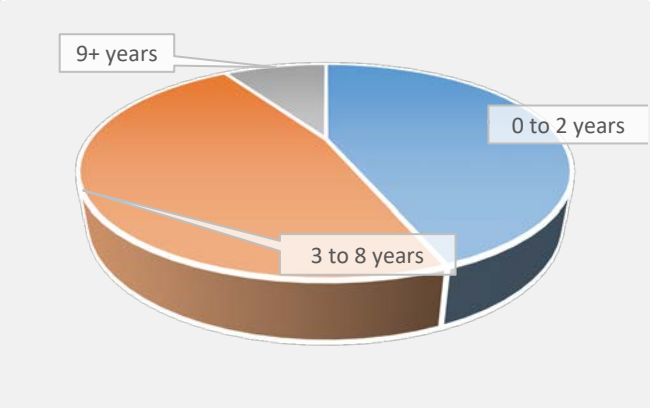
	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**15,289**	**97%**	**$80,847**	**35 Days**	**1.0**
Bay Area	521	167%	$80,420	29 Days	1.5
Boston	215	60%	$88,945	21 Days	0.7
Chicago	338	132%	$83,421	35 Days	0.7
Miami	108	42%	$60,386	35 Days	0.4
New York	558	42%	$100,954	29 Days	0.6
Southern Ohio	278	136%	$75,948	25 Days	1.0
Washington, D.C.	2,570	78%	$103,994	31 Days	7.7

Across the geographies analyzed, cybersecurity Specialists have fewer sub-baccalaureate opportunities than the national average, but these opportunities are still relatively plentiful. In Boston and New York, however, only 20% and 18% of postings, respectively, are open to candidates without a four-year degree.

Job Postings for Specialists (15,289 Nationally)







	A.S.	B.S.	M.S.	Ph.D.
Nationally	**5,639 (37%)**	**6,717 (44%)**	**1,364 (9%)**	**1,569 (10%)**
Bay Area	135 (26%)	249 (48%)	65 (12%)	73 (14%)
Boston	42 (20%)	135 (63%)	26 (12%)	12 (5%)
Chicago	87 (26%)	212 (63%)	14 (4%)	25 (7%)
Miami	35 (32%)	57 (53%)	12 (11%)	4 (4%)
New York	99 (18%)	369 (66%)	69 (12%)	21 (4%)
Southern Ohio	101 (36%)	119 (43%)	42 (15%)	16 (6%)
Washington, D.C.	795 (31%)	1,334 (52%)	199 (8%)	241 (9%)

Opportunities for entry-level cybersecurity Specialists vary widely across geographies. In Boston, for example, only 21% of openings are open to workers with two or fewer years of experience; however, in Southern Ohio 54% of openings request entry-level candidates. Similarly, mid-level workers who have three to eight years of experience are requested in less than 40% of Specialist openings in both Southern Ohio and Washington, D.C., but over 60% of postings in New York and Boston request candidates with this moderate range of experience.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**6,661 (44%)**	**7,246 (47%)**	**1,382 (9%)**
Bay Area	172 (33%)	309 (59%)	40 (8%)
Boston	45 (21%)	147 (68%)	23 (11%)
Chicago	129 (38%)	189 (56%)	20 (6%)
Miami	50 (46%)	49 (45%)	9 (9%)
New York	155 (28%)	341 (61%)	62 (11%)
Southern Ohio	149 (54%)	106 (38%)	22 (8%)
Washington, D.C.	1,230 (48%)	1,003 (39%)	337 (13%)

Architect

Architects oversee the design and implementation of an organization's information security systems. In 2014, there were 8,409 postings for cybersecurity Architects. They have grown in-step with the broader cybersecurity job market, with demand increasing 95% since 2010. Architects are commanding the highest salaries in the cybersecurity landscape: on average, advertised salaries for Architects are $112,659. Despite these high salaries, Architect openings are remaining open 37 days, on average – 8% shorter than cybersecurity jobs overall.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Architect	8,409	95%	$112,659	37 Days

Over 80% of openings for cybersecurity Architects request workers with at least a bachelor's degree, and there is significant demand for workers with graduate degrees as well – 29% of openings request at least a master's. Although the majority of openings seek candidates with at least a four-year degree, there is also demand for sub-baccalaureate workers. Overall, 19% of openings are open to workers with less than a bachelor's degree, suggesting that some employers are willing to substitute the right mix of skills and experience for advanced educational attainment.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Architect	1,617 (19%)	4,422 (53%)	1,981 (24%)	389 (5%)

Although cybersecurity Architects offer some sub-baccalaureate opportunities, the entry-level opportunities are scarce. Only 4% of openings are open to workers with two years or less of prior experience, and a third of openings request advanced workers with over eight years of work history.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Architect	302 (4%)	5,356 (64%)	2,751 (33%)

Architects require the same mix of core cybersecurity and networking skills common across cybersecurity roles – such as network security, firewalls, cryptography, and Cisco – but they also have strong demand for big data expertise and the requisite tools to manage both structured and unstructured datasets – such as Apache Hadoop and SQL. They also require more web-specific expertise, such as web application development, JavaScript, and XML.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	Cisco
Organizational Skills	Network Security	JAVA
Writing	Firewalls	LINUX
Planning	Cryptography	SQL
Project Management	Wide Area Network (WAN)	UNIX
Problem Solving	Network Engineering	Oracle
Research	System Architecture	Virtual Private Networking (VPN)
Troubleshooting	Mentoring	Transmission Control Protocol - Internet Protocol (TCP - IP)
Presentation Skills	System and Network Configuration	ITIL
Customer Service	Business Process	JavaScript
Leadership	Web Application Development	Microsoft C#
Building Effective Relationships	HIPAA	Platform as a Service
Articulate	Systems Development Life Cycle (SDLC)	SSL
Multi-Tasking	Big Data	Apache Hadoop
Creativity	Disaster Recovery Planning	Extensible Markup Language (XML)
Change Management	Optimization	Domain Name System (DNS)
Time Management	Technical Support	Middleware
Quality Assurance and Control	Business Strategy	OSPF
Detail-Oriented	Network Administration	Agile Development

Architects have strong demand for CISSP, with 25% of openings requesting the credential. Additional certifications are also in-demand – such as CISA, CISM, and various networking credentials – but none of these certifications are requested in more than 10% of openings.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	2,109	25%
Certified Information Systems Auditor (CISA)	644	8%
Certified Information Security Manager (CISM)	589	7%
Cisco Certified Network Professional (CCNP)	573	7%
Cisco Certified Internetwork Expert (CCIE)	565	7%
Cisco Certified Network Associate	444	5%
TOGAF	421	5%
Microsoft Certified Systems Engineer (MCSE)	333	4%
It Infrastructure Library	236	3%
Cisco Certified Design Professional (CCDP)	183	2%

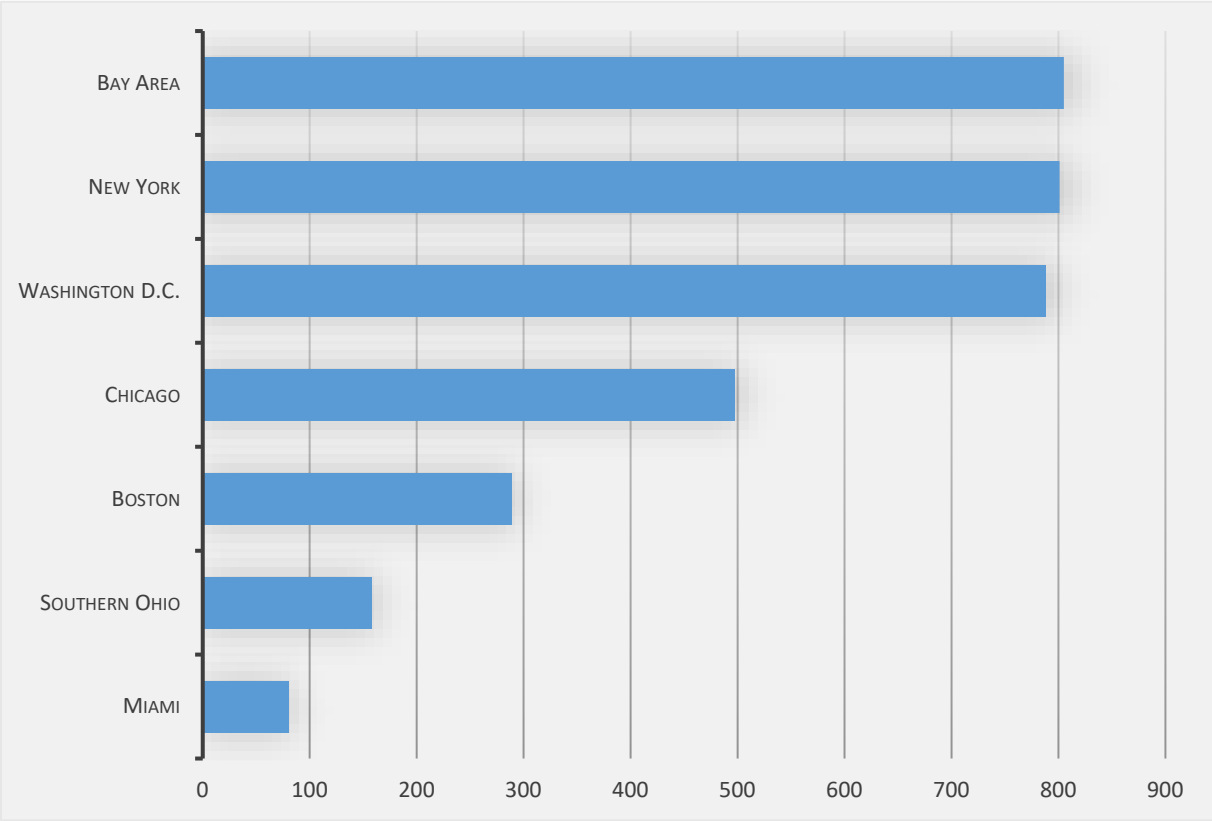
As with other cybersecurity categories, New York and Washington, D.C. have the greatest magnitude of openings for cybersecurity Architects. Unlike other cybersecurity categories, however, San Jose has the greatest concentration for cybersecurity Architects, rather than the nation's capital.

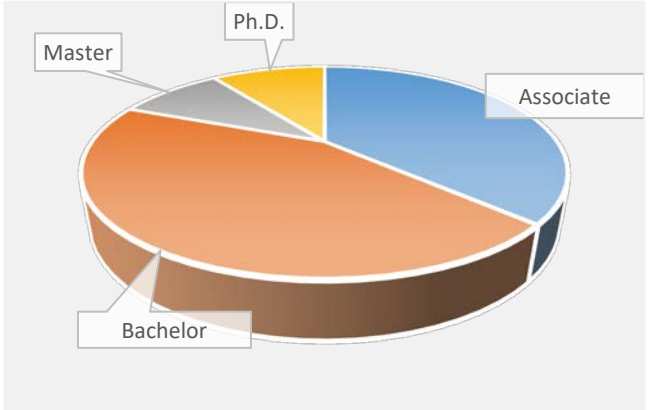
Top Metropolitan Areas

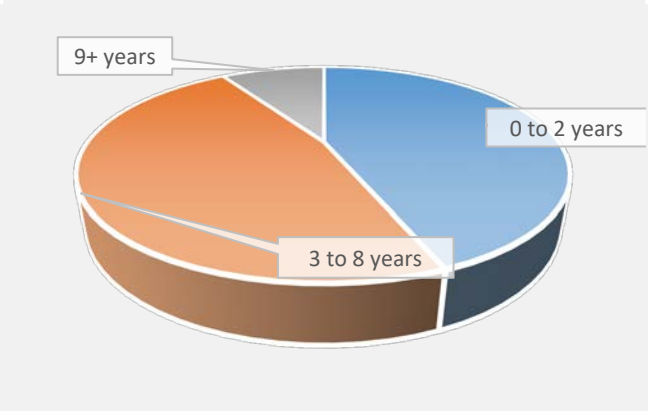
Metro Area	Postings
New York	801
Washington, D.C.	788
Chicago	497
San Jose	412
Dallas	409
San Francisco	393
Atlanta	325
Boston	289
Los Angeles	243
Phoenix	186

Metro Area	Location Quotient
San Jose	6.8
Washington, D.C.	4.3
Austin	3.0
San Francisco	3.0
Atlanta	2.2
Dallas	2.1
Chicago	1.8
Boston	1.8
Portland, OR	1.7
Denver	1.7

Job Postings for Architects (8,409 Nationally)







Location Analysis

Cybersecurity Architects consistently offer strong opportunities across geographies, although their demand dynamics vary across the key locations. Demand growth for Architects since 2010 varies from 38% in Washington, D.C. to 176% in Miami, where the concentration of Architects still has plenty of room to grow. Advertised salaries are consistently robust across geographies, in most cases pushing well into the six-figures. Posting duration does differ significantly across regions, however. In Southern Ohio and New York, openings for architects are remaining open, on average, for fewer than 30 days; in Boston and the Bay Area, by contrast, they are remaining open for 42 days – 14% longer than the national average.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**8,409**	**95%**	**$112,659**	**37 Days**	**1.0**
Bay Area	805	120%	$136,180	42 Days	4.2
Boston	289	64%	$111,621	42 Days	1.8
Chicago	497	125%	$115,115	32 Days	1.8
Miami	80	176%	$96,944	37 Days	0.5
New York	801	100%	$125,500	29 Days	1.5
Southern Ohio	158	63%	$105,024	25 Days	1.1
Washington, D.C.	788	38%	$117,029	39 Days	4.3

This increased hiring difficulty in Boston and the Bay Area may be related to the increased educational credentials requested of cybersecurity Architects in these locations. In both cities, 88% of openings request at least a four-year degree, compared with 81% nationally. In Southern Ohio, however, nearly one-third of openings are open to workers without a bachelor's degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**1,617 (19%)**	**4,422 (53%)**	**1,981 (24%)**	**389 (5%)**
Bay Area	100 (12%)	393 (49%)	218 (27%)	94 (12%)
Boston	36 (12%)	153 (53%)	94 (32%)	6 (2%)
Chicago	78 (16%)	315 (63%)	98 (20%)	5 (1%)
Miami	13 (17%)	49 (62%)	16 (20%)	1 (2%)
New York	106 (13%)	439 (55%)	214 (27%)	42 (5%)
Southern Ohio	48 (30%)	80 (51%)	26 (16%)	4 (3%)
Washington, D.C.	81 (10%)	447 (57%)	208 (26%)	52 (7%)

Entry-level opportunities remain scarce across geographies: in none of the locations analyzed are more than 7% of Architect postings open to workers with two or fewer years of experience. Advanced workers are most demanded in Washington, D.C., where over 50% of openings request workers with over eight years of experience.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**302 (4%)**	**5,356 (64%)**	**2,751 (33%)**
Bay Area	39 (5%)	490 (61%)	276 (34%)
Boston	13 (5%)	198 (68%)	78 (27%)
Chicago	33 (7%)	294 (59%)	170 (34%)
Miami	0 (0%)	59 (74%)	21 (26%)
New York	28 (3%)	493 (62%)	280 (35%)
Southern Ohio	4 (3%)	101 (64%)	53 (34%)
Washington, D.C.	21 (3%)	368 (47%)	399 (51%)

Auditor

Auditors conduct security audits to assess the effectiveness of an organization's information security protocols and infrastructure. They may also investigate prior breaches to understand the factors that led to a breakdown in an organization's security systems. In 2014, there were over 7,500 postings for cybersecurity Auditors, representing 132% growth since 2010 – the fastest rate of demand growth across the cybersecurity landscape. Possibly as a result of this rapid growth, Auditor postings are taking longer to fill than any other cybersecurity job category, remaining open 43 days on average. This suggests that employers are having the greatest difficulty filling these emerging roles. Despite this hiring difficulty, advertised salaries are below the average for all cybersecurity roles, though they are still in excess of $80,000.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Auditor	7,533	132%	$80,750	43 Days

Auditors are among the most stringent cybersecurity job categories in terms of educational requirements, with virtually all openings demanding candidates with at least a four-year degree. In addition, 34% of openings request a graduate degree, of which 7% request a PhD.

Educational Requirements

	A.S.	B.S.	M.S.	Ph.D.
Auditor	74 (1%)	4,907 (65%)	2,055 (27%)	496 (7%)

Although Auditors are almost exclusively bachelor's-level jobs, they do offer strong entry-level opportunities. Almost one-third of Auditor job postings are open to workers with two or fewer years of experience, and only 2% of postings request workers with over eight years of experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Auditor	2,361 (31%)	5,017 (67%)	155 (2%)

Auditors are among the most hybridized cybersecurity jobs, as they require a diverse mix of auditing, risk management, business administration, data analysis, and information security expertise. These skills are rarely taught concurrently in training programs, which is likely responsible for a lack of workers possessing the skills needed for Auditor positions. This is also likely a prime driver of the heightened difficulty employers have filling these roles.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Internal Auditing	Oracle
Planning	Audit Planning	SAP
Writing	Risk Assessment	UNIX
Organizational Skills	Public Accounting	Enterprise Resource Planning (ERP)
Project Management	Business Process	SQL
Microsoft Excel	Audit Reports	ITIL
Microsoft Office	Sarbanes-Oxley (SOX)	PeopleSoft
Building Effective Relationships	Audit Experience	LINUX
Problem Solving	Risk Management	Word Processing
Analytical Skills	Information Security	SAS
Presentation Skills	Business Administration	SQL Server
Research	Mainframes	Microsoft SQL
Microsoft PowerPoint	Operational Auditing	JD Edwards
Detail-Oriented	Generally accepted Accounting Principles (GAAP)	IBM Resource Access Control Facility (RACF)
Computer Skills	Sarbanes-Oxley (Sox) Audit	Visual Basic
Change Management	Management Information System (MIS)	Hyperion
Supervisory Skills	Data Analysis	Sybase
Multi-Tasking	Audit Program Development	Virtual Private Networking (VPN)
Time Management	Financial Auditing	Cisco
Microsoft Visio	Financial Reporting	Microsoft SharePoint

Cybersecurity Auditors are also among the most heavily certified positions in cybersecurity, with over 60% of openings requesting CISA certification. Over 40% of postings also request a CPA, and 21% of postings request a CISSP, which few workers are likely to have in conjunction with some of the auditing and accounting-related credentials also requested among Auditor positions.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Auditor (CISA)	4,730	63%
Certified Public Accountant	3,316	44%
Certified Information Systems Security Professional (CISSP)	1,573	21%
Certified Fraud Examiner	792	11%
Certified Internal Auditor	662	9%
Certified Information Security Manager (CISM)	627	8%
IT Infrastructure Library	184	2%
Risk And Information Systems Control	157	2%
Project Management Certification (E.G. PMP)	150	2%
Certified In The Governance Of Enterprise IT	104	1%

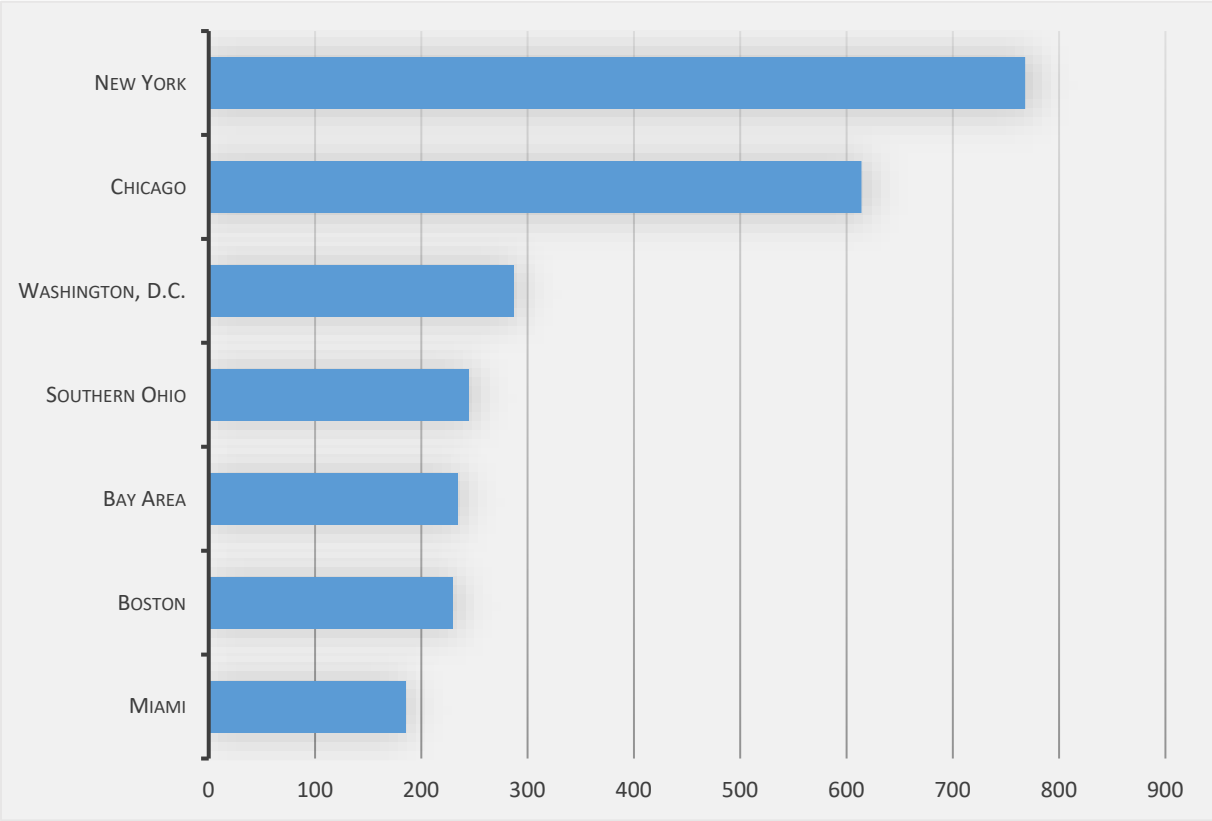
Cybersecurity auditors are most-demanded in New York, Chicago, and Atlanta, rather than Washington, D.C. or other defense and tech hubs where cybersecurity jobs are usually located. Moreover, Auditors are most heavily concentrated in finance and insurance hubs such as Bridgeport, Hartford, and Charlotte.

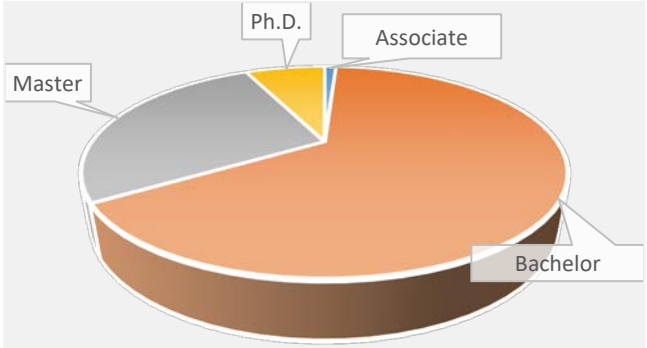
Top Metropolitan Areas

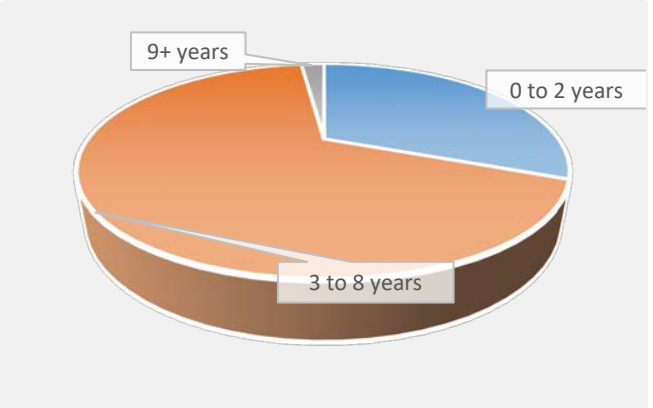
Metro Area	Postings
New York	768
Chicago	614
Atlanta	330
Dallas	291
Washington, D.C.	287
Los Angeles	231
Boston	230
Philadelphia	192
Houston	186
Miami	185

Metro Area	Location Quotient
Bridgeport	4.5
Hartford, CT	2.9
Chicago	2.5
Atlanta	2.5
Milwaukee	2.5
Richmond, VA	2.4
Cincinnati	2.1
Columbus	2.0
Charlotte	2.0
Washington, D.C.	1.7

Job Postings for Auditors (7,533 Nationally)







Location Analysis

Demand for cybersecurity Auditors has grown rapidly across key geographies, but the most dramatic growth has occurred in Chicago, Miami, and Southern Ohio. In each location, demand has surged multiple times faster than the national average. This may be a result of the main industries in these locations – which are not the traditional targets for cybersecurity of defense or technology – demanding workers to audit and improve their existing information security infrastructures. These locations also see some of the longest average posting durations for Auditors, suggesting they suffer from the greatest dearth of qualified Auditor candidates. With the exception of Southern Ohio, these fast-growing locations for Auditors also have above average advertised salaries, though they are still well below the average advertised salaries in the Bay Area, New York, and Washington, D.C., which are all in excess of $90,000.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**7,533**	**132%**	**$80,750**	**43 Days**	**1.0**
Bay Area	234	92%	$98,332	37 Days	1.4
Boston	230	107%	$70,666	32 Days	1.6
Chicago	614	234%	$82,800	49 Days	2.5
Miami	185	340%	$81,749	48 Days	1.4
New York	768	128%	$93,800	40 Days	1.6
Southern Ohio	245	528%	$77,343	44 Days	1.8
Washington, D.C.	287	90%	$94,472	46 Days	1.7

In all locations, cybersecurity Auditors are almost exclusively bachelor's-level jobs or above, which is in-line with national norms. In Boston their educational requirements spike, with almost half of all openings requesting a graduate degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**74 (1%)**	**4,907 (65%)**	**2,055 (27%)**	**496 (7%)**
Bay Area	1 (<1%)	169 (72%)	50 (21%)	13 (6%)
Boston	2 (1%)	116 (50%)	58 (25%)	54 (24%)
Chicago	5 (<1%)	401 (65%)	158 (26%)	50 (8%)
Miami	1 (<1%)	119 (64%)	52 (28%)	13 (7%)
New York	8 (1%)	465 (61%)	241 (31%)	54 (7%)
Southern Ohio	4 (2%)	200 (82%)	34 (14%)	8 (3%)
Washington, D.C.	5 (2%)	222 (77%)	49 (17%)	11 (4%)

Cybersecurity Auditors also offer strong entry-level opportunities across geographies. In every location over 20% of Auditor openings seek candidates with no more than two years of experience, and in Boston over 40% of openings are open to entry-level workers.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**2,361 (31%)**	**5,017 (67%)**	**155 (2%)**
Bay Area	54 (23%)	179 (76%)	1 (<1%)
Boston	93 (41%)	135 (59%)	1 (<1%)
Chicago	188 (31%)	412 (67%)	15 (2%)
Miami	60 (33%)	123 (67%)	1 (<1%)
New York	220 (29%)	534 (69%)	14 (2%)
Southern Ohio	91 (37%)	152 (62%)	1 (<1%)
Washington, D.C.	87 (30%)	184 (64%)	16 (6%)

Consultant

Consultants provide advice to inform the design and implementation of an organization's information security solutions. Consultants are the smallest cybersecurity job category in terms of total postings, as well as the slowest growing. From 2010 to 2014, demand for cybersecurity Consultants grew a relatively modest 44%. Consultants also show the least evidence of a skills gap, with postings remaining open only 31 days on average. Nonetheless, Consultant positions are still highly lucrative, advertising average salaries of $95,311.

Summary Statistics

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Consultant	6,294	44%	$95,311	31 Days

Although Consultant positions are lucrative, they are primarily bachelor's-level positions. Only 11% of jobs are open to workers without a bachelor's degree, and 20% of openings request graduate-level credentials.

Educational Requirements

	3A.S.	B.S.	M.S.	Ph.D.
Consultant	671 (11%)	4,388 (70%)	1,076 (17%)	158 (3%)

Despite the heightened educational requirements for Consultants, there are stronger opportunities for entry-level job seekers, with 19% of openings requesting candidates with no more than two years of previous work experience. Most of the remaining openings are seeking mid-level workers, with 69% of postings requesting workers with three to eight years of experience.

Experience Requirements

	0 to 2 years	3 to 8 years	9+ years
Consultant	1,222 (19%)	4,345 (69%)	728 (12%)

In additional to core cybersecurity and networking skills, Consultants require knowledge of risk management and risk assessment, legal compliance, and auditing. Some Consulting positions also require programming skills such as Java, C++, and Python.

Top Skills

Baseline Skills	Specialized Skills	Software and Programming Skills
Communication Skills	Information Security	UNIX
Organizational Skills	Firewalls	Oracle
Writing	Network Security	JAVA
Project Management	Business Process	LINUX
Problem Solving	Cryptography	SAP
Planning	HIPAA	SQL
Customer Service	Risk Management	Cisco
Presentation Skills	Risk Assessment	Transmission Control Protocol - Internet Protocol (TCP - IP)
Troubleshooting	Network Engineering	PERL
Research	System and Network Configuration	C++
Building Effective Relationships	Legal Compliance	Python
Microsoft Office	Sales	Virtual Private Networking (VPN)
Microsoft Excel	Internal Auditing	Enterprise Resource Planning (ERP)
Time Management	Business Development	ITIL
Analytical Skills	Sarbanes-Oxley (SOX)	McAfee
Detail-Oriented	Mentoring	Symantec Packages
English	Technical Writing - Editing	.NET Programming
Leadership	System Architecture	ArcSight
Microsoft PowerPoint	Technical Support	Tivoli
Project Planning and Development Skills	Workshops	Microsoft C#

Consultants are heavily certificated, with 32% of postings requesting a CISSP, 22% requesting a CISA, and 13% requesting a CISM.

Top Certifications

Certification	Postings	Percent of Title Area
Certified Information Systems Security Professional (CISSP)	4,730	32%
Certified Information Systems Auditor (CISA)	3,316	22%
Certified Information Security Manager (CISM)	1,573	13%
Certified Public Accountant	792	5%
Project Management Certification (E.G. PMP)	662	3%
Cisco Certified Network Associate	627	3%
GIAC Security Essentials	184	2%
Certified In Risk And Information Systems Control	157	2%
Microsoft Certified Systems Engineer (MCSE)	150	2%
IT Infrastructure Library	104	2%

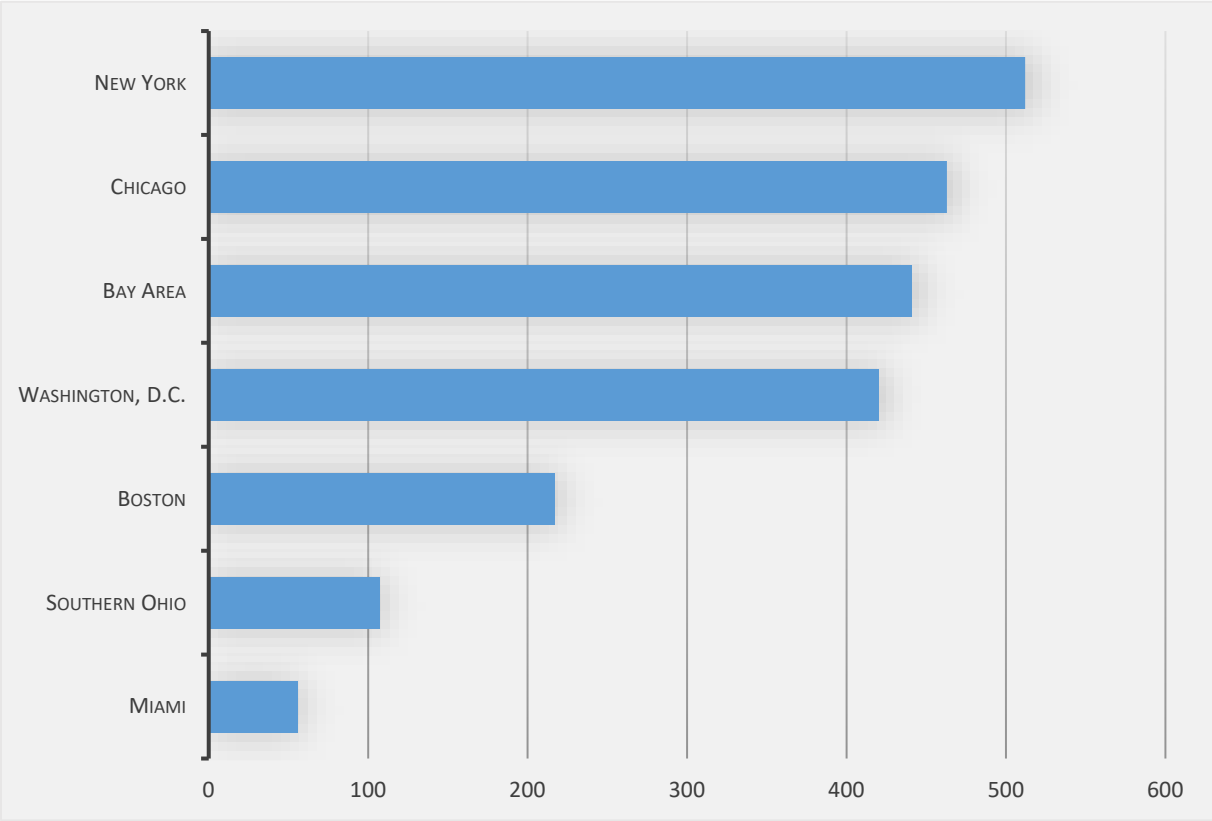
New York and Chicago are the top locations for cybersecurity Consultants, with Washington, D.C. coming in a close third. San Jose has the greatest concentration of demand for Consultants, though emerging markets for cybersecurity – such as Charlotte and Minneapolis – also show strong concentrations of openings for cybersecurity Consultants.

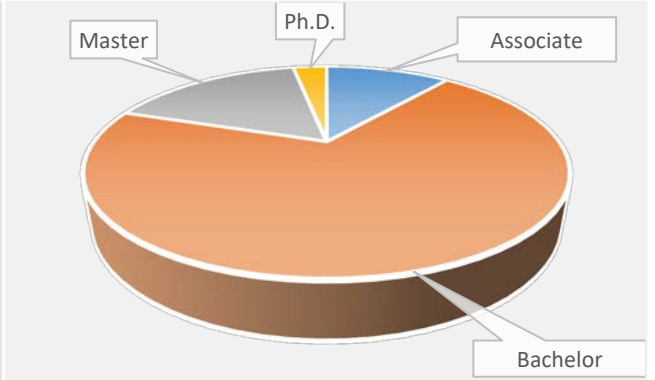
Top Metropolitan Areas

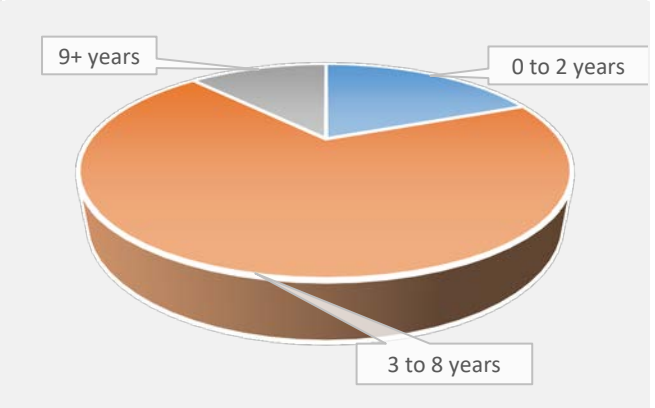
Metro Area	Postings
New York	512
Chicago	463
Washington, D.C.	420
Dallas	362
San Francisco	277
Boston	217
Atlanta	210
Los Angeles	201
Minneapolis	183
San Jose	164

Metro Area	Location Quotient
San Jose	3.6
Washington, D.C.	3.1
San Francisco	2.8
Charlotte	2.8
Dallas	2.5
Austin	2.3
Denver	2.3
Chicago	2.3
Kansas City	2.2
Minneapolis	2.2

Job Postings for Consultants (6,294 Nationally)







Location Analysis

Across the key geographies, demand growth for Consultants has fluctuated between 123% in Chicago to a decrease of 27% in Washington, D.C. Salaries also vary widely, ranging from about $75,000 in Miami to over $115,000 in Boston and Southern Ohio. Average posting durations are consistently below the overall average for cybersecurity, although they are considerably longer than the overall average for Consultants in Chicago and the Bay Area – in each city, Consultant job postings remain open for 39 days on average.

	Total Postings	Growth (2010 to 2014)	Average Salary	Average Days Open	Location Quotient
Nationally	**6,294**	**44%**	**$95,311**	**31 Days**	**1.0**
Bay Area	441	74%	$96,680	39 Days	3.1
Boston	217	113%	$116,409	33 Days	1.8
Chicago	463	123%	$102,315	39 Days	2.3
Miami	56	40%	$75,263	36 Days	0.5
New York	512	21%	$92,135	29 Days	1.3
Southern Ohio	107	51%	$117,198	24 Days	1.0
Washington, D.C.	420	-27%	$111,330	32 Days	3.1

Opportunities for Consultants consistently require, at minimum, a bachelor's degree across geographies. In every location except Southern Ohio fewer than 10% of openings call for candidates with less than a four-year degree.

	A.S.	B.S.	M.S.	Ph.D.
Nationally	**671 (11%)**	**4,388 (70%)**	**1,076 (17%)**	**158 (3%)**
Bay Area	26 (6%)	342 (78%)	61 (14%)	11 (3%)
Boston	19 (9%)	153 (71%)	39 (18%)	6 (3%)
Chicago	19 (4%)	364 (79%)	72 (16%)	8 (2%)
Miami	2 (3%)	42 (76%)	12 (22%)	0 (0%)
New York	25 (5%)	355 (69%)	117 (23%)	14 (3%)
Southern Ohio	13 (12%)	69 (65%)	24 (23%)	0 (0%)
Washington, D.C.	33 (8%)	296 (71%)	65 (15%)	26 (6%)

Consultants are primarily experienced-level roles – over 75% of Consultant postings in each location require at least three years of work experience – but entry-level opportunities vary widely. In Miami and Southern Ohio, only 8% of Consultant openings are entry-level; in Chicago and New York, however, almost 25% of postings request entry-level candidates.

	0 to 2 years	3 to 8 years	9+ years
Nationally	**1,222 (19%)**	**4,345 (69%)**	**728 (12%)**
Bay Area	70 (16%)	312 (71%)	59 (13%)
Boston	42 (19%)	155 (71%)	20 (9%)
Chicago	107 (23%)	314 (68%)	41 (9%)
Miami	5 (8%)	47 (84%)	5 (8%)
New York	121 (24%)	335 (65%)	56 (11%)
Southern Ohio	8 (8%)	87 (81%)	12 (11%)
Washington, D.C.	79 (19%)	281 (67%)	60 (14%)

REGIONAL ANALYSIS

Bay Area

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**13,869**	**88%**	**$117,026**	**42 Days**
Engineer	3,749	61%	$115,418	39 Days
Manager	1,666	65%	$100,304	40 Days
Analyst	1,073	126%	$94,886	42 Days
Specialist	521	167%	$80,420	29 Days
Architect	805	120%	$136,180	42 Days
Auditor	234	92%	$98,332	37 Days
Consultant	441	74%	$96,680	39 Days

Boston

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**6,918**	**99%**	**$104,384**	**40 Days**
Engineer	1,608	97%	$102,920	45 Days
Manager	872	67%	$103,302	37 Days
Analyst	658	147%	$89,381	35 Days
Specialist	215	60%	$88,945	21 Days
Architect	289	64%	$111,621	42 Days
Auditor	230	107%	$70,666	32 Days
Consultant	217	113%	$116,409	33 Days

Chicago

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**9,623**	**164%**	**$102,301**	**41 Days**
Engineer	1,527	143%	$103,993	39 Days
Manager	1,210	145%	$106,640	41 Days
Analyst	1,068	286%	$86,885	39 Days
Specialist	338	132%	$83,421	35 Days
Architect	497	125%	$115,115	32 Days
Auditor	614	234%	$82,800	49 Days
Consultant	463	123%	$102,315	39 Days

Miami

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**2,872**	**158%**	**$93,050**	**39 Days**
Engineer	532	173%	$87,975	34 Days
Manager	461	152%	$96,239	43 Days
Analyst	399	146%	$67,732	37 Days
Specialist	108	42%	$60,386	35 Days
Architect	80	176%	$96,944	37 Days
Auditor	185	340%	$81,749	48 Days
Consultant	56	40%	$75,263	36 Days

New York

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**17,982**	**90%**	**$111,202**	**36 Days**
Engineer	2,778	89%	$107,440	34 Days
Manager	2,468	81%	$108,481	37 Days
Analyst	1,853	72%	$101,241	36 Days
Specialist	558	42%	$100,954	29 Days
Architect	801	100%	$125,500	29 Days
Auditor	768	128%	$93,800	40 Days
Consultant	512	21%	$92,135	29 Days

Southern Ohio

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**3,908**	**151%**	**$84,257**	**31 Days**
Engineer	533	118%	$91,393	29 Days
Manager	449	94%	$79,183	27 Days
Analyst	507	137%	$67,900	33 Days
Specialist	278	136%	$75,948	25 Days
Architect	158	63%	$105,024	25 Days
Auditor	245	528%	$77,343	44 Days
Consultant	107	51%	$117,198	24 Days

Washington, D.C.

	Total Postings	Growth (2010-2014)	Average Salary	Average Days Open
Overall	**27,246**	**39%**	**$108,908**	**37 Days**
Engineer	5,793	13%	$101,233	37 Days
Manager	3,094	47%	$98,282	37 Days
Analyst	2,817	7%	$94,387	37 Days
Specialist	2,570	78%	$103,994	31 Days
Architect	788	38%	$117,029	39 Days
Auditor	287	90%	$94,472	46 Days
Consultant	420	-27%	$111,330	32 Days

ACKNOWLEDGEMNTS

We would like to express our gratitude to the individuals and organizations that have made this report possible.

First, we want to thank Burning Glass Technologies for their commitment and contributions to this research. In particular, we are grateful for the leadership of Will Markow and the analysis, insights, and commentary of Josh Konieczny and Matej Mavricek. Their selection of the appropriate data to include in this report demonstrated a real understanding of the career issues facing our young college graduates.

We are especially thankful for the direction, guidance and support of BATEC's National Visiting Committee and the contributions of BATEC's Academic Partners. Together, this collaborative group of engaged professionals bring heart, meaning and substance to the issues of Technical Education.

There are many who have contributed their ideas and input throughout this research project. That said, all errors, omissions, and views remain the responsibility of the authors.

About BATEC

www.batec.org

BATEC (Broadening Advanced Technological Education Connections), a National Science Foundation-funded Center of Excellence for Computing and Information Technologies, is dedicated to the complex mission of developing career-focused pathways and practical work experience for motivated, typically underserved high school, community college and university students in urban environments which feature a high demand for skilled labor.

About Burning Glass

www.burning-glass.com

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. Burning Glass is reshaping how the job market works, with data that identify the skill gaps that keep job seekers and employers apart and tools that enable both sides to bridge that gap and connect more easily. Based in Boston, Burning Glass is playing a growing role in informing the global conversation on education and the workforce, and in creating a job market that works for everyone.

About NSF

www.nsf.gov

The National Science Foundation's (NSF) Advanced Technological Education (ATE) program seeks to improve the education of technicians who work in advanced industries that are important to the nation's economy and security. The program involves partnerships between academic institutions and industry to promote improvement in the education of science and engineering technicians at the undergraduate and secondary school levels. The ATE program supports curriculum development; professional development of college

faculty and secondary school teachers; career pathways to two-year colleges from secondary schools and from two-year colleges to four-year institutions; and other activities.

This report was prepared with support from the National Science Foundation under grant DUE-110415 to the University of Massachusetts. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the editor and the principal investigators of the BATEC ATE Center. They do not necessarily reflect the views of the National Science Foundation.

BATEC

National Center of Excellence for Computing and Information Technologies
Headquartered at University of Massachusetts Boston
www.batec.org

- College and Career Pathways
- Employability and Problem-Solving Skills
- Internship Opportunities
- Industry Trends and Workforce Needs
- Education, Business, and Community Connections

Serving Boston, Chicago, Las Vegas, and San Francisco

UMASS BOSTON

COLLEGE OF ADVANCING AND PROFESSIONAL STUDIES
UNIVERSITY OF MASSACHUSETTS BOSTON

UMass Boston is a public research university with a dynamic culture of teaching and learning, and a special commitment to urban and global engagement. BATEC is headquartered in the College of Advancing and Professional Studies (CAPS) at UMass Boston, offering an opportunity to address the workforce and community needs of our regions.

UMASS BOSTON

Cyber Training Best Practices

Federal Government Segment

©2016,Comtech Telecommunications Corp. Proprietary Level 2

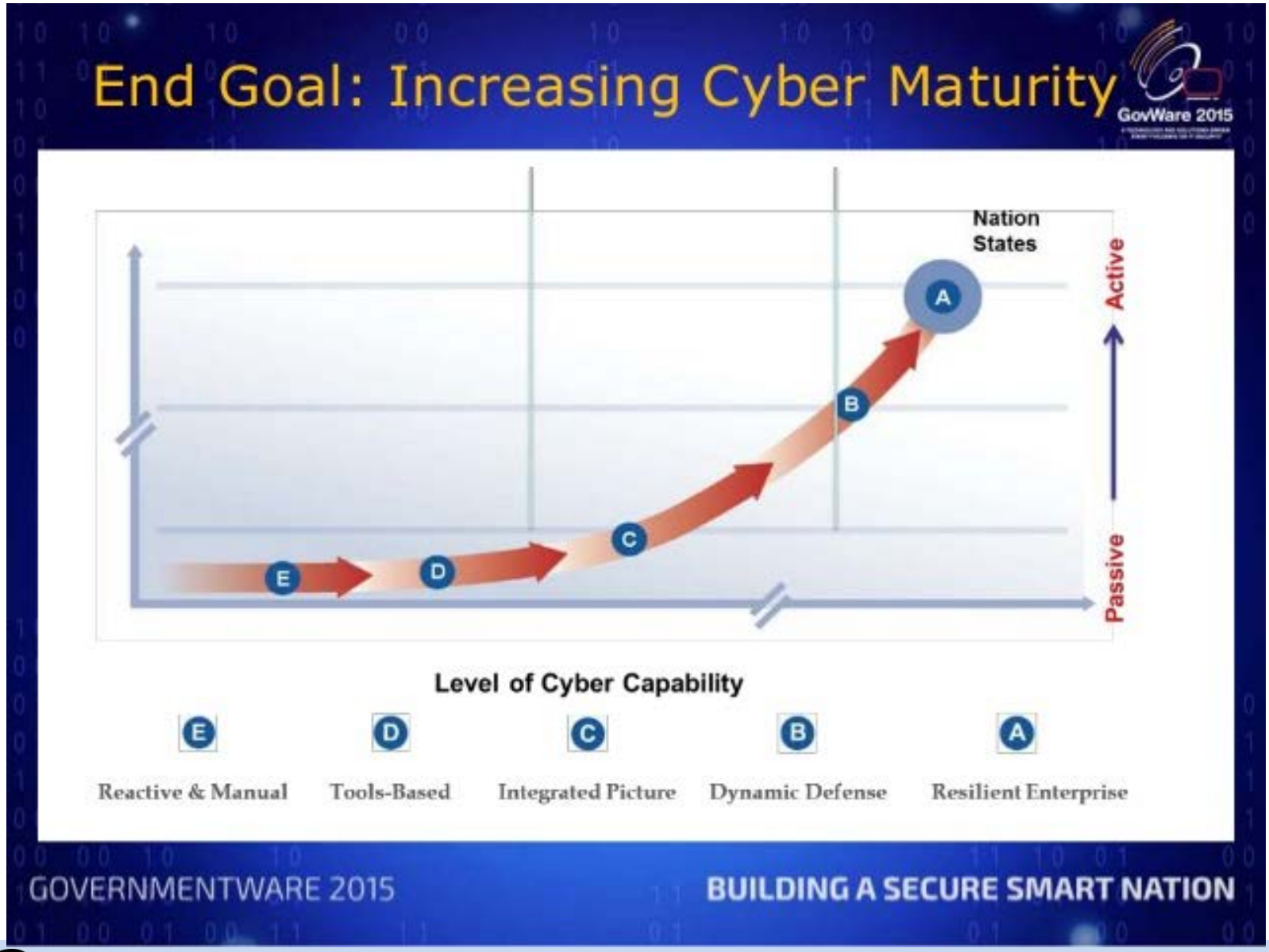
COMTECH
Command & Control Technologies

Leader in Competency-Based, Performance-Based, and Role-Based Cyber Security Education Tools and Training

- Cyber Security Training
  - AoE™ Flagship
  - JCAC – Information Warfare Training Center
  - Custom Curriculum – ISACA, CISCO
  - Commercial and International Government SOC Training
- Assessment Methods
  - PerformanScore™
  - TalentScore™
  - ITADS – Intelligent Tutoring

©2016, Comtech Telecommunications Corp. Proprietary Level 2

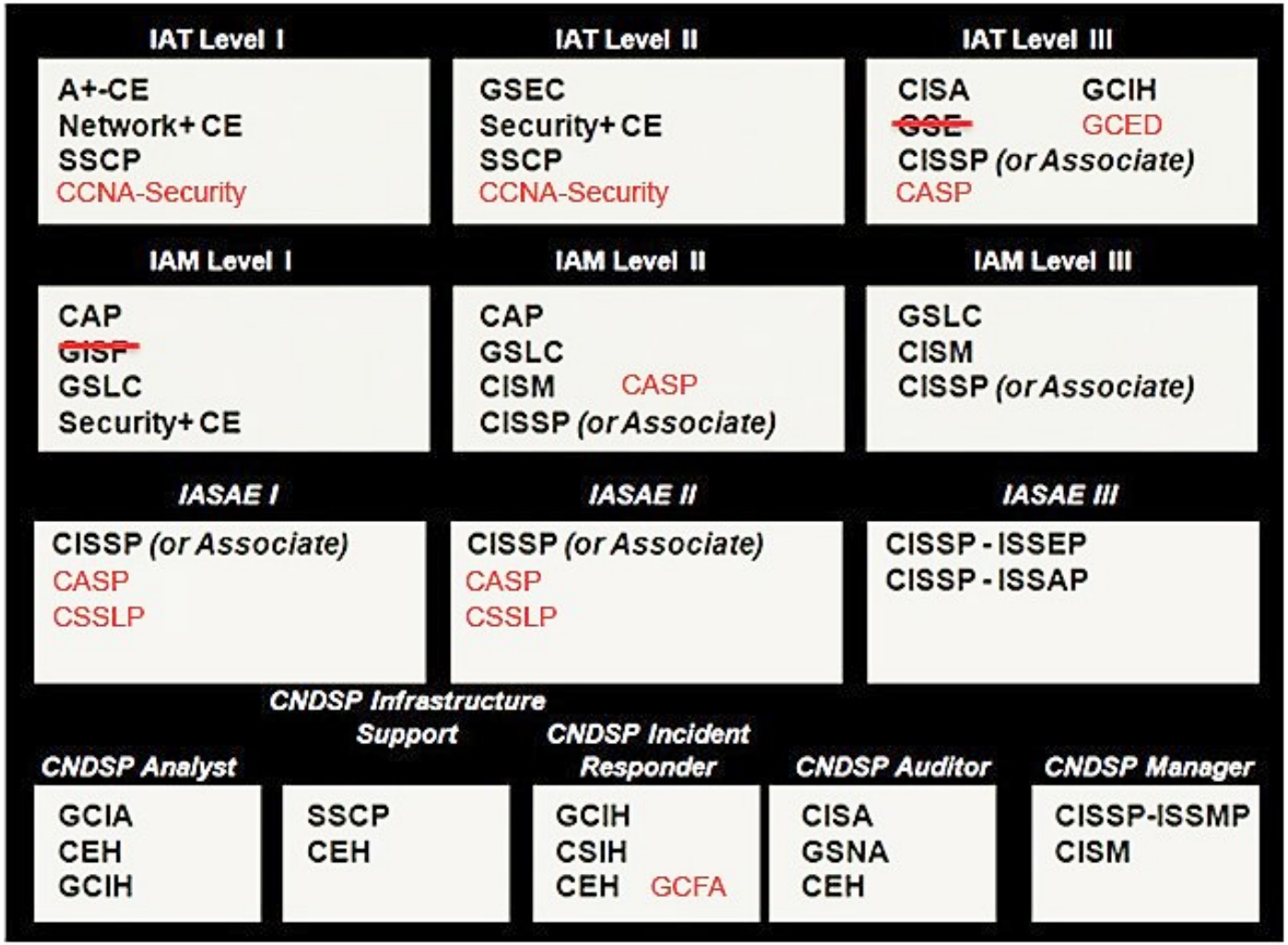
How to increase cyber maturity



©2016, Comtech Telecommunications Corp. Proprietary Level 2

8570 – Certification Based

Table AP3.T2 DoD Approved Baseline Certifications



8140 – Performance Based

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate & Maintain	Data Administration	Info System Security Mgt	Knowledge Mgt	Customer & Tech Support	Network Services	System Administration	Systems Security Analysis
Protect & Defend	Computer Network Defense (CND)	Incident Response	CND Infrastructure Support	Security Program Mgt	Vulnerability Assessment & Mgt		
Analyze	Cyber Threat Analysis	Exploitation Analysis	All-source Analysis	Targets			
Operate & Collect	Collection Operations	Cyber Operational Planning	Cyber Operations				
Oversight & Development	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training				
Investigate	Investigation	Digital Forensics					

Establishing National Standards

Job

Task/Workrole

Knowledge, Skills, and Abilities (KSA)

and 8140

Best Practices in Cyber Training

- Pre Assessment
- Training Plan
- Training
- Tutoring / Mentoring
- Post Assessment (certification)

- Items needed for Successful Training
  - Cyber Range / Labs
  - Training /Curriculum
  - Assessment / Scoring
- Long Term Measurement of Training and Outcomes (Analytics)

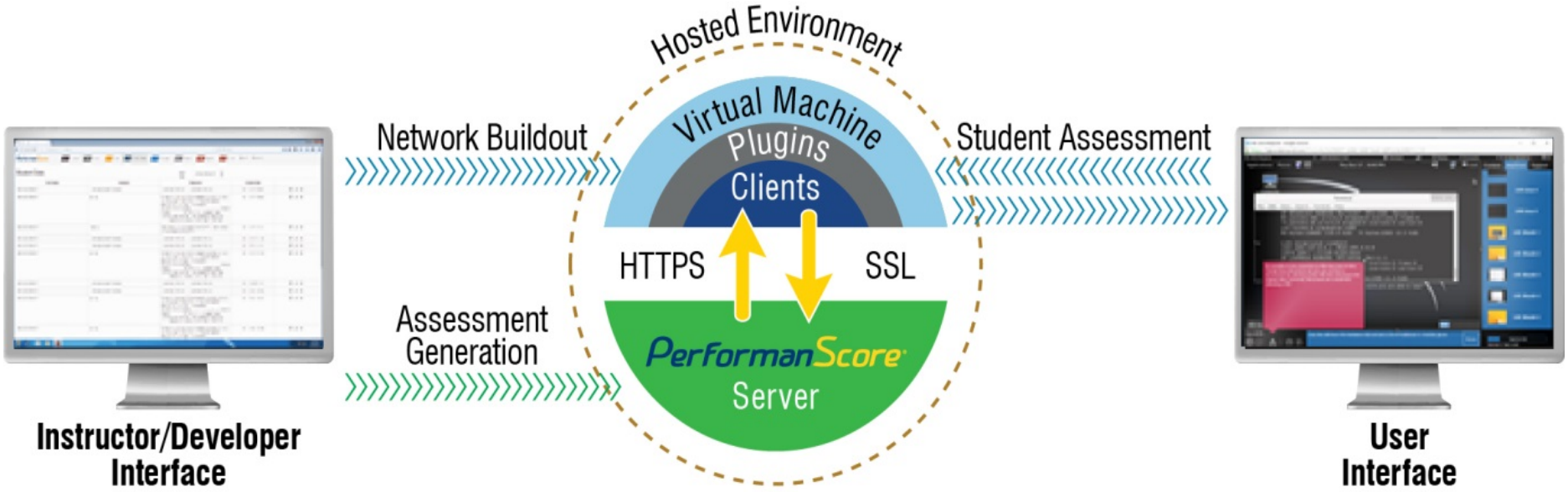
©2016, Comtech Telecommunications Corp. Proprietary Level 2

Best Practices (Representative examples)

- Nation States
  - Range Environment
  - Heavy hands on - 60/40 ratio Hands on/Training
  - Knowledge is not sufficient
  - Hands on training in realistic simulated environments
  - Assessment (Pre/Post)
- Government Trainer
  - Range Environment
  - Movement to hands on
  - Performance Based Assessment
  - Asynchronous Delivery
- DoD
  - Range Environment
  - Performance based Assessments
  - ASVAB, A school, B school tracking and analytics
- Major Certification Provider
  - Range Environment
  - Commercially Available Performance Based Assessment
  - Mapped to CSF
  - Hands On
  - Government and Industry Customers
  - Asynchronous Delivery

©2016, Comtech Telecommunications Corp. Proprietary Level 2

Performance Based Scoring



PerformanScore (PnS) is a tool that scores a user based on their ability to perform specific tasks. As a user works through an activity, plugins and clients monitor, collect, and send completed tasks to a scoring server that assesses their progress against a performance rubric. A task completion score is automatically calculated and reported to authorized agents when the activity is completed.

©2016, Comtech Telecommunications Corp. Proprietary Level 2

Contact Us

Erik Wallace
Director, Product Management
410-280-1184 (o) | 443-223-6230 (m)

275 West Street
Annapolis, MD 21401

Erik.Wallace@
comtechtel.com

@comtechtel.com

www.comtechtel.com

©2016, Comtech Telecommunications Corp. Proprietary Level 2

State CIO Priorities for 2016

November 10, 2015

A. Priority Strategies, Management Processes and Solutions
Top 10 Final Ranking

1. **Security and Risk Management**: governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases, determining what constitutes "due care" or "reasonable"

2. **Cloud Services**: cloud strategy, proper selection of service and deployment models, scalable and elastic IT-enabled capabilities provided "as a service" using internet technologies, governance, service management, service catalogs, platform, infrastructure, security, privacy, data ownership

3. **Consolidation/Optimization**: centralizing, consolidating services, operations, resources, infrastructure, data centers, communications and marketing "enterprise" thinking, identifying and dealing with barriers

4. **Business Intelligence and Data Analytics**: applying BI/BA within the enterprise, communicating the value, building expertise, delivering shared services, exploring big data, data analytics

5. **Legacy Modernization**: enhancing, renovating, replacing, legacy platforms and applications, business process improvement

6. **Enterprise Vision and Roadmap for IT**: vision and roadmap for IT, recognition by administration that IT is a strategic capability, integrating and influencing strategic planning and visioning with consideration of future IT innovations, aligning with Governor's policy agenda

7. **Budget and Cost Control**: managing budget reduction, strategies for savings, reducing or avoiding costs, dealing with inadequate funding and budget constraints

8. **Human Resources/Talent Management**: human capital/IT workforce, workforce reduction, attracting, developing and retaining IT personnel, retirement wave planning, succession planning, support/training, portal for workforce data and trends

9. **Agile and Incremental Software Delivery**: iterative design and incremental development of software solutions, allows for design modifications, prototyping and addition of new capabilities as part of the development process

10. **Disaster Recovery/Business Continuity**: improving disaster recovery, business continuity planning and readiness, pandemic/epidemic and IT impact, testing

B. Priority Technologies, Applications and Tools
Top 10 Final Ranking

1. **Security Enhancement Tools**: continuous diagnostic monitoring (CDM), digital forensics
2. **Cloud Solutions**: software as a service
3. **Legacy Application Modernization/Renovation**
4. **Data Management**: master client index/master data management, information exchanges (e.g., health, justice, transportation, environmental)
5. **Business Intelligence (BI), Business Analytics (BA)**: applications, big data, data analytics
6. **Identity and Access Management**: technologies and solutions
7. **Mobile Workforce**: technologies and solutions
8. **Virtualization**: servers, desktop, storage, applications, data center
9. **Networking**: voice and data communications, unified
10. **Document/Content/Records/E-mail Management**

State Level Cybersecurity Workforce Initiatives

This document provides supplemental information for each state that highlights cybersecurity specific workforce development initiatives and participating institutions.

States

Alabama

- MS-ISAC link http://www.cybersecurity.alabama.gov/ - no specific workforce initiatives noted
- CAE schools

Institution	Designation	Designated	Expiration
Auburn University	CAE-CDE 4Y	2014	2020
	CAE-R	2014	2019
Jacksonville State University	CAE-CDE 4Y	2014	2021
Northeast Alabama Community College	CAE-CDE 2Y	2014	2019
Snead State Community College	CAE/IAE 2Y	2012	2017
The University of Alabama	CAE-R	2014	2019
The University of Alabama at Birmingham	CAE-IA-R	2012	2017
	CAE-R	2014	2019
Tuskegee University	CAE/IAE 4Y	2012	2017
University of Alabama, Huntsville	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of South Alabama	CAE-CDE 4Y	2014	2021

Alaska

- MS-ISAC link broken
- No specific cybersecurity workforce initiatives noted discovered
- some cybersecurity coverage via e-newsletters found on http://doa.alaska.gov/ets/security/newsletters/
- No CAE schools

Arizona

- https://aset.az.gov/security - no specific workforce initiatives noted

Institution	Designation	Designated	Expiration
Arizona State University	CAE/IAE 4Y	2012	2017

	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Estrella Mountain Community College	CAE-CDE 2Y	2014	2019
The University of Arizona, Tucson	CAE-CDE 4Y	2014	2021
University of Advancing Technology	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2020

Arkansas

- http://www.adem.arkansas.gov/AEM/index.php - Department of Emergency Management Site – no specific cybersecurity workforce initiatives noted

Institution	Designation	Designated	Expiration
University of Arkansas	CAE-IA-R	2012	2017
	CAE-R	2014	2019
University of Arkansas at Little Rock	CAE-CDE 4Y	2014	2021

California

- Cybersecurity Task Force http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force
  - Workforce Development and Education Subcommitee Objective 1 - Develop a consistent definition and criteria for cybersecurity expertise to serve the State of California http://www.caloes.ca.gov/cal-oes-divisions/Cybersecurity-Task-Force/Task-Force-Subcommittees/Workforce-Development-and-Education-Subcommittee
- MS-ISAC link http://www.cio.ca.gov/ois/
- https://oag.ca.gov/cybersecurity
- The California Apprenticeship Initiative (CAI) Grant from the Community College Chancellor's Office to define, develop, and deploy a cybersecurity apprenticeship program. http://extranet.cccco.edu/Divisions/WorkforceandEconDev/PolicyAlignmentandOutreach/Apprenticeship.aspx

Institution	Designation	Designated	Expiration
California State Polytechnic University, Pomona	CAE-CDE 4Y	2014	2021
California State University, Sacramento	CAE/IAE 4Y	2012	2017
California State University, San Bernardino	CAE-CDE 4Y	2014	2021
Coastline Community College	CAE-CDE 2Y	2014	2019
National University	CAE-CDE 4Y	2014	2020
Naval Postgraduate School	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
San Jose State University	CAE-CDE 4Y	2014	2019
University of California, Davis	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of California, Irvine	CAE-R	2014	2019

Colorado

- MS-ISAC link http://www.oit.state.co.us/ois

- In December 2015, Governor John Hickenlooper declared Colorado Springs as America's Cyber Capital, launching an initiative to focus Colorado's economic development efforts in cyber in the region.7 Employers, workforce planners, and education stakeholders recognize that these new investments in the cybersecurity sector reflect the importance of entry-level positions and a mature career pathway as a critical workforce development element. As part of Governor Hickenlooper's initiative, Pikes Peak Community College (PPCC) leaders agreed to develop a new cybersecurity associate degree program, supplemented by non-credit industry certification programs that would help to develop a qualified workforce quickly.

Institution	Designation	Designated	Expiration
Colorado School of Mines	CAE-CDE 4Y	2016	2021
Colorado State University-Pueblo	CAE-CDE 4Y	2016	2021
Colorado Technical University	CAE-CDE 4Y	2014	2021
Regis University	CAE/IAE 4Y	2012	2017
United States Air Force Academy	CAE-CDE 4Y	2014	2021
University of Colorado, Colorado Springs	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
University of Denver	CAE-CDE 4Y	2014	2020

Connecticut

- MS-ISAC link http://www.ct.gov/best/cwp/view.asp?a=1244&Q=301858
- House Bill No. 6317, Special Act No. 15-13 Be it enacted by the Senate and House of Representatives in General Assembly convened: Section 1. (Effective from passage) (a) The Department of Administrative Services, in consultation with the Department of Emergency Services and Public Protection, shall, within available appropriations, conduct a study to identify cybersecurity issues facing the state and to make recommendations regarding specific actions that the state can implement to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness. (b) Not later than January 1, 2017, the Department of Administrative Services shall submit the results of such study and any recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to public safety and security, in accordance with the provisions of section 11-4a of the general statutes. The UNH team has met and discussed House Bill No. 6317

Institution	Designation	Designated	Expiration
University of Connecticut	CAE-R	2014	2019

Delaware

- University of Delaware Cybersecurity Initiative (UDCSI) - The UD Cybersecurity Initiative (UDCSI) was established in 2014 as a partnership among the state, the University, federal agencies, and the private sector to advance education, training, and research for understanding, defining, addressing, and solving cybersecurity problems. UDCSI programs feature handson practical applications, a strong faculty, distinguished lectures series, and fundamental research focused on developing solutions to advancing threats, best practices and standard protocols for optimal security so that every type and size of business can protect itself. The Initiative works closely with the University's cybersecurity undergraduate minor and Masters' program, and is actively developing a state-supported cybersecurity range that will enable simulations which prepare existing and future cyber-professionals for real world

situations. The University of Delaware is accredited through the National Security Agency and the Department of Homeland Cyber Defense Education as a National Center of Academic Excellence in Cyber Defense Education through academic year 2021. UD's status as a CAE and the UDCSI's ongoing initiatives will serve as key resources available for assisting DACEE in the achievement of its goals.

- Under the leadership of Governor Markell, the State of Delaware has established several cyber-related initiatives in addition to its support for the UDCSI cybersecurity range. Executive Order 55 established the Delaware Cyber Security Council to promote cybersecurity partnerships among higher education, government, and small and large businesses and make recommendations on best practices for advancing security in Delaware. UDCSI's Director serves on the Council and will seek to engage members of this Council in the work of DACEE. The Governor also initiated the Delaware Blockchain Initiative to advance the State's standing as a desirable, efficient location to incorporate.
- Delaware TechHire Initiative
- Cyber Camp: Each summer the University of Delaware sponsors a US Cyber Challenge cybersecurity boot-camp that provides a week of workshops, skill building, a job fair, and a capture the flag competition. This program is aimed as high school, undergraduate, and graduate participants and is used as an outreach and recruitment platform.

Institution	Designation	Designated	Expiration
University of Delaware	CAE-CDE 4Y	2016	2021
Wilmington University	CAE-CDE 4Y	2014	2021

District of Columbia

Institution	Designation	Designated	Expiration
Georgetown University	CAE-R	2016	2021
The George Washington University	CAE-R	2014	2019

Florida

- New Skills for a New Fight (NSNF), a no-cost cybersecurity training and certification program for selected military veterans http://thefc2.org/education/forveterans.aspx

Institution	Designation	Designated	Expiration
Daytona State College	CAE-CDE 4Y	2016	2021
Embry-Riddle Aeronautical University - Daytona Beach Campus	CAE-CDE 4Y	2016	2021
Florida A&M University	CAE/IAE 4Y	2012	2017
Florida Atlantic University	CAE-IA-R	2012	2017
	CAE-R	2014	2019
Florida Institute of Technology	CAE-R	2014	2019
Florida International University	CAE-CDE 4Y	2014	2019
	CAE-R	2016	2021
Florida State University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Nova Southeastern University	CAE-CDE 4Y	2014	2021

Saint Leo University	CAE-CDE 4Y	2016	2021
University of Central Florida	CAE-CDE 4Y	2016	2021
University of Florida	CAE-R	2014	2019
University of South Florida	CAE-CDE 4Y	2014	2019
University of West Florida	CAE-CDE 4Y	2016	2021
Valencia College	CAE/IAE 2Y	2012	2017

Georgia

Armstrong State University	CAE-CDE 4Y	2016	2021
Augusta University	CAE-CDE 4Y	2016	2021
Columbus State University	CAE-CDE 4Y	2016	2021
Georgia Institute of Technology	CAE-R	2014	2019
Kennesaw State University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
University of North Georgia	CAE-CDE 4Y	2016	2021

Hawaii

Institution	Designation	Designated	Expiration
Honolulu Community College	CAE-CDE 2Y	2014	2021
University of Hawaii – West Oahu	CAE-CDE 4Y	2016	2021
University of Hawaii at Manoa	CAE-R	2014	2019

Idaho

Institution	Designation	Designated	Expiration
Idaho State University	CAE-CDE 4Y	2014	2020
University of Idaho	CAE-CDE 4Y	2014	2021

Illinois

- Kirk Lonbom, the state's CISO, is putting together a cybersecurity workforce hiring plan for the state.

Institution	Designation	Designated	Expiration
DePaul University	CAE-CDE 4Y	2014	2021
Illinois Institute of Technology	CAE-CDE 4Y	2014	2020
Illinois State University	CAE-CDE 4Y	2014	2020
John A Logan College	CAE-CDE 2Y	2016	2021
Lewis University	CAE-CDE 4Y	2016	2021
Moraine Valley Community College	CAE-CDE 2Y	2014	2020
University of Illinois at Springfield	CAE-CDE 4Y	2014	2020
University of Illinois, Urbana-Champaign	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

Indiana

Indiana

Institution	Designation	Designated	Expiration
Indiana University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Ivy Tech Community College	CAE/IAE 2Y	2012	2017
Purdue University	CAE-R	2014	2019
Purdue University Calumet	CAE-CDE 4Y	2014	2019

Iowa

Iowa State University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

Kansas

Institution	Designation	Designated	Expiration
Fort Hays State University	CAE-CDE 4Y	2014	2020
Kansas State University	CAE-R	2014	2019
University of Kansas	CAE-CDE 4Y	2014	2020

Kentucky

Institution	Designation	Designated	Expiration
Northern Kentucky University	CAE-CDE 4Y	2014	2019
University of Louisville, Kentucky	CAE-CDE 4Y	2014	2019

Louisiana

- http://www.louisianabelieves.com/ - Cyber Engineering Pathway
  - http://www.louisianabelieves.com/docs/default-source/jumpstart/cyber-engineering-pathway.pdf?sfvrsn=14

Institution	Designation	Designated	Expiration
Bossier Parish Community College	CAE/IAE 2Y	2012	2017
	CAE-CDE 2Y	2014	2021
Louisiana Tech University	CAE-CDE 4Y	2014	2020
	CAE-IA-R	2012	2017
	CAE-R	2014	2020
University of New Orleans	CAE-R	2014	2019

Maine

Maine

Institution	Designation	Designated	Expiration
University of Maine System	CAE-CDE 4Y	2014	2019

Maryland

- Department of Labor TAACCCT Grant - http://webapps.dol.gov/DOLGrantData/GrantInformation.aspx?appid=20256

Institution	Designation	Designated	Expiration
Anne Arundel Community College	CAE-CDE 2Y	2014	2020
Bowie State University	CAE-CDE 4Y	2014	2020
Capitol Technology University	CAE-CDE 4Y	2014	2021
College of Southern Maryland	CAE-CDE 2Y	2014	2020
Hagerstown Community College	CAE-CDE 2Y	2014	2020
Harford Community College	CAE/IAE 2Y	2012	2017
	CAE-CDE 2Y	2014	2020
Howard Community College	CAE-CDE 2Y	2014	2020
Montgomery College	CAE/IAE 2Y	2012	2017
Morgan State University	CAE-CDE 4Y	2016	2021
Prince George's Community College	CAE-CDE 2Y	2014	2021
The Community College of Baltimore County	CAE-CDE 2Y	2014	2021
The Johns Hopkins University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Towson University	CAE-CDE 4Y	2014	2021
United States Naval Academy	CAE-CDE 4Y	2014	2020
University of Maryland University College	CAE-CDE 4Y	2014	2021
University of Maryland, Baltimore County	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of Maryland, College Park	CAE-R	2014	2019

Massachusetts

Institution	Designation	Designated	Expiration
Boston University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Northeastern University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of Massachusetts Lowell	CAE-R	2016	2021

Worcester Polytechnic Institute	CAE-R	2014	2019

Michigan

- MS-ISAC link http://www.michigan.gov/cybersecurity/ - no specific workforce initiatives noted beyond cybersecurity awareness

Institution	Designation	Designated	Expiration
Davenport University	CAE-CDE 4Y	2014	2020
Eastern Michigan University	CAE-CDE 4Y	2016	2021
Ferris State University	CAE-CDE 4Y	2014	2020
University of Detroit Mercy	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2016	2021
Walsh College	CAE-CDE 4Y	2016	2021

Minnesota

Institution	Designation	Designated	Expiration
Capella University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
Metropolitan State University	CAE-CDE 4Y	2014	2020
Minneapolis Community and Technical College	CAE/IAE 2Y	2012	2017
St. Cloud State University	CAE-CDE 4Y	2014	2021
Walden University	CAE-CDE 4Y	2014	2019

Mississippi

Institution	Designation	Designated	Expiration
Mississippi State University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

Missouri

Institution	Designation	Designated	Expiration
Missouri University of Science and Technology	CAE/IAE 4Y	2012	2017
	CAE-R	2014	2019
University of Missouri-St. Louis	CAE-CDE 4Y	2016	2021

Montana

- No CAE schools

Nebraska

Institution	Designation	Designated	Expiration
Bellevue University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
University of Nebraska, Omaha	CAE-CDE 4Y	2014	2021

New Hampshire

Institution	Designation	Designated	Expiration
Dartmouth College	CAE-R	2014	2019

New Jersey

Institution	Designation	Designated	Expiration
Fairleigh Dickinson University	CAE-CDE 4Y	2014	2020
New Jersey City University	CAE-CDE 4Y	2014	2020
New Jersey Institute of Technology	CAE-CDE 4Y	2014	2020
Princeton University	CAE-R	2014	2019
Rutgers, The State University of New Jersey	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Stevens Institute of Technology	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

New Mexico

Institution	Designation	Designated	Expiration
Eastern New Mexico University - Ruidoso Branch Community College	CAE-CDE 2Y	2014	2019
New Mexico Tech	CAE-R	2014	2019
University of New Mexico	CAE/IAE 4Y	2012	2017
	CAE-IA-R	2012	2017

New York

Institution	Designation	Designated	Expiration
Excelsior College	CAE-CDE 4Y	2014	2019
Mercy College	CAE-CDE 4Y	2014	2020
Mohawk Valley Community College	CAE-CDE 2Y	2016	2021
New York Institute of Technology	CAE-CDE 4Y	2016	2021
New York University	CAE-R	2014	2021
Pace University	CAE/IAE 4Y	2012	2017
Rochester Institute of Technology	CAE-CDE 4Y	2014	2021
Syracuse University	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021

	CAE-R	2014	2021
University at Buffalo, the State University of New York	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
US Military Academy, West Point	CAE/IAE 4Y	2012	2017
Utica College	CAE-CDE 4Y	2014	2019

North Carolina

East Carolina University	CAE-CDE 4Y	2014	2021
Forsyth Technical Community College	CAE-CDE 2Y	2014	2019
North Carolina A&T State University	CAE-CDE 4Y	2014	2021
North Carolina State University	CAE-R	2014	2019
Rowan-Cabarrus Community College	CAE-CDE 2Y	2014	2019
University of North Carolina, Charlotte	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

North Dakota

- No CAE schools

Ohio

Institution	Designation	Designated	Expiration
Air Force Institute of Technology	CAE-R	2014	2019
Sinclair Community College	CAE/IAE 2Y	2012	2017
The Ohio State University	CAE-CDE 4Y	2014	2020
University of Cincinnati	CAE-CDE 4Y	2016	2021

Oklahoma

Institution	Designation	Designated	Expiration
Francis Tuttle Technology School	CAE/IAE 2Y	2012	2017
Oklahoma City Community College	CAE-CDE 2Y	2016	2021
Oklahoma Department of Career & Technology	CAE/IAE 2Y	2012	2017
Oklahoma State University	CAE-CDE 4Y	2014	2020
	CAE-R	2014	2020
Rose State College	CAE-CDE 2Y	2014	2020
University of Tulsa	CAE-CDE 4Y	2014	2020
	CAE-R	2014	2020

Oregon

Institution	Designation	Designated	Expiration
Mt. Hood Community College	CAE-CDE 2Y	2014	2019

University of Oregon	CAE-R	2014	2019

Pennsylvania

Institution	Designation	Designated	Expiration
Bloomsburg University of Pennsylvania	CAE-CDE 4Y	2016	2021
Carnegie Mellon University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Drexel University	CAE/IAE 4Y	2012	2017
East Stroudsburg University	CAE-CDE 4Y	2014	2020
Indiana University of Pennsylvania	CAE-CDE 4Y	2016	2021
Pennsylvania State University	CAE-CDE 4Y	2014	2021
University of Pittsburgh	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
West Chester University of Pennsylvania	CAE-CDE 4Y	2014	2020

Rhode Island

Institution	Designation	Designated	Expiration
University of Rhode Island	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

South Carolina

Institution	Designation	Designated	Expiration
The Citadel	CAE-CDE 4Y	2016	2021
University of South Carolina	CAE-CDE 4Y	2014	2020
	CAE-R	2014	2020

South Dakota

Institution	Designation	Designated	Expiration
Dakota State University	CAE/IAE 4Y	2012	2017
	CAE-IA-R	2012	2017

Tennessee

Institution	Designation	Designated	Expiration
Fountainhead College of Technology	CAE-CDE 4Y	2014	2020
Jackson State Community College	CAE/IAE 2Y	2012	2017
Tennessee Tech University	CAE-CDE 4Y	2016	2021
The University of Tennessee at Chattanooga	CAE-CDE 4Y	2014	2021

University of Memphis	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

Texas

Institution	Designation	Designated	Expiration
Our Lady of the Lake University	CAE/IAE 4Y	2012	2017
San Antonio College	CAE-CDE 2Y	2014	2020
Southern Methodist University	CAE-CDE 4Y	2014	2021
St. Philip's College	CAE-CDE 2Y	2014	2020
Texas A&M University	CAE-CDE 4Y	2016	2021
	CAE-R	2016	2021
Texas A&M University-Corpus Christi	CAE-CDE 4Y	2016	2021
Texas A&M University-San Antonio	CAE/IAE 4Y	2012	2017
The University of Texas at Austin	CAE-R	2014	2019
The University of Texas at San Antonio	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of Dallas	CAE-CDE 4Y	2014	2021
University of Houston	CAE-CDE 4Y	2014	2020
	CAE-R	2014	2020
University of North Texas	CAE/IAE 4Y	2012	2017
	CAE-IA-R	2012	2017
	CAE-R	2014	2019
University of Texas at Dallas	CAE/IAE 4Y	2012	2017
	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
University of Texas at El Paso	CAE-CDE 4Y	2014	2020

Utah

Institution	Designation	Designated	Expiration
Brigham Young University	CAE/IAE 4Y	2012	2017

Vermont

Institution	Designation	Designated	Expiration
Champlain College	CAE/IAE 4Y	2012	2017
Norwich University	CAE/IAE 4Y	2012	2017

Virginia

- Cyber Initiatives Included in the 2017-18 Budget Bill https://cyberva.virginia.gov/ and https://governor.virginia.gov/media/3330/eo-8-launching-cyber-virginia-and-the-virginia-cyber-security-commission.pdf
- Virginia Tech awarded $20 million grant for cyber workforce development from the National Science Foundation (NSF) to help increase cyber workforce development and encourage scientific partnerships to deliver innovation in the field.

Institution	Designation	Designated	Expiration
George Mason University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021
Hampton University	CAE-CDE 4Y	2016	2021
James Madison University	CAE-CDE 4Y	2014	2020
Lord Fairfax Community College	CAE-CDE 2Y	2016	2021
Marymount University	CAE-CDE 4Y	2014	2020
Norfolk State University	CAE-CDE 4Y	2014	2020
Northern Virginia Community College	CAE-CDE 2Y	2014	2020
Radford University	CAE-CDE 4Y	2016	2021
Tidewater Community College	CAE-CDE 2Y	2016	2021
Virginia Polytechnic Institute and State University	CAE-R	2014	2021

Washington

Institution	Designation	Designated	Expiration
City University of Seattle	CAE-CDE 4Y	2014	2019
Highline College	CAE-CDE 2Y	2014	2020
University of Washington	CAE/IAE 4Y	2012	2017
	CAE-R	2014	2019
Whatcom Community College	CAE-CDE 2Y	2014	2021

West Virginia

Institution	Designation	Designated	Expiration
Blue Ridge Community and Technical College	CAE-CDE 2Y	2016	2021
West Virginia University	CAE-CDE 4Y	2014	2021
	CAE-R	2014	2021

Wisconsin

- No CAE schools

Wyoming

- No CAE schools

How to Generate a 4,100% ROI Without Breaking a Sweat

Cutting the cost of recruiting and developing emerging Cybersecurity talent.

Investment and ROI
iQ4 and the Cybersecurity Workforce Alliance (CWA) is designed by industry members to better align education's supply to industry's need for entry level Cybersecurity talent. The CWA engagement model accelerates project based real-world scenario applied learning while students are in University; cutting the post hire training and development time and cost equal to 3-months in employment. The CWA process also helps ensure a hiring decision that is a "good fit". Note that a "bad fit" hire typically costs 6 times that of a good one. (Credit Suisse's William Wolfe stated, "Bad hires are costing $75-100 million a year"). Also, CWA member employers advise iQ4 that their first year attrition rate is 25-30% or more.

Global HR Executives Viewpoint on the Cybersecurity Workforce Alliance (CWA) value. Profile: 180,000+ employees, hiring 15,000+ plus graduates/apprentices a year. First year emerging talent attrition rate of 25-30% causing a retention and replacement cost/issue. ([1]Attribution to name and company withheld due to corp. policy)

"..So, as a HR Executive, why would I want to be a part of this program?

1) *A training program which is run in a way that is likely to be more successful than a regular classroom or online course. It is also a very extended interview. I get to see my candidates learn and develop. This gives me a great insight into who they are and how they are likely to perform in my company. It also gives me a great opportunity to build a relationship which will reduce the rejection rate.*
2) *I have access to talent which is more 'work ready'. If I do not have to do any more training when they join, I have shortened their onboarding time considerably and reduced the potential failure rate (the point about the cost of bad hires is very true).*
3) *I have a lot of information about my candidates as a living resume / skills database.*

The CWA is a global community on the iQ4 Workforce Optimization and Skills Development Platform, which is virtual and scalable. *The proven CWA operating model saves time and expense; accelerating new hire time to productivity and return $41 for every $1 dollar invested in the program.* Note: U.K. model yet to be developed.

		$Cost Savings – IQ4-CWA vs Traditional Methods					ROI
Hires	**Investment**	**A Recruiting**	**B Training**	**A+ B= Productivity**	**Retention/ Replacement**	**Total**	
1	5,000	-	75,000	75,000	40,658	115,658	22.1x
8	22,500	17,500	600,000	617,500	328,218	945,718	41.0x
100	282,500	217,500	7,500,000	7,171,500	4,102,508	11,820,008	40.8x
1,000	2,812,500	2,187,500	75,000,000	77,187,500	41,027,188	118,214,688	41.0x

- Class Cost - $2,500 per student per 10-12 week class (cost sources: School -$1,000; iQ4-CWA $1,500)
- Mentor Cost – $2,500/class, est. up to 2 hours/week for 12 weeks, est $200,000 salary with on-costs
- Post Hire Training – reduce training 25% (savings based on 3 months @ $25/mth= $75k total)
- Recruiting – reduced because the courses creates a prolonged interview where candidates are identified and cultivated to be more workforce ready minimizing traditional HR processing costs.
- Retention improved from assuring "good fit" hiring thus reducing Replacement cost.
- Retention improvement – from assuring "good fit" hiring and from employee engagement from training.

USA: Frank Cicio, CEO iQ4 and Founder of CWA + 1 212 914 4655 frank@iq4.com

International: Peter Meehan, SVP, International/CWA +44 (0) 7788 715517 peter@iQ4.com

. © iQ4 2010-Present All rights reserved

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

July 12, 2016

M-16-15

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director
Office of Management and Budget

Beth F. Cobert
Acting Director
Office of Personnel Management

Tony Scott
Federal Chief Information Officer
Office of Management and Budget

SUBJECT: Federal Cybersecurity Workforce Strategy

Executive Summary

Every day, Federal departments and agencies face increasingly sophisticated and persistent cyber threats that pose strategic, economic, and security challenges to our Nation. These cyber threats demonstrate the need for critical security tools, and equally as important, the need to employ the Federal civilian cybersecurity workforce with the necessary knowledge, skills, and abilities to use those tools to enhance the security of the Federal digital infrastructure and improve the ability to detect and respond to cyber incidents when they occur. Both Federal and private sector executives cite the lack of professionals with the requisite knowledge and skills as a significant impediment to improving their cybersecurity. However, there simply is not a sufficient supply of cybersecurity talent to meet the increasing demand of the Federal Government. Recent industry reports project this shortfall will expand rapidly over the coming years unless companies and the Federal Government act to expand the cybersecurity workforce to meet the increasing demand for talent.

To develop and strengthen the workforce of Federal cybersecurity professionals, the Government must demonstrate that it is the employer of choice for such professionals, as it offers rewarding,

unique, and dynamic careers that rival opportunities anywhere else in the world. In particular, the Federal cybersecurity workforce is entrusted with the mission of protecting government information technology (IT) systems, networks, and data from the most sophisticated adversaries; safeguarding sensitive data; supporting our Nation's financial systems; and securing our critical infrastructure, and intelligence systems. The Government is seeking college students and industry employees of all skill and experience levels to bring their skills into public service to take on these challenging missions and further expand the existing, highly capable Federal cybersecurity workforce. Moreover, the Government seeks to provide cybersecurity professionals the flexibility to join Federal service at different times in their careers to create new opportunities for career growth, development, and innovation for such professionals across private industry, academia, and Government.

This Federal Cybersecurity Workforce Strategy (the Strategy) details government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats. Most importantly, the Strategy presents new approaches to address persistent Federal workforce challenges. The Strategy anticipates that the Government will see the return on its investment through enhancements to Federal cybersecurity and the improved knowledge, skills, and abilities incoming cybersecurity talent bring to the Federal workforce.

Introduction

Addressing the Nation's growing challenges requires a capable Federal cybersecurity workforce that possesses the necessary cybersecurity knowledge, skills, and competencies to counter increasingly sophisticated and ever-changing threats. The Federal Government, however, faces a cybersecurity workforce shortage due to persistent recruitment, hiring, and retention challenges, and increasing competition with private sector companies for top talent.

The Federal Government must take immediate and broad-sweeping actions to address the growing workforce shortage and establish a pipeline of well-qualified cybersecurity talent. To this end, in June of 2015, the Office of Management and Budget (OMB) launched the Cybersecurity Sprint to rapidly improve cybersecurity across the Federal Government. The Cybersecurity Sprint included a review of Federal cybersecurity policies, plans, and procedures, which revealed two key observations about the Federal cybersecurity workforce:

1. The vast majority of Federal agencies cite a lack of cybersecurity and IT talent as a major resource constraint that impacts their ability to protect information and assets; and,
2. There are a number of existing Federal initiatives to address this challenge, but implementation and awareness of these programs are inconsistent.

Accordingly, OMB issued the *OMB Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government"* on October 30, 2015. The CSIP called for OMB and the Office of Personnel Management (OPM) to publish a Cybersecurity Human Resources (*i.e.*, Workforce) Strategy and identify possible actions within the following areas to help the Federal Government recruit, develop, and maintain a pipeline of cybersecurity talent:

1. **Identify Cybersecurity Workforce Needs**. Improving the government-wide understanding of the cybersecurity workforce by identifying key capability and capacity gaps in order to enhance workforce planning;
2. **Expand the Cybersecurity Workforce through Education and Training.** Working with educational institutions, professional organizations, training organizations, and other experts on cybersecurity program guidance from P-12 through university-level education to significantly expand the pipeline of skilled cybersecurity talent available for the Government and beyond;
3. **Recruit and Hire Highly Skilled Talent**. Engaging in government-wide and agency-specific efforts to expand the cybersecurity workforce through recruitment of highly-skilled talent, and streamlining the hiring and security clearance process while still meeting applicable law and standards; and,
4. **Retain and Develop Highly Skilled Talent**. Promoting an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce.

The Cybersecurity National Action Plan (CNAP), announced on February 9, 2016, builds on the CSIP activities while calling for innovation and investments in cybersecurity education and training to strengthen the talent pipeline. As part of the CNAP, the FY 2017 President's Budget proposes investing $62 million to expand the CyberCorps®: Scholarship for Service program, develop a cybersecurity core curriculum for academic institutions, and strengthen the National Centers for Academic Excellence in Cybersecurity Program to increase the number of participating academic institutions and expand cybersecurity education across the Nation. These initiatives will help the Federal Government recruit and retain cybersecurity talent with well-rounded skillsets comprised of the technical acumen, policy expertise, and leadership abilities necessary to secure Federal assets and networks well into the future.

To develop the Strategy, OPM led four teams of representatives from the Government, private sector, and academia to perform a comprehensive review of existing and forward-leaning strategies for recruiting, developing, and retaining cybersecurity professionals. The teams focused on identifying approaches that would help the Federal Government build the cybersecurity workforce and recruit, hire, develop, and retain top talent. OMB and OPM incorporated the findings of the review into the Strategy and considered the following principles

in developing the Strategy:

- Cybersecurity is a shared responsibility among agency leadership, employees, contractors, private industry, and the American people.
- The cybersecurity workforce includes employees who join Federal service at different times in their careers and have different levels of expertise.
- The cybersecurity workforce includes a mix of technical and non-technical professionals focused on all aspects of institutional mission.
- This is a government-wide human capital strategy requiring ownership and action from multiple agencies and entities.
- These initiatives focus primarily on the Federal workforce with the understanding that contractors also play vital roles in Federal cybersecurity.
- The initiatives will provide corresponding resources to non-cyber professionals, such as foundational cybersecurity training and development, and career mobility opportunities.
- While every agency is responsible for managing cybersecurity risks and will have staff that serves part of the cybersecurity workforce, the majority of the civilian cybersecurity workforce will serve in positions at agencies with cybersecurity missions.

I. Identify Cybersecurity Workforce Needs

The Federal Government must adjust its approach for conducting cybersecurity workforce planning. In particular, the Government and Federal agencies should move away from using the term "cyber professionals" as a catchall for the workforce, as the term encompasses over 30 discrete job functions with varying levels of skill and complexity. The National Initiative for Cybersecurity Education (NICE) partner agencies[1] are actively working to address this issue by revising the National Cybersecurity Workforce Framework (Workforce Framework). The Workforce Framework, started in 2011, provides a blueprint for organizing the way we think and talk about cybersecurity work, understanding workforce requirements, and establishing training and development opportunities for employees.

Federal agencies used the Workforce Framework to identify the number of cybersecurity positions and workforce gaps as part of the CSIP review process. Although the CSIP process served as a meaningful first step toward identifying cybersecurity needs, it did not provide a method for agencies to prioritize which position gaps to close. Accordingly, the revised version of the Workforce Framework will enable agencies to examine specific IT, cybersecurity, and cyber-related work roles, and identify personnel skills gaps, rather than merely examining the number of vacancies by job series. Additionally, OPM, the NICE partner agencies, and other Federal agencies are taking the following actions to improve cybersecurity workforce planning:[2]

a. Educate Federal agency Human Resources (HR) and Chief Information Officer (CIO) staff about the Workforce Framework, the tools associated with the Workforce Framework, and the benefits of aligning to the Workforce Framework.
b. Expand cybersecurity position coding to capture work roles outlined in the Workforce Framework, and align those roles with cybersecurity vacancies.
c. Conduct Strategic Workforce Planning, and work with the private sector to explore trends and anticipate future workforce needs.

[1] The NICE partner agencies include the National Institute of Standards and Technology (NIST), DHS, DOD, OPM, Office of the Director of National Intelligence, Department of Commerce, the Department of Education, the National Science Foundation (NSF), the National Security Agency (NSA), Department of Energy, Federal Communications Commission, the Department of Labor, and the Executive Office of the President. For more information, see https://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education.
[2] See Appendix A, Goal 1.

II. Expand the Cybersecurity Workforce through Education and Training

There is a critical shortage of cybersecurity talent across the Nation, as the demand for personnel with cyber expertise in both the public and private sectors far exceeds the supply. Within the Federal Government, recruitment and retention challenges and competition from the private sector exacerbate this staff shortage. This results in an increasing demand for cybersecurity professionals who can implement mechanisms for defending systems, networks, and data, and address complex and emerging cyber threats.

The CNAP identified several actions to address workforce challenges and expand the talent pipeline. In particular, the CNAP recognized that long-term investments in nationwide cybersecurity education are crucial to establishing a sustainable cybersecurity workforce. Expanding cybersecurity education will require the Government to stimulate interest in the cyber-related fields through initiatives such as Computer Science for All, which aims to provide all P-12 students access to a rigorous computer science education. The Government must also foster students' academic growth through the development of a flexible cybersecurity core curriculum at institutions of higher education and provide employment opportunities that further develop and apply those skills once students graduate.

In addition to expanding these programs, the Federal Government must take additional steps to expand the pipeline of cybersecurity talent that is available to enter into Federal service. These steps include:

- Collaborating with academic institutions to address skill gaps by identifying or promoting existing foundational curriculum that institutions can consult and adopt; and
- Providing resources to academic institutions to accelerate and expand cybersecurity education across the Nation.

Collaborating with Academic Institutions to Address Skills Gaps through Curriculum

Cybersecurity is a burgeoning academic discipline that encompasses technical and non-technical areas of study with a wide range of complexity. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated nearly 200 academic institutions as National Centers of Academic Excellence in Cyber (CAE) based on specified criteria for certain cybersecurity focus areas across the academic disciplines. Each institution in the program develops cybersecurity curricula that align with the specified criteria. While these institutions graduate a broad range of talented students, these students do not always possess a common knowledge base when they enter into Federal service. As a result, agencies are often times spending their limited training funds to close skills gaps and familiarize incoming employees with foundational knowledge, skills, and abilities that universities, colleges, and graduate schools could otherwise teach.

OMB, NSA, and DHS, in coordination with the other NICE partner agencies will collaborate with academic institutions to take the following actions and identify, compile, and disseminate foundational cybersecurity guidelines for academic institutions across the nation to consult and voluntarily adopt:[3]

a. Survey the current state of cybersecurity curriculum with academic partners and other leading institutions to determine common learning outcomes that align cybersecurity education with specific work roles and career paths.
b. Develop cybersecurity curriculum guidelines, knowledge units[4] that provide minimum learning requirements in specific areas, and learning outcomes in partnership with academic organizations.
c. Work with colleges and universities, including minority-serving institutions, to increase recruitment efforts and increase the number of students studying cybersecurity as a profession.

Funding Cybersecurity Higher Education across the Nation

The Government will collaborate with academic institutions to expand cyber education across the Nation through the CAE program. The purpose of the CAE program is to promote higher education in cyber defense and to educate and develop professionals that can address cybersecurity challenges. NSA, in coordination with DHS and the NICE partner agencies, will undertake the following actions to increase the capacity of CAEs, students studying at CAEs, and faculty serving at CAEs:

a. Work with educational organizations to establish financial and professional incentives for cybersecurity experts to serve as faculty at a CAE.[5]
b. Measure the success of supported educational programs such that agencies can document a student's proficiency in the competencies, and knowledge, skills, and abilities associated with each category and Specialty Area in the Workforce Framework.
c. Provide grants to current and prospective CAEs to incentivize academic institutions to enhance the quality of their cybersecurity education programs and expand their programs by increasing capacity to enroll and graduate additional students, teach additional courses, and hire additional faculty.

[3] See Appendix A, Goal 2.
[4] Information on knowledge units is available at https://www.iad.gov/NIETP/documents/Requirements/CAE_IA-CD_KU.pdf.
[5] The CyberCorps® SFS Capacity Track provides funding to increase the number of cybersecurity teachers; curriculum resources; cyber laboratories, test beds and ranges; and professional development.

III. Recruit and Hire Highly-Skilled Cybersecurity Talent

The Government must expand its recruitment campaigns in order to raise awareness of employment opportunities and compete for top cybersecurity talent. Federal agencies can offer prospective cybersecurity employees an opportunity to serve their country in a dynamic work environment that is unlike anywhere else in the public or private sectors. However, the Federal Government struggles to attract and retain cybersecurity talent from both colleges and universities, including the CAEs, and industry.

To overcome these challenges, Federal agencies must engage in strategic recruitment and awareness campaigns, and pursue individuals with cyber talent who, historically, may not have sought out Government careers. Agencies should enhance outreach efforts to reach all segments of society and highlight the ways in which their organizations value diversity and inclusion. Recruiting activities should include outreach to women, who OPM estimates compromise less than 25% of the current cyber workforce. Agencies should sustain their efforts to attract minority students to this work, as OPM estimates that minorities comprise 32% of the cyber workforce compared to 35% of the overall civilian labor force. Additionally, enhancing recruitment efforts will require the Government to dedicate human capital personnel to finding ways to streamline hiring and security clearance processes for cybersecurity personnel consistent with governing law and applicable standards. This effort also includes exploring available authorities or pursuing new authorities to offer prospective employees more competitive compensation and providing meaningful work as part of a clear career path through thoughtful consideration to position descriptions and how grade progressions function.

In an effort to reshape cybersecurity recruitment, the CSIP tasked OPM to provide agencies with information on a number of hiring, pay, and leave flexibilities[6] to help recruit and retain individuals in cybersecurity positions. In addition, OPM issued a memorandum that provided *Guidance on Recruitment, Relocation and Retention Incentives*, which allowed agencies to approve exceptions for certain employees to a calendar year 2010 spending limit on incentives. OPM also held numerous forums and summits with agency CIOs, Chief Human Capital Officers, human capital management professionals, managers with hiring or HR responsibilities, and executives who have responsibility for recruiting and hiring a cybersecurity workforce. These activities helped familiarize agency staff with existing hiring authorities, including direct hire authorities for information security professionals,[7] which will help increase recruitment and hiring efforts across the Government in the near term.

---

[6] Information on hiring, pay, and leave flexibilities is available at: https://www.chcoc.gov/content/Cybersecurity-hiring-pay-and-leave-flexibilities.

[7] Information on direct hire authorities is available at: https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority.

OMB, OPM, DHS, and other Federal agencies will take the following actions to enhance outreach, recruitment, hiring, and retention of cybersecurity talent into the Federal Government:[8]

a. In accordance with the CNAP, establish the DHS Cybersecurity Surge Corps, which would dispatch teams of cybersecurity experts to assist agencies with incident response, systems engineering, and enterprise security and policy projects, using a consultant multi-project, multi-skill, multi-disciplinary approach.
b. Develop a Federal Cybersecurity Career Awareness Campaign and Communications Strategy for applicants and agency HR and hiring managers.
c. Establish a cybersecurity HR Cadre, an expert group of HR professionals from across the Government, who will execute a model cybersecurity end-to-end hiring process at agencies that is tailored, timely, and a high quality experience for both applicants and hiring managers.
d. Promote the use of the PushButtonPD™ that managers, supervisors, and HR Specialists can use to rapidly draft a Federal employee Position Description (PD) leveraging accumulated knowledge in order to streamline position classification.
e. Implement a government-wide recruitment strategy aimed at recruiting diverse talent from among veterans, existing civil service employees, CyberCorps®: Scholarships for Service students, apprenticeship program graduates, and traditional sources. Where possible under existing law, the strategy should also provide opportunities for private sector employees to participate in rotational assignments at Federal agencies, enabling professionals who may be reluctant to commit to a career in Federal service for short periods of time to share their skills with Federal employees while gaining Federal service experience.
f. Examine opportunities to expand mechanisms to bring onboard cybersecurity talent including a cybersecurity track in the Presidential Management Fellows program, exploring direct hire for additional occupations related to cybersecurity, and developing legislation on industry exchange programs and expert and consultants.
g. Establish programs to assist Federal agencies in their use of existing flexibilities for compensation and explore opportunities for new or revised pay programs for cybersecurity positions consistent with other special Federal pay programs (e.g., special salary rates and/or market sensitive pay structures).[9]

[8] See Appendix A, Goal 3.
[9] Information on special salary rates is available at: https://apps.opm.gov/SpecialRates/Index.aspx.

IV. Retain and Develop Highly-Skilled Cybersecurity Talent

In order to retain cybersecurity talent, agencies must foster an environment that provides rewarding and hands-on training experiences; supplies useful and appropriate technology; empowers employees; creates a positive and supportive workplace culture; and acknowledges that some of the cybersecurity employees the Federal Government hopes to attract may only wish to stay for a short period of service. This is a different way of thinking about the Federal workforce and requires new programs, initiatives, and ways of approaching recruitment and retention efforts. Such non-traditional opportunities for training and skills refreshment must be considered in order to retain cybersecurity talent.

Whether employees are entry-level, mid-career, or seasoned executives, developmental and training opportunities are critical to retaining employees. Entry-level staff tend to focus on honing their technical skill sets, gaining access to innovative technology, establishing support and mentoring networks, and gaining meaningful hands-on experience. Mid-career professionals often focus on shaping their career path and advancing their skill sets through job rotations, obtaining certifications, and project management and supervisory experience. Seasoned or executive-level professionals may prioritize making contributions to their domains of expertise within the cybersecurity field, leadership development opportunities, and mentoring the next generation.[10]

An OPM-led team of representatives from the Government, the private sector, and academia performed a comprehensive review of the existing education and talent development opportunities for cybersecurity professionals in the Federal Government, focusing on approaches that will help the Government retain top talent. The team found that while a myriad of talent development opportunities exist, cybersecurity professionals may not be aware of or may not have adequate access to the opportunities. Based on this gap analysis, the team developed a series of findings and recommendations to close these gaps.

Establish an Enterprise-wide Approach to Cybersecurity Employee Retention and Development

An OPM-led team recommended that NIST, the Department of Defense (DOD), and DHS convene to determine what actions are required for each work role with a specific interest on major talent gaps for both Federal employees and contractor employees, in order to fully utilize the existing retention and talent development opportunities. Enterprise-wide workforce planning includes efforts to incorporate certifications and training opportunities so that cybersecurity professionals remain knowledgeable about emerging trends in their area(s) of responsibility, with these and other professional development opportunities serving as retention strategies. In

[10] https://niccs.us-cert.gov/sites/default/files/documents/files/Cybersecurity%20Workforce%20Development%20Toolkit_1.pdf

addition, to strengthen enterprise-wide retention and development efforts, DHS will develop a security-training program for non-cybersecurity employees in occupations and work roles that support the core cybersecurity community. There will also be expanded anti-phishing and other behavior-based training, enabling all Federal employees to possess the requisite knowledge to protect themselves from cyber threats on a daily basis.

OMB, OPM, DHS, and other Federal agencies will take the following actions to promote the most effective cybersecurity talent development and management across the Federal cybersecurity workforce:[11]

a. Increase the focus on retention for top performers by helping agencies develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility.
b. Develop a government-wide cybersecurity orientation program for new cybersecurity professionals.
c. Develop and promote cybersecurity career paths, rotational assignments, and mentoring and coaching programs, to provide employees with opportunities to become subject matter experts in their field or move into managerial roles and take on increased responsibilities.
d. Develop and leverage existing tailored cybersecurity training (e.g., FedVTE) for employees, senior managers, and executives who work in related career fields outside of cybersecurity, including finance and acquisitions, so that budget planning, financial management, and contracting help improve agencies' cybersecurity posture.
e. Develop and leverage existing competitions, certifications, and credentialing to improve the skills of existing employees that may qualify them for potential pay increases or promotions based on demonstrated improvements in technical abilities. Explore a legislative proposal for a cybersecurity skills and education incentive, where employees receive additional compensation based on their demonstrated skills and education.
f. Develop a common training program for specific categories of cybersecurity professionals, including but not limited to those personnel engaged in incident response and penetration testing activities.

[11] See Appendix A, Goal 4.

Conclusion

The Strategy details numerous initiatives that will help strengthen the Federal cybersecurity workforce. We must recognize, however, that these changes will take time to implement. To address cybersecurity challenges in the immediate future, the Administration will invest in the existing Federal workforce through initiatives focused on training and retaining existing talent. At the same time, the Government will adjust the way it recruits talented students and potential employees in the cybersecurity workforce outside Federal service. The long-term success of this Strategy requires concerted attention, innovation, and resources. The initiatives discussed in this Strategy represent a meaningful first step toward engaging Federal and non-Federal stakeholders, and the first step toward providing the resources necessary to establish, strengthen, and grow a pipeline of cybersecurity talent well into the future.

###

APPENDIX A

CYBERSECURITY HUMAN CAPITAL STRATEGY GOAL AND ACTION TRACKER

Goal 1: Identify Cybersecurity Workforce Needs

Purpose Improving the government-wide understanding of the cybersecurity workforce while identifying key capability and capacity gaps in order to enhance workforce planning.

Outcome Improve agencies' understanding of their current cybersecurity workforce to better identify current resource and skill gaps, and improve long-term cybersecurity workforce planning and talent development.

Action	Deadline	Lead Agency/Agencies
Educate Federal agency Human Resources (HR) and Chief Information Officer (CIO) staff about the Workforce Framework, the tools associated with the Workforce Framework, and the benefits of aligning to the Workforce Framework.	3 Months	OPM, NIST, DOD
Expand cybersecurity position coding to capture work roles outlined in the Workforce Framework and aligning those roles with cybersecurity vacancies.	9 Months	OPM, NIST
Conduct Strategic Workforce Planning and work with the private sector to explore trends and anticipate future workforce needs.	12+ Months	All Federal Agencies

Goal 2: Expand the Cybersecurity Workforce through Education and Training

Purpose Collaborate with educational and training organizations to provide guidance on cybersecurity program development.

Outcome Increase awareness of Federal cybersecurity career paths for potential applicants for current vacancies, and develop a pipeline of talent to fill long-term gaps in the cybersecurity workforce.

Action	Deadline	Lead Agency/Agencies
Survey the current state of cybersecurity curriculum with academic partners and other leading institutions to determine common learning	9 Months	NSA, DHS, NIST

outcomes that align cybersecurity education with specific work roles and career paths.		
Work with colleges and universities, including minority-serving institutions, to increase recruitment efforts and increase the number of students studying cybersecurity as a profession.	9 Months	NSA, DHS
Provide grants to current and prospective CAEs to incentivize academic institutions to enhance the quality of their cybersecurity education programs and expand their programs by increasing capacity to enroll and graduate additional students, teach additional courses, and hire additional faculty.	9 Months	NSA
Work with educational organizations to establish financial and professional incentives for cybersecurity experts to serve as faculty at a CAE.	12+ Months	NSA, NICE Partner Agencies
Develop cybersecurity curriculum guidelines, knowledge units that provide minimum learning requirements in specific areas, and learning outcomes in partnership with academic organizations.	12+ Months	NSA, NICE Partner Agencies
Measure the success of supported educational programs such that agencies can document a student's proficiency in the competencies and knowledge, skills, and abilities associated with each category and Specialty Area in the Workforce Framework.	12+ Months	NSA, NICE Partner Agencies

Goal 3: Recruit and Hire Highly Skilled Talent

Purpose Engage in government-wide and agency-specific efforts to conduct outreach and recruitment for cybersecurity talent and improve and expand on existing hiring and retention efforts

Outcome Increase the pipeline of cyber talent entering the Federal workforce, including candidates who have not traditionally considered Federal employment, and provide reliable and effective HR services that enable agencies to immediately fill vacancies.

Action	Deadline	Lead Agency/ Agencies
Promote the use of the PushButtonPD™ that managers, supervisors, and HR Specialists can use to rapidly draft a Federal employee Position Description (PD) leveraging accumulated knowledge in order to streamline position classification.	3 Months	DHS, OPM

Establish the DHS Cybersecurity Surge Corps, which would dispatch teams of cybersecurity experts to assist agencies with incident response, systems engineering and enterprise security, and policy projects, using a consultant multi-project, multi-skill, multi-disciplinary approach.	6 Months	DHS, OPM, OMB, NSF
Establish a cybersecurity HR Cadre, an expert group of HR professionals from across the Government, who will execute a model cybersecurity end-to-end hiring process at agencies that is tailored, timely, and a high quality experience for both applicants and hiring managers.	6 Months	OPM, DHS
Establish programs to assist Federal agencies in their use of existing flexibilities for compensation and explore opportunities for new or revised pay programs for cybersecurity positions consistent with other special Federal pay programs (e.g., special salary rates and/or market sensitive pay structures.	6 Months	OPM
Implement a government-wide recruitment strategy aimed at recruiting diverse talent from among veterans, existing civil service employees, CyberCorps®: Scholarships for Service students, apprenticeship program graduates, and traditional sources. Where possible under existing law, the strategy should also provide opportunities for private sector employees to participate in rotational assignments at Federal agencies, enabling professionals who may be reluctant to commit to a career in Federal service for short periods of time to share their skills with Federal employees while gaining Federal service experience.	6 Months	OPM
Develop a Federal Cybersecurity Career Awareness Campaign and Communications Strategy for applicants and agency HR and hiring managers.	9 Months	OPM, DHS
Examine opportunities to expand mechanisms to bring onboard cybersecurity talent including a cybersecurity track in the Presidential Management Fellows program, exploring direct hire for additional occupations related to cybersecurity, and developing legislation on industry exchange programs and expert and consultants.	12 Months	OPM

Goal 4: Retain and Develop Highly Skilled Talent

Purpose Establish an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce and its infrastructure.

Outcome Create a network of cybersecurity professionals to facilitate knowledge sharing, identify potential cybersecurity professionals inside the Federal workforce, and promote long-term professional development through informal and formal channels to improve retention efforts and incentivize greater workforce capabilities.

Action	Deadline	Lead Agency
Increase the focus on retention for top performers by helping agencies develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility.	6 Months and Ongoing	OPM
Develop and leverage existing tailored cybersecurity training (e.g. FedVTE) for employees, senior managers, and executives who work in related career fields outside of cybersecurity, including finance and acquisitions so that budget planning, financial management, and contracting help improve agencies' cybersecurity posture.	6 Months	DHS, NIST, DOD
Develop a common training program for specific categories of cybersecurity professionals, including but not limited to those personnel engaged in incident response and penetration testing activities.	6 Months	DHS, OPM
Develop a government-wide cybersecurity orientation program for new cybersecurity professionals.	9 Months	OPM, NIST, DOD, OMB DHS
Develop and leverage existing competitions, certifications, and credentialing to improve the skills of existing employees that may qualify them for potential pay increases or promotions based on demonstrated improvements in technical abilities. Explore a legislative proposal for a cybersecurity skills and education incentive, where employees receive additional compensation based on their demonstrated skills and education.	9 Months	OPM, DOD

Develop and promote cybersecurity career paths, rotational assignments, and mentoring and coaching programs, to provide employees with opportunities to become subject matter experts in their field or move into managerial roles and take on increased responsibilities.	9 Months and Ongoing	OPM, NIST

APPENDIX B

ACRONYMS

Acronym	Definition
CAE	National Centers of Academic Excellence
CIO	Chief Information Officer
CNAP	Cybersecurity National Action Plan
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	Department of Homeland Security
DOD	Department of Defense
HR	Human Resources
IT	Information Technology
NIST	National Institute of Standards of Technology
NSA	National Security Agency
NSF	National Science Foundation
NICE	National Initiative for Cybersecurity Education
OMB	Office of Management and Budget
OPM	Office of Personnel Management
The Strategy	Federal Cybersecurity Workforce Strategy
Workforce Framework	National Cybersecurity Workforce Framework

ACM Joint Task Force to Develop Global Cybersecurity Curricular Guidelines
Survey Report – October 2016

INTRODUCTION

The ACM Joint Task Force on Cybersecurity Education (JTF) launched in September 2015 to develop the first set of global curricular guidelines in cybersecurity education. Cybersecurity is defined here as:

> *"A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."*

The JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP).

After a year of community engagement and developmental work, the JTF launched a survey in September 2016 to solicit broad input on the proposed curricular thought model. Stakeholders were invited to participate in the survey through direct invitations, announcements in public educational and scientific forums, social media outreach via the JTF website and LinkedIn, and invitations sent through the distribution lists of participating professional associations. This report summarizes the 229 completed survey responses received during the survey period of September 16 – October 3, 2016.

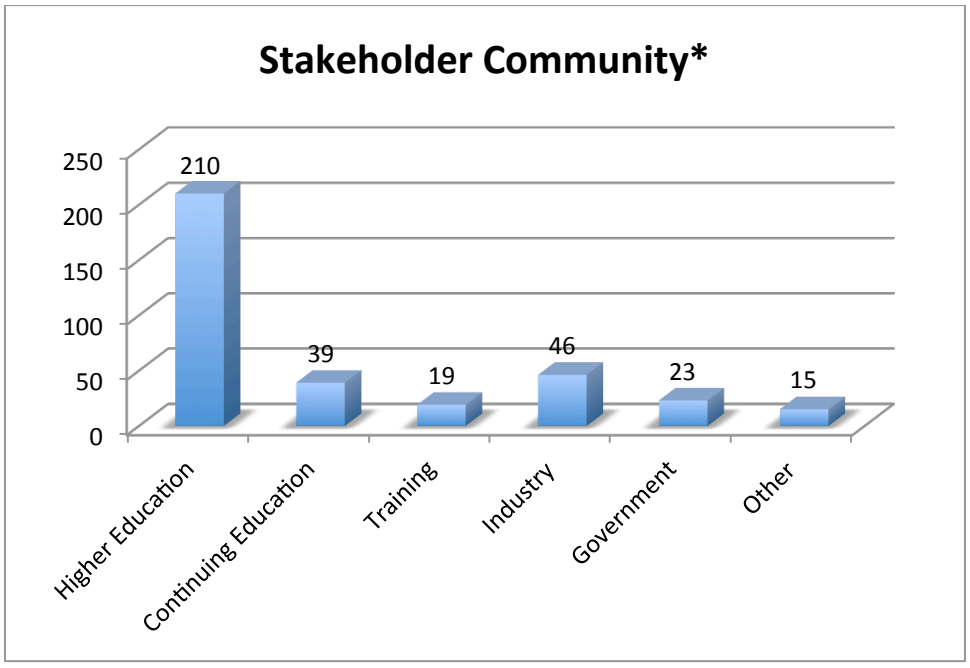
RESPONDENT DEMOGRAPHICS

Gender: Approximately 71% (162) of respondents were male, 26% (60) were female, and six respondents did not indicate gender.

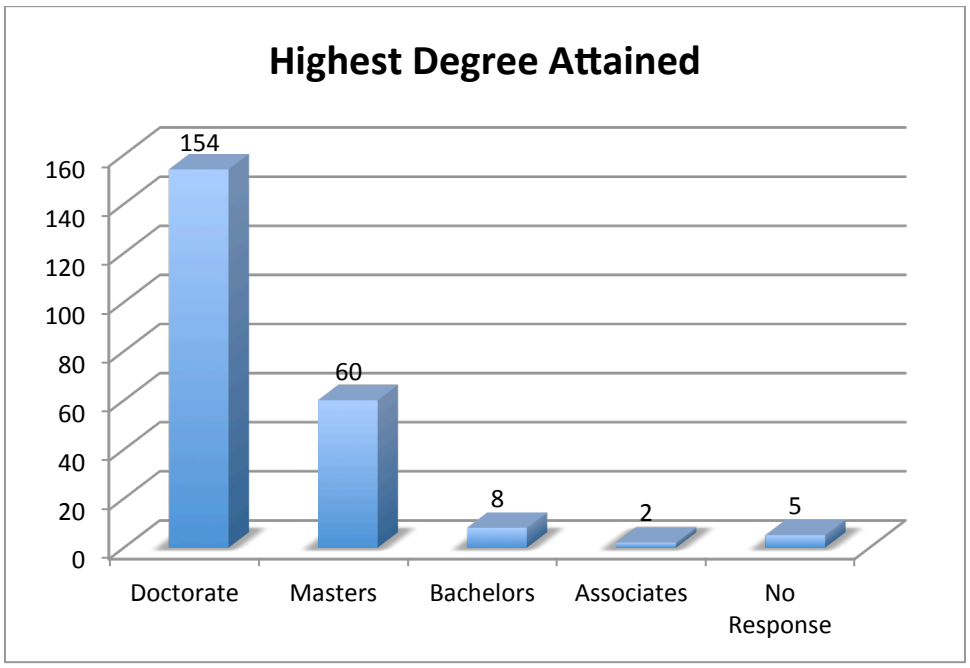
Geographic distribution: Nearly 88% (201) of survey respondents reported the United States as their primary work location. The remaining 22% of survey respondents were distributed as follows[1]: Australia (6), Norway (3), Italy (2), South Africa (2), and Sweden (2); with one completed survey from each of the following countries: Bulgaria, Canada, China, Hong Kong, India, Netherlands, New Zealand, Portugal, Qatar, Singapore, Slovenia, Spain, and Thailand.

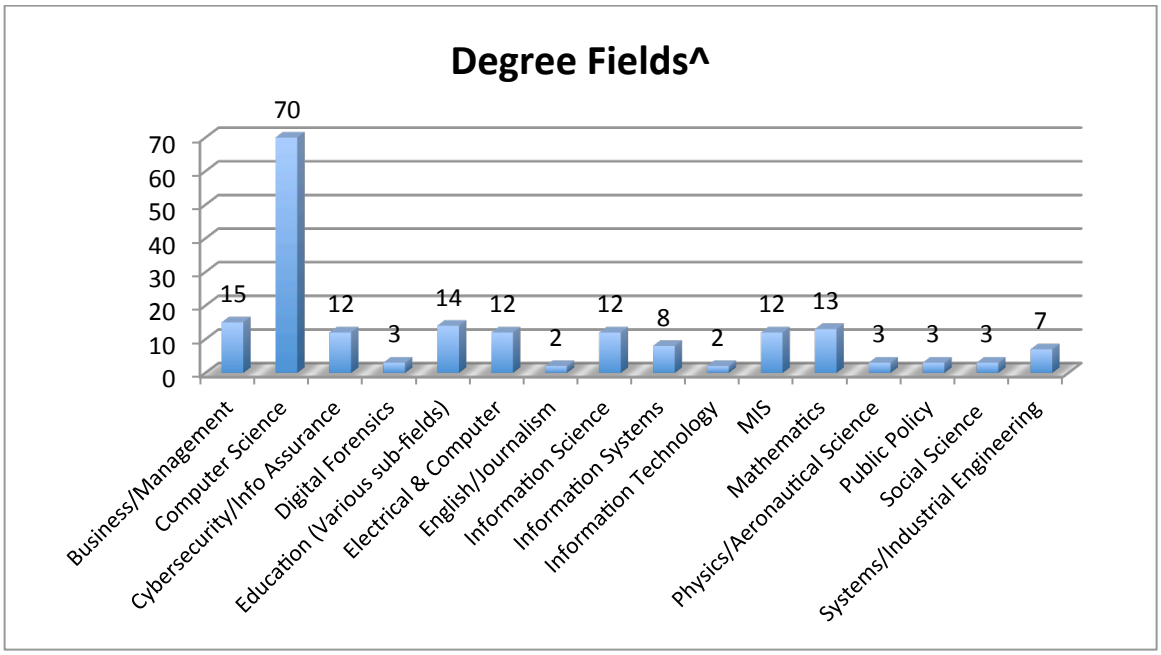
[1] The number of respondents per country is shown in the parentheses.

The charts below provide additional information on the background of survey respondents.

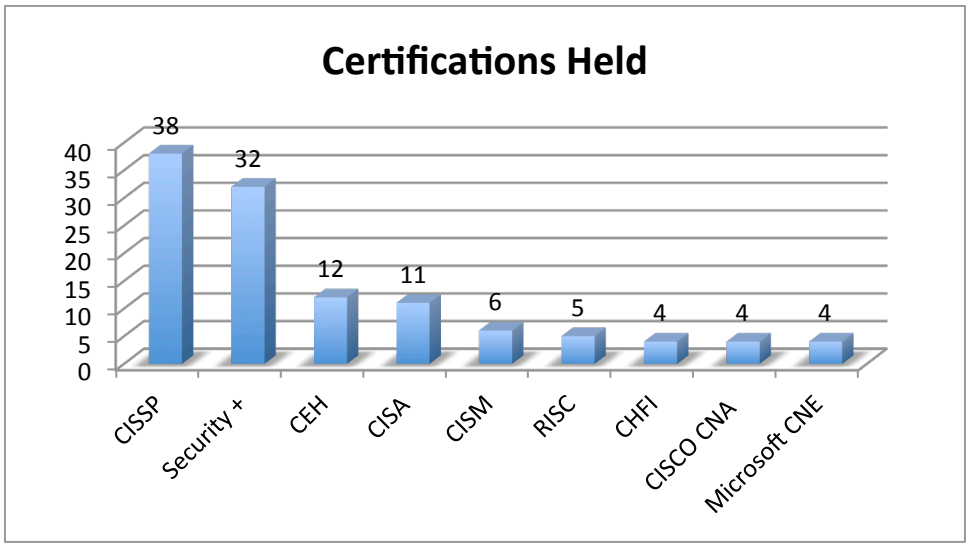


*Respondents were permitted to select all applicable stakeholder groups.





^Degree fields represent all degree levels (doctorate, masters, bachelors, and associates).



Many respondents reported holding multiple certifications. The most frequently held certifications included: the Certified Information Systems Security Professional (CISSP), Security +, Certified Ethical Hacker (CEH), Certified Information Auditor (CISA), Certified Information Security Manager (CISM), Risk and Information System Control (RISC), Computer Hacking Forensic Investigator, Cisco Certified Network Associate, and Microsoft Certified Systems Engineer. Certifications held by three or fewer respondents

included Certified Cyber Forensics Professional, Project Management Professional, Cisco Certified Network Associate (Security), or Certified Could Security Professional. Of the 229 respondents, 31 reported that they did not hold a security-related certification.

FEEDBACK ON THE PROPOSED THOUGHT MODEL

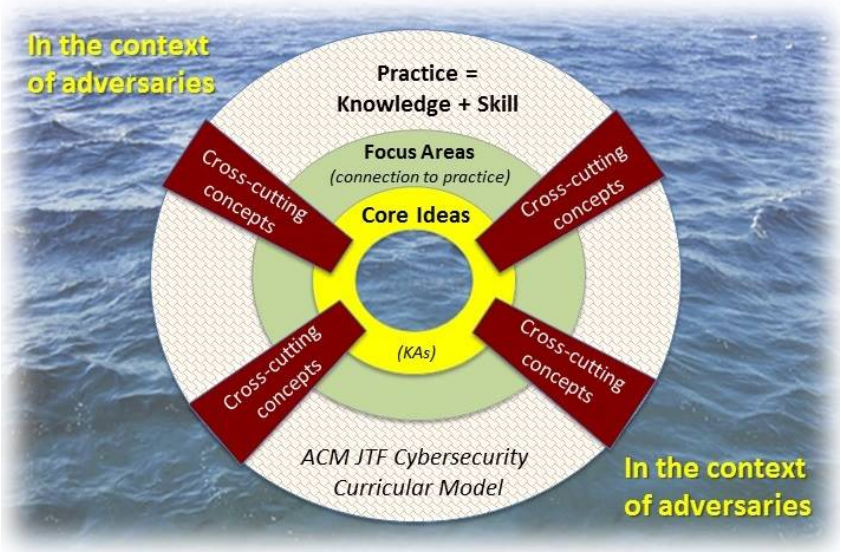
Survey participants were asked to provide feedback on the JTF curricular thought model. The curricular thought model was presented as a modification of U.S. National Research Council Next Generation Science Standards (nextgenscience.org). Survey respondents were asked to comment specifically on (1) the graphical representation and (2) the four structural elements of the thought model: Core Ideas, Focus Areas, Practices, and Cross-Cutting Concepts for cybersecurity education.

- **Core Ideas** are knowledge areas or domains;
- **Focus Areas** are different professional practice contexts;
- **Practices** are the combination of knowledge and skills that culminate into competency when connected with a particular focus area; and
- **Cross-Cutting Concepts** bridge core ideas practice and focus areas.

Feedback on each component is provided below.

(1) Graphical Representation

Survey respondents were asked to consider the proposed graphic and respond to the 3 questions listed in the table below.



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1 - The above graphic clearly communicates that engaging in cybersecurity investigation requires not only skill but also knowledge that is specific to each Practice	**47** (20.5%)	**81** (35.4%)	**31** (13.5%)	**53** (23.1%)	**17** (7.4%)
Q2--The above graphic clearly communicates that Cross-Cutting Concepts bridge Core Ideas, Practices, and Focus Areas.	**72** (31.4%)	**91** (39.7%)	**23** (10%)	**33** (14.4%)	**10** (4.4%)
Q3 --The above graphic clearly communicates that Core Ideas have the power to focus cybersecurity curriculum, instruction and assessments.	**31** (13.5%)	**67** (29.3%)	**53** (23.1%)	**55** (24%)	**23** (10%)

As indicated by the responses to each question, survey respondents were generally favorable about the graphic. However, a summary of the 73 comments offered as respondent narratives, suggest several areas for improvement:

- Include specific Practice Areas and revise the graphic to show that multiple practice areas exist.
- Expand the definition of each of the model elements and clarify the distinction between them.
- Align the graphical representation and the model more tightly. The current representation is not intuitive or easily understood without the model.
- Simplify the diagram.

(2) Structural Elements of the Thought Model

Summary feedback on each the four structural elements of the thought model: Core Ideas, Focus Areas, Practices, and Cross-Cutting Concepts for cybersecurity education; is provided below.

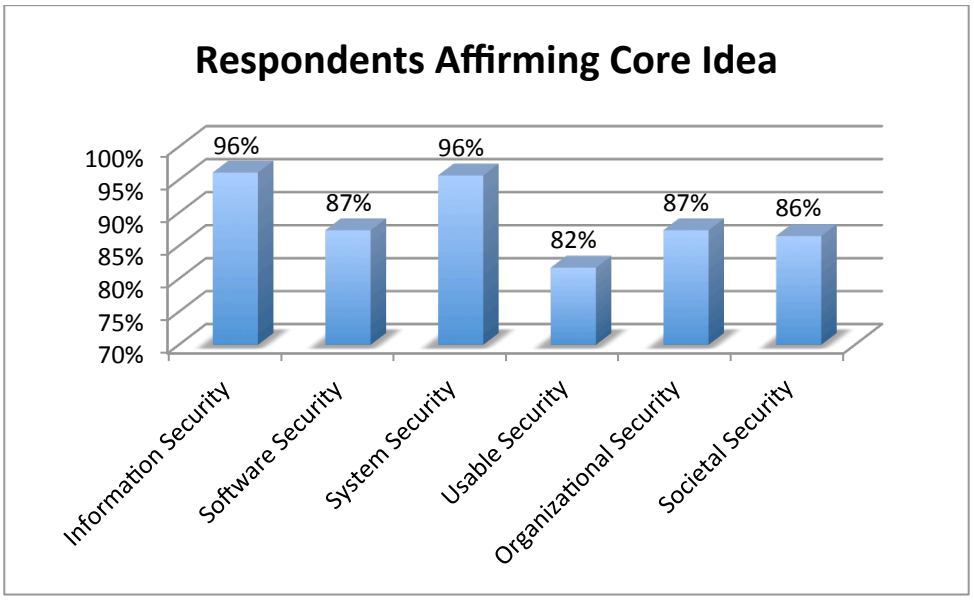
Core Ideas

Core Ideas are defined as knowledge areas or domains. Survey respondents were asked to review the Core Ideas listed below and (A) indicate if each listed Core Idea should be included in the curricular volume; (B) suggest any changes to the definition of the Core Idea and recommend the addition of Core Ideas not currently included.

Core Ideas:

1. Information Security [Includes: information confidentiality, data integrity, availability, cryptography and cryptanalysis]
2. Software Security [Includes: secure software engineering, software reverse engineering, malware analysis]
3. System Security [Includes: availability, authentication, access controls, secure systems design, computer network defense and CNA/penetration testing, reverse engineering (hardware), cyber physical systems, digital forensics, supply chain mtg]
4. Usable Security [Includes: identity management, social engineering, social networks, human-computer interaction]
5. Organizational Security [Includes: risk management, mission assurance, disaster recovery, business continuity, security evaluations/compliance, organizational behavior, intelligence, economics]
6. Societal Security [Includes: cyber crime, cyber law, ethics, policy, privacy, intellectual property, professional responsibility, global societal impacts]

A. Percentage of respondents affirming Core Idea



(B) Summary Comments on the Core Ideas

Survey respondents made several recommendations regarding the list of Core Ideas. The recommendations summarized below reflect the themes for each Core Idea.

Information Security

- Reconsider the inclusion of cryptography and cryptanalysis. These topics should be removed as Core Ideas and instead included as topics for specific groups.
- Provide a more thorough rationale for the set of Core Ideas included in the model. As they are presented, the breadth of topics does not provide sufficient curricular focus.
- Include topics of privacy authentication and non-repudiation. If these topics are addressed in the existing categories, clarify their placement.

Software Security

- Many of the topics included in the category are specialized and might not be relevant for the all portions of the broad audience to be served by this document. Given this, should the topics here be re-classified.
- Reconsider the inclusion of topics that seem more related to practice. For example, malware analysis and reverse engineering might be more appropriately classified as a practice rather than a core idea.
- Provide a stronger reference to, and consider relabeling this category as, the security software development lifecycle.

System Security

- Several topics, while important for some specialized areas, are not relevant for the broad audience to be served by this document. For instance, CNA, digital forensics, and supply chain management should not be listed as Core Ideas.
- Reconsider the inclusion of topics that seem more related to practice. For example, hardware reverse engineering should be removed.

Usable Security

- Identity management is a critical topic related to access control but is misplaced in this category. Move it to Organizational Security.
- Consider relabeling this category. Is the theme here 'user' or 'human factors' security? If so, consider using one of these labels to clarify the meaning of 'usable' security.
- Many of the ideas included in this category are tightly coupled with practice. This content may be misclassified as a Core Idea.

Organizational Security

- The topics included in this category are important but reconsider whether or not they have the same level of importance as the other categories.
- Risk management is a critical topic but the other content included in this category may not be as important. For example, is economics important to include here.
- Critical, but missing, topics include resilience and physical security. These topics should be added.

Societal Security

- The topics included in this category are important but reconsider whether or not they have the same level of importance as the other categories. Privacy is the only exception to this comment.
- The category is extremely broad. Identify the specific topics to be included here.

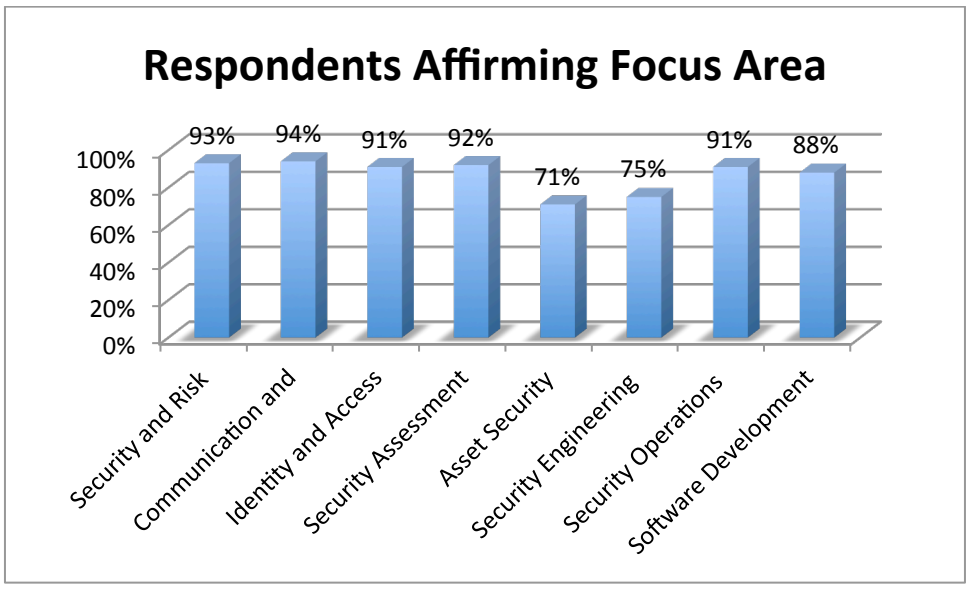
Focus Areas

Focus Areas are defined as different professional practice contexts. Survey respondents were asked to review the Focus Areas listed below and (A) indicate if each listed Focus Area should be included in the curricular volume; (B) suggest any changes to the definition of the Focus Area and recommend the addition of Focus Areas not currently included.

Focus Areas:

1. Security and Risk Management [Includes: Security, Risk, Compliance, Law, Regulations, and Business Continuity]
2. Communication and Network Security [Includes: Designing and Protecting Network Security]
3. Identity and Access Management [Includes: Controlling Access and Managing Identity]
4. Security Assessment and Testing [Includes: Designing, Performing, and Analyzing Security Testing]
5. Asset Security [Includes: Protecting Security of Assets]
6. Security Engineering [Includes: Engineering and Management of Security]
7. Security Operations [Includes: Foundational Concepts, Investigations, Incident Management, and Disaster Recovery]
8. Software Development Security [Includes: Understanding, Applying, and Enforcing Software Security]

(A) Percentage of respondents affirming Focus Area



(B) Summary Comments on the Focus Areas

Survey respondents made several recommendations regarding the list of Focus Areas. The recommendations summarized below reflect the themes for each Focus Area.

Security and Risk Management

- Change the label of this category to "Governance, Risk, and Compliance" in order to highlight the importance of each of these topics.
- Reconsider the inclusion of business continuity. While it is an important topic, is it appropriately categorized here?
- Add audit to this category.

Communication and Network Security

- The content of this Focus Area should be reclassified as a Core Idea.
- Clarify the definition of the category and more precisely describe the content.

Identity and Access Management

- The content of this Focus Area is important, but may be too narrowly defined to stand as a separate category.

Security Assessment and Testing

- This category should include certification and audit.
- While important topics, this category is too narrow and should be combined with another focus area.

Asset Security

- Clarify the definition of assets (e.g. digital/physical/information) in this category.
- While important topics, this category is too narrow and should be combined with another focus area.

Security Engineering

- Clarify the definition of security engineering as a focus area.
- Exclude management from this category.

Security Operations

- Clarify the foundation concepts to be included in this category.
- Respondents affirmed the importance of this content within this category but were conflicted about whether the category was too broadly or too narrowly defined.

Software Development Security

- Clarify how this category differs from security engineering and from security operations. Should the categories be combined?

Other Comments

- Additional topics to include: incident management, ethics, social engineering, physical security, and policy.
- How were these areas determined? Consider using the NIST Framework and leveraging the categories: Identify, Protect, Detect, Respond, and Recover.
- Several overlapping areas of management should be included.

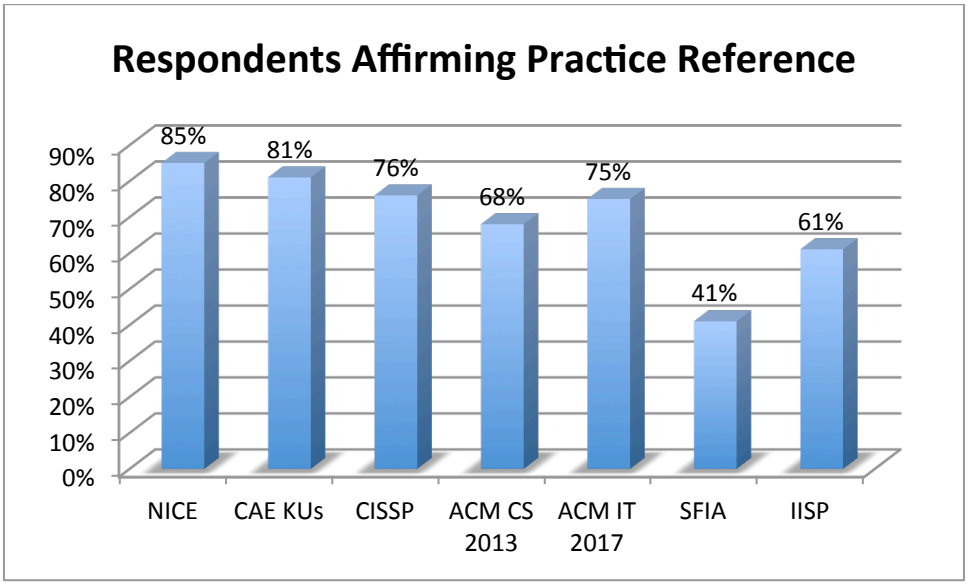
Practice

Practices are the combination of knowledge and skills that culminate into professional competency when connected with a particular Focus Area. Survey respondents were asked to consider the list of references below and (A) indicate if the practices derived from those sources should be included in the cybersecurity curricular volume; and (B) suggest any additional sources to include.

Practice:

- National Cybersecurity Workforce framework – NICE
- NSA Center of Academic Excellence, Knowledge Units - NSA KU
- (ISC)2 Certified Information Systems Security Professional – CISSP
- ACM Computer Science Curricula 2013 - CS 2013
- ACM/IEEE Information Technology Curriculum 2017 - IT 2017
- Skills Framework for the Information Age – SFIA
- Institute for Information Security Professionals Framework 2.0 - IISP 2.0

(A) Percentage of respondents affirming Practice Reference



(B) Summary Comments on Practice References

- Do not lean to heavily on any of these references. The relative quality and value of various references was mixed and many respondents noted that relevance will depend on the audience.
- The references are heavily US-centric. Add additional global reference points.
- Articulate how the inclusion of these practice references aligns with the purpose of the curricular volume. The references have many overlapping concepts and the inclusion of multiple frameworks will be confusing. A significant contribution of this volume would be to provide a guide to overlapping practices in these, and other frameworks.
- Cautiously distinguish between education and training – developing skills versus understanding concepts.
- Academic institutions of varying types continue to struggle in the process of mapping their curricula to any of these references. Guidance on this process would be valuable to the audience of this curricular volume – noting however, that the value of each reference is dependent upon the specific audience.

Cross-Cutting Concepts

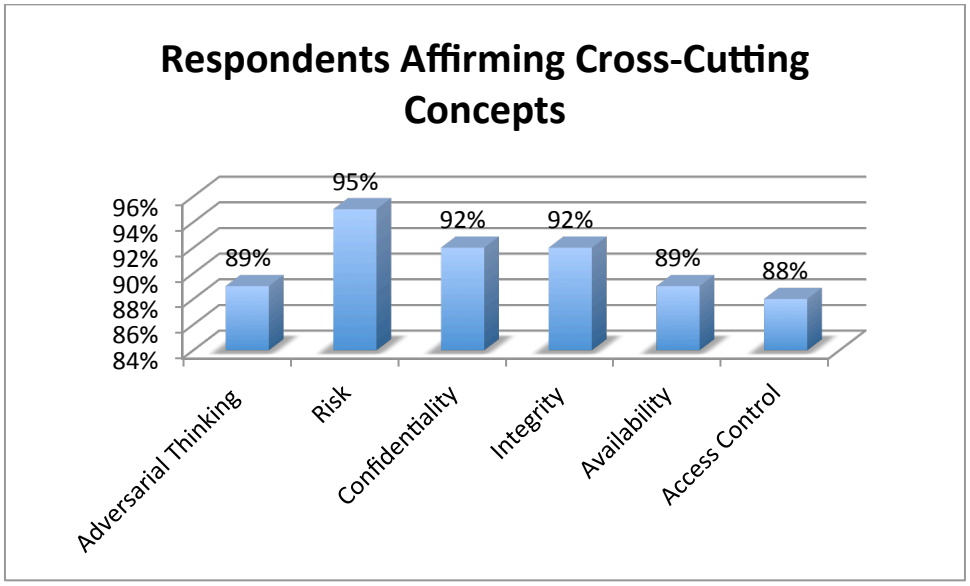
Cross-Cutting Concepts bridge core ideas, practices and focus areas. Survey respondents were asked to review the Cross-Cutting Concepts listed below and (A) indicate if each

listed Cross-Cutting Concepts should be included in the curricular volume; (B) suggest any changes to the definition of the Cross-Cutting Concepts and recommend the addition of Cross-Cutting Concepts not currently included.

Cross-Cutting Concepts:

1. Adversarial Thinking
2. Risk
3. Confidentiality
4. Integrity
5. Availability
6. Access control

(A) Percentage of respondents affirming Cross-Cutting Concept



(B) Summary Comments on Cross-Cutting Concepts

Survey respondents made several recommendations regarding the list of Cross-Cutting Concepts. The recommendations summarized below reflect the themes for each Cross-Cutting Concepts.

Adversarial Thinking

- Clarify the definition of adversarial thinking. Based on the definition, this concept could be foundational or it could be more oriented toward attacker/offensive thinking.

Risk

- Clarify the definition of risk. Is this concept related to IT management or considered more broadly with a business/organizational focus?

Confidentiality

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Integrity

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Availability

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Access control

- Access control is not at the same level of importance as the other cross-cutting concepts.
- Clarify the definition of access control. Is it more than a mechanism or a technology?

Overall Comments

- Clarify the definition of cross-cutting concepts. What is the underlying principle that guides the content of this section? Is the intent to provide foundational knowledge or cross-cutting ideas? Rethink the level of the concepts and the breadth of topics included in the category.
- Consider adding ethics, privacy, non-repudiation and human-factors/people-oriented ideas.

Summary Comments on the Thought Model

General feedback on the thought model provided additional insight for the development process. Summary comments include:

- Clarify the intended audience of the curricular volume.
- Clarify the definitions and distinguish between the elements.
- Provide additional information on the content of each of the categories.

- Simplify the model.
- Provide a logical placement for emerging topics.

This report provides an overview of the feedback received from the stakeholder survey on the development of the first set of global cybersecurity curricular guidelines. The Joint Task Force continues to review and incorporate the detailed feedback into the development process.

The first draft of the Cybersecurity Curricular Volume will be released to the public in late 2016. Community engagement opportunities will be continuously updated on the csec2017.org website and community members are welcome to provide specific feedback to the JTF via that website at anytime.

The Joint Task Force will hold a Special Session at the ACM SIGCSE Meeting, March 8-11, 2017 in Seattle, Washington USA to discuss the draft document. Details on the specific time and location of the special session are forthcoming. Please plan to attend.