PAPERWORK REDUCTION ACT STATEMENT

According to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The OMB control number for this collection is 3170-0024. It expires on 05/31/2022. The time required to complete this information collection is estimated to average approximately one half hour per response. Comments regarding this collection of information, including the estimated response time, suggestions for improving the usefulness of the information, or suggestions for reducing the burden to respond to this collection should be submitted to Bureau of Consumer Financial Protection (Attention: PRA Office), 1700 G Street NW, Washington, DC 20552, or by email to PRA_Comments@cfpb.gov. The Cybersecurity Team is conducting a survey of contractors to inform a skills gap analysis as part of a process to increase cybersecurity maturity levels at the Bureau.

PRIVACY NOTICE

The Cybersecurity Team is conducting a survey of contractors to inform a skills gap analysis as part of a process to increase cybersecurity maturity levels at the Bureau.

No Personally Identifiable Information (PII) will be collected in this anonymized survey. However, due to possible small sample sizes on certain teams there is a risk that your survey response may be re-identifiable based on your answers to the questions.

Participation in this survey is voluntary.

Particiants will be asked to rate their knowledge, on a scale from 1 to 5 with 1 being no experience and 5 being advanced/expert experience, for several key functional areas relating to the specific workforce role they have been assigned.

NICE Work Role	OPM Cyber Code	Shortcut	Link to Public Results
Technical Support Specialist	411	View KSA	
Database Administrator	421	View KSA	
Data Analyst	422	View KSA	
Knowledge Manager	431	View KSA	
Network Operations Specialist	441	View KSA	
System Administrator	451	View KSA	
Cyber Defense Analyst	511	View KSA	
Cyber Defense Incident Responder	531	View KSA	
Software Developer	621	View KSA	
Secure Software Assessor	622	View KSA	
Enterprise Architect	651	View KSA	
Security Architect	652	View KSA	
Research & Development Specialist	661	View KSA	
System Testing and Evaluation Specialist	671	View KSA	
Information Systems Security Manager	722	View KSA	
Cyber Legal Advisor	731	View KSA	
Cyber Policy and Strategy Planner	752	View KSA	
Executive Cyber Leadership	901	View KSA	
COR	COR	View KSA	
Exploitation Analyst	121	View KSA	
Systems Security Analyst	461	View KSA	
Cyber Defense Infrastructure Support Specialist	521	View KSA	
Vulnerability Assessment Assistant	541	View KSA	
Security Control Assessor	612	View KSA	
Information Systems Security Developer	631	View KSA	
Systems Developer	632	View KSA	
Cyber Instructional Curriculum Developer	711	View KSA	
Cyber Instructor	712	View KSA	
Program Manager	801	View KSA	
IT Project Manager	802	View KSA	
IT Investment/Portfolio Manager	804	View KSA	
Systems Requirements Planner	641	View KSA	

Click to return to TOC

641- Systems Requirements Planner

Ability to interpret and translate customer requirements into operational capabilities.

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, avail

Ability to identify critical infrastructure systems with information communication technology that were designed without syste

Knowledge of computer networking concepts and protocols, and network security methodologies.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

Knowledge of cybersecurity and privacy principles.

Knowledge of cyber threats and vulnerabilities.

Knowledge of specific operational impacts of cybersecurity lapses.

Knowledge of applicable business processes and operations of customer organizations.

Knowledge of capabilities and requirements analysis.

Knowledge of encryption algorithms

Knowledge of cryptography and cryptographic key management concepts

Knowledge of resiliency and redundancy.

Knowledge of installation, integration, and optimization of system components.

Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmiss

Knowledge of industry-standard and organizationally accepted analysis principles and methods.

Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, avai

Knowledge of information security systems engineering principles (NIST SP 800-160).

Knowledge of information technology (IT) architectural concepts and frameworks.

Knowledge of microprocessors.

Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML)

Knowledge of new and emerging information technology (IT) and cybersecurity technologies.

Knowledge of operating systems.

Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open

Knowledge of parallel and distributed computing concepts.

Knowledge of Privacy Impact Assessments.

Knowledge of process engineering concepts.

Knowledge of secure configuration management techniques.

Knowledge of key concepts in security management (e.g., Release Management, Patch Management).

Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.

Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International O

Knowledge of system life cycle management principles, including software security and usability.

Knowledge of systems testing and evaluation methods.

Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Mul

Knowledge of the organization’s enterprise information technology (IT) goals and objectives.

Knowledge of the systems engineering process.

Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)

Knowledge of critical information technology (IT) procurement requirements.

Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., eleme

Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch gui

Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, an

Knowledge of critical infrastructure systems with information communication technology that were designed without system
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring
Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory serv
Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-of
Knowledge of controls related to the use, processing, storage, and transmission of data.

Skill in applying and incorporating information technologies into proposed solutions.
Skill in applying confidentiality, integrity, and availability principles.
Skill in applying organization-specific systems analysis principles and techniques.
Skill in conducting capabilities and requirements analysis.
Skill in design modeling and building use cases (e.g., unified modeling language).
Skill in conducting reviews of systems.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availab

Click to return to TOC

804- IT Investment/Portfolio Manager

Ability to oversee the development and update of the life cycle cost estimate.

Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of cybersecurity and privacy principles.
Knowledge of cyber threats and vulnerabilities.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Risk Management Framework (RMF) requirements.
Knowledge of resource management principles and techniques.
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the exte
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of the organization's core business/mission processes.
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of risk threat assessment.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements
Knowledge of how to leverage research and development centers, think tanks, academic research, and industry systems.
Knowledge of information technology (IT) acquisition/procurement requirements.
Knowledge of the acquisition/procurement life cycle process.

Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended ente

Click to return to TOC

121 - Exploitatin Analyst

Ability to accurately and completely source all data used in intelligence, assessment and/or planning produc
Ability to collaborate effectively with others.
Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner t
Ability to develop or recommend analytic approaches or solutions to problems and situations for which info
Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradi
Ability to expand network access by conducting target analysis and collection to identify targets of interest.
Ability to identify/describe target vulnerability.
Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
Ability to select the appropriate implant to achieve operational goals.

Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.
Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.
Knowledge of collection management processes, capabilities, and limitations.
Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologie
Knowledge of common networking devices and their configurations.
Knowledge of common reporting databases and tools.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of concepts, terminology, and operations of a wide range of communications media (computer a
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation o
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optica
Knowledge of data flow process for terminal or environment collection.
Knowledge of evasion strategies and techniques.
Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (
Knowledge of identification and reporting processes.
Knowledge of implants that enable cyber collection and/or preparation activities.
Knowledge of internal and external customers and partner organizations, including information needs, obje
Knowledge of Internet and routing protocols.
Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port num
Knowledge of intrusion sets.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of midpoint collection (process, objectives, organization, targets, etc.).
Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection
Knowledge of network topology.
Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objecti
Knowledge of organizational and partner policies, tools, capabilities, and procedures.
Knowledge of physical computer components and architectures, including the functions of various compone
Knowledge of principles of the collection development processes (e.g., Dialed Number Recognition, Social N
Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, M
Knowledge of relevant reporting and dissemination procedures.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of scripting

Knowledge of security concepts in operating systems (e.g., Linux, Unix.)
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of strategies and tools for target research.
Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, I
Knowledge of target intelligence gathering and operational preparation techniques and life cycles.
Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).
Knowledge of the basic structure, architecture, and design of converged applications.
Knowledge of the basic structure, architecture, and design of modern communication networks.
Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process manageme
Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
Knowledge of website types, administration, functions, and content management system (CMS).

Skill in analyzing traffic to identify network devices.
Skill in creating and extracting important information from packet captures.
Skill in creating collection requirements in support of data acquisition activities.
Skill in creating plans in support of remote operations. (i.e., hot/warm/cold/alternative sites, disaster recove
Skill in depicting source or collateral data on a network map.
Skill in determining the effect of various router and firewall configurations on traffic patterns and network p
Skill in evaluating accesses for intelligence value.
Skill in generating operation plans in support of mission and target requirements.
Skill in identifying gaps in technical capabilities.
Skill in identifying the devices that work at each level of protocol models.
Skill in identifying, locating, and tracking targets via geospatial analysis techniques
Skill in interpreting compiled and interpretive programming languages.
Skill in interpreting metadata and content as applied by collection systems.
Skill in navigating network visualization software.
Skill in performing data fusion from existing intelligence for enabling new and continued collection.
Skill in recognizing and interpreting malicious network activity in traffic.
Skill in recognizing midpoint opportunities and essential information.
Skill in recognizing technical information that may be used for leads to enable remote operations (data inclu
Skill in researching vulnerabilities and exploits utilized in traffic.
Skill in target development in direct support of collection operations.
Skill in using databases to identify target-relevant information.
Skill in using non-attributable networks.
Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruct
Skill in writing (and submitting) requirements to meet gaps in technical capabilities.

:ts.

hrough verbal, written, and/or visual means.
rmation is incomplete or for which no precedent exists.
:tory) into high quality, fused targeting/intelligence products.

:s, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.

ınd telephone networks, satellite, fiber, wireless).
f privileges, maintaining access, network exploitation, covering tracks).

ıl devices, removable media).

(e.g., email, http).

:tives, structure, capabilities, etc.

bering).

ı).

ves.

ents and peripherals (e.g., CPUs, Network Interface Cards, data storage).
etwork Analysis).
IcAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities.

OS, Android, and Windows operating systems.

ent, directory structure, installed applications).

ery).

erformance in both LAN and WAN environments.

ides users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, dom

ion.

ıain servers, SMTP header information).

Click to return to TOC

411 - Technical Support Specialist

Ability to accurately define incidents, problems, and events in the trouble ticketing system.

Ability to design capabilities to find solutions to less common and more complex system problems.

Ability to develop, update, and/or maintain standard operating procedures (SOPs).

Knowledge of an organization's information classification program and procedures for information compromise.

Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.

Knowledge of organizational security policies.

Knowledge of Payment Card Industry (PCI) data security standards.

Knowledge of Personal Health Information (PHI) data security standards.

Knowledge of Personally Identifiable Information (PII) data security standards.

Knowledge of procedures used for documenting and querying reported incidents, problems, and events.

Knowledge of remote access processes, tools, and capabilities related to customer support.

Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.

Knowledge of the basic operation of computers.

Knowledge of the operations and processes for incident, problem, and event management.

Skill in conducting research for troubleshooting novel client-level problems.

Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or sp

Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mi

Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.

Skill to design incident response for cloud service models.

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC Click to return to TOC Click to return to TOC

Click to return to TOC

421 - Database Administrator

Ability to maintain databases. (i.e., backup, restore, delete data, transaction log files, etc.).

Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) se
Knowledge of current and emerging data remediation security features in databases.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of data administration and data standardization policies.
Knowledge of data backup and recovery.
Knowledge of data mining and data warehousing principles.
Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
Knowledge of database management systems, query languages, table relationships, and views.
Knowledge of database theory.
Knowledge of digital rights management.
Knowledge of enterprise messaging systems and associated software.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SP
Knowledge of operating systems.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of policy-based and risk adaptive access controls.
Knowledge of query languages such as SQL (structured query language).
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of sources, characteristics, and uses of the organization’s data assets.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of the characteristics of physical and virtual data storage media.

Skill in allocating storage capacity in the design of data management systems.
Skill in conducting queries and developing algorithms to analyze data structures.
Skill in generating queries and reports.
Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).
Skill in optimizing database performance.

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to ret

Click to return to TOC

422 - Database Analyst

Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
Ability to build complex data structures and high-level programming languages.
Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
Ability to identify basic common coding flaws at a high level.
Ability to use data visualization tools (e.g., Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tablea
Knowledge of advanced data remediation security features in databases.
Knowledge of applications that can log errors, exceptions, and application faults and logging.
Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of computer programming principles
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of data administration and data standardization policies.
Knowledge of data mining and data warehousing principles.
Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
Knowledge of database management systems, query languages, table relationships, and views.
Knowledge of database theory.
Knowledge of digital rights management.
Knowledge of enterprise messaging systems and associated software.
Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and Pig to explore data.
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compressio
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of low-level computer languages (e.g., assembly languages).
Knowledge of machine learning theory and principles.
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SP
Knowledge of operating systems.
Knowledge of policy-based and risk adaptive access controls.
Knowledge of programming language structures and logic.
Knowledge of query languages such as SQL (structured query language).
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of secure coding techniques.
Knowledge of sources, characteristics, and uses of the organization’s data assets.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of the capabilities and functionality associated with various technologies for organizing and managing informa
Skill in assessing the predictive power and subsequent generalizability of a model.
Skill in conducting queries and developing algorithms to analyze data structures.
Skill in creating and utilizing mathematical or statistical models.
Skill in data mining techniques (e.g., searching file systems) and analysis.
Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering
Skill in developing data dictionaries.
Skill in developing data models.
Skill in developing machine understandable semantic ontologies.
Skill in generating queries and reports.

Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Informatio
Skill in identifying hidden patterns or relationships.
Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
Skill in performing format conversions to create a standard representation of the data.
Skill in performing sensitivity analysis.
Skill in reading Hexadecimal data.
Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Met
Skill in the use of design modeling (e.g., unified modeling language).
Skill in transformation analytics (e.g., aggregation, enrichment, processing).
Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).
Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).
Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS).
Skill in using data mapping tools.
Skill in using outlier identification and removal techniques.
Skill in writing code in a currently supported programming language (e.g., Java, C++).
Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.
Skill to identify sources, characteristics, and uses of the organization’s data assets.

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to ret

Click to return to TOC

431 - Knowledge Manager

Ability to match the appropriate knowledge repository technology for a given application or environment.

Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurem
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.
Knowledge of data mining techniques.
Knowledge of database theory.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of taxonomy and semantic ontology theory.
Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networkin
Knowledge of the capabilities and functionality associated with various technologies for organizing and managing informa
Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).
Knowledge of the organization's core business/mission processes.
Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and s
Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).

Skill in conducting information searches.
Skill in conducting knowledge mapping (e.g., map of knowledge repositories).
Skill in the measuring and reporting of intellectual capital.
Skill in using knowledge management technologies.

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to ret

Click to return to TOC

441 - Network Operations Specialist

Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
Ability to monitor measures or indicators of system performance and availability.
Ability to monitor traffic flows across the network.
Ability to operate common network tools (e.g., ping, traceroute, nslookup).
Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Vic
Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related
Ability to operate the organization's LAN/WAN pathways.

Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmissic
Knowledge of communication methods, principles, and concepts that support the network infrastructure.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone
Knowledge of controls related to the use, processing, storage, and transmission of data.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transr
Knowledge of cybersecurity and privacy principles.
Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], O
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of local area and wide area networking principles and concepts including bandwidth management.
Knowledge of measures or indicators of system performance and availability.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., app
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitor
Knowledge of network tools (e.g., ping, traceroute, nslookup)
Knowledge of organization's Local and Wide Area Network connections.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of remote access technology concepts.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
Knowledge of server administration and systems engineering theories, concepts, and methods.
Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastruct
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of symmetric key rotation techniques and concepts.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, N
Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web for
Knowledge of the common attack vectors on the network layer.
Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).
Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wirel
Knowledge of Virtual Private Network (VPN) security.
Knowledge of Voice over IP (VoIP).

Knowledge of web filtering technologies.
Knowledge of Wi-Fi.

Skill in analyzing network traffic capacity and performance characteristics.
Skill in applying various subnet techniques (e.g., CIDR)
Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate
Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection system
Skill in establishing a routing schema.
Skill in implementing and testing network infrastructure contingency and recovery plans.
Skill in implementing, maintaining, and improving established network security practices.
Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.
Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
Skill in securing network communications.
Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

rom operating correctly.

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to retClick to retClick to ret

Click to return to TOC

451 - System Administrator

Ability to accurately define incidents, problems, and events in the trouble ticketing system.
Ability to apply an organization's goals and objectives to develop and maintain architecture.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, a
Ability to collaborate effectively with others.
Ability to develop, update, and/or maintain standard operating procedures (SOPs).
Ability to establish and maintain automated security control assessments
Ability to function effectively in a dynamic, fast-paced environment.
Ability to monitor measures or indicators of system performance and availability.
Ability to operate common network tools (e.g., ping, traceroute, nslookup).

Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Exter
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of local area and wide area networking principles and concepts including bandwidth management.
Knowledge of measures or indicators of system performance and availability.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., app
Knowledge of operating system command-line tools.
Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, acc
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of performance tuning tools and techniques.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of principles and methods for integrating system components.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of server and client operating systems.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system/server diagnostic tools and fault identification techniques.
Knowledge of systems administration concepts.
Knowledge of systems engineering theories, concepts, and methods.
Knowledge of the enterprise information technology (IT) architecture.
Knowledge of the type and frequency of routine hardware maintenance.
Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wirel
Knowledge of Virtual Private Network (VPN) security.
Knowledge of virtualization technologies and virtual machine development and maintenance.

Skill in conducting system/server planning, management, and maintenance.
Skill in configuring and optimizing software.
Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti
Skill in correcting physical and technical problems that impact system/server performance.
Skill in diagnosing connectivity problems.
Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.

Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).
Skill in interfacing with customers.
Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
Skill in monitoring and optimizing system/server performance.
Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install a
Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).
Skill in troubleshooting failed system components (i.e., servers)
Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Comp

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

rom operating correctly.

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to retClick to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret	Click to ret	Click to ret	Click to ret	Click to ret	Click to ret	Click to ret	Click to ret	Click to ret	Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret Click to ret

Click to ret Click to ret Click to ret

Click to return to TOC

461 - Systems Security Analyst

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.

Knowledge of an organization's information classification program and procedures for information compron
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of configuration management techniques.
Knowledge of countermeasure design for identified security risks.
Knowledge of cryptography and cryptographic key management concepts
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of database systems.
Knowledge of developing and applying user credential management system.
Knowledge of embedded systems.
Knowledge of encryption algorithms
Knowledge of how to evaluate the trustworthiness of the supplier and/or product.
Knowledge of how to use network analysis tools to identify vulnerabilities.
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of human-computer interaction principles.
Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.
Knowledge of information technology (IT) risk management policies, requirements, and procedures.
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zone
Knowledge of information technology (IT) service catalogues.
Knowledge of installation, integration, and optimization of system components.
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operationa
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network design processes, to include understanding of security objectives, operational object
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of operating systems.
Knowledge of parallel and distributed computing concepts.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security management.
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model
Knowledge of security system design tools, methods, and techniques.
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of software engineering.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of systems security testing and evaluation methods.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectr

Knowledge of the systems engineering process.
Knowledge of various types of computer architectures.
Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-5
Skill in assessing security systems designs.
Skill in designing the integration of hardware and software solutions.
Skill in determining how a security system should work (including its resilience and dependability capabilitie
Skill in developing and applying security system access controls.
Skill in evaluating the adequacy of security designs.
Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
Skill in writing code in a currently supported programming language (e.g., Java, C++).
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality

ity, integrity, availability, authentication, non-repudiation).

nise.

lity, integrity, availability, authentication, non-repudiation).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

es, encryption).

al analysis).
nID, SAML, SPML).
ives, and trade-offs.
iples (e.g., application of defense-in-depth).
nance monitoring), and tools.

).

ogy Infrastructure Library, current version [ITIL]).

ral efficiency, Multiplexing).

3, Cybersecurity Framework, etc.).

s) and how changes in conditions, operations, or the environment will affect these outcomes.

, integrity, availability, authentication, non-repudiation).

ent version [ITIL]).

Click to return to TOC

511 - Cyber Defense Analyst

Ability to accurately and completely source all data used in intelligence, assessment and/or planning produc
Ability to analyze malware.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to apply techniques for detecting host and network-based intrusions using intrusion detection techno
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).

Knowledge of adversarial tactics, techniques, and procedures.
Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, exe
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of authentication, authorization, and access control methods.
Knowledge of collection management processes, capabilities, and limitations.
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of countermeasure design for identified security risks.
Knowledge of cryptography and cryptographic key management concepts
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation o
Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation spo
Knowledge of cyber defense and information security policies, procedures, and regulations.
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of database systems.
Knowledge of defense-in-depth principles and network security architecture.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
Knowledge of embedded systems.
Knowledge of encryption algorithms
Knowledge of encryption methodologies.
Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
Knowledge of how to use network analysis tools to identify vulnerabilities.
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of incident response and handling methodologies.
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zone
Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
Knowledge of interpreted and compiled computer languages.
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intru
Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network mapping and recreating network topologies.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),

Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of network tools (e.g., ping, traceroute, nslookup)
Knowledge of network traffic analysis methods.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of operating system command-line tools.
Knowledge of operating systems.
Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of policy-based and risk adaptive access controls.
Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activi
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model
Knowledge of security system design tools, methods, and techniques.
Knowledge of signature implementation impact for viruses, malware, and attacks.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of systems security testing and evaluation methods.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectr
Knowledge of the common attack vectors on the network layer.
Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organi
Knowledge of the use of sub-netting tools.
Knowledge of Virtual Private Network (VPN) security.
Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vul
Knowledge of Windows/Unix ports and services.

Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-5
Skill in collecting data from a variety of cyber defense resources.
Skill in conducting trend analysis.
Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
Skill in determining how a security system should work (including its resilience and dependability capabilitie
Skill in developing and deploying signatures.
Skill in evaluating the adequacy of security designs.
Skill in performing packet-level analysis.
Skill in reading and interpreting signatures (e.g., snort).
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
Skill in using incident handling methodologies.
Skill in using protocol analyzers.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality
Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.

:ts.

ity, integrity, availability, authentication, non-repudiation).
ologies.

ecutive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

f privileges, maintaining access, network exploitation, covering tracks).
onsored).

lity, integrity, availability, authentication, non-repudiation).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

es, encryption).

usions.

nID, SAML, SPML).

and directory services.

iples (e.g., application of defense-in-depth).
nance monitoring), and tools.

ities.

).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio

ral efficiency, Multiplexing).

ization.

nerabilities.

3, Cybersecurity Framework, etc.).

s) and how changes in conditions, operations, or the environment will affect these outcomes.

, integrity, availability, authentication, non-repudiation).

ent version [ITIL]).

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

521 - Cyber Defense Analyst

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Knowledge of basic system, network, and OS hardening techniques.

Knowledge of computer networking concepts and protocols, and network security methodologies.

Knowledge of cyber defense and information security policies, procedures, and regulations.

Knowledge of cyber threats and vulnerabilities.

Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Knowledge of cybersecurity and privacy principles.

Knowledge of data backup and recovery.

Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).

Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).

Knowledge of incident response and handling methodologies.

Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.

Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.

Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

Knowledge of network traffic analysis (tools, methodologies, processes).

Knowledge of network traffic analysis methods.

Knowledge of packet-level analysis.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of specific operational impacts of cybersecurity lapses.

Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).

Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.

Knowledge of Virtual Private Network (VPN) security.

Knowledge of web filtering technologies.

Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.

Skill in applying host/network access controls (e.g., access control list).

Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).

Skill in securing network communications.

Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).

Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.

Skill in tuning sensors.

Skill in using incident handling methodologies.

Skill in using Virtual Private Network (VPN) devices and encryption.

Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Click to return to TOC

531 - Cyber Defense Incident Responder

Ability to apply techniques for detecting host and network-based intrusions using intrusion detection techn
Ability to design incident response for cloud service models.

Knowledge of an organization's information classification program and procedures for information compron
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of business continuity and disaster recovery continuity of operations plans.
Knowledge of cloud service models and how those models can limit incident response.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation o
Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation spo
Knowledge of cyber defense and information security policies, procedures, and regulations.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of data backup and recovery.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
Knowledge of incident categories, incident responses, and timelines for responses.
Knowledge of incident response and handling methodologies.
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intr
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of malware analysis concepts and methodologies.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network services and protocols interactions that provide network communications.
Knowledge of network traffic analysis methods.
Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
Knowledge of packet-level analysis.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), a
Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vul

Skill in performing damage assessments.
Skill in preserving evidence integrity according to standard operating procedures or national standards.
Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, sp
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Skill in securing network communications.
Skill in using security event correlation tools.
Skill of identifying, capturing, containing, and reporting malware.
Skill to design incident response for cloud service models.

ologies.

nise.

f privileges, maintaining access, network exploitation, covering tracks).
onsored).

usions.

and directory services.
iples (e.g., application of defense-in-depth).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio
nd how they interact to provide network communications.
nerabilities.

pam filters).

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

541 - Vulnerability Assessment Assistant

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to apply programming language structures (e.g., source code review) and logic.
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
Ability to share meaningful insights about the context of an organization’s threat environment that improve

Knowledge of an organization’s threat environment.
Knowledge of an organization's information classification program and procedures for information compron
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of application vulnerabilities.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cryptography and cryptographic key management concepts
Knowledge of cryptology.
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation o
Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation spo
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of data backup and recovery.
Knowledge of data backup and restoration concepts.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of ethical hacking principles and techniques.
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of programming language structures and logic.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, I
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of systems diagnostic tools and fault identification techniques.
Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vul

Skill in conducting application vulnerability assessments.
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
Skill in mimicking threat behaviors.
Skill in performing impact/risk assessments.

Skill in reviewing logs to identify evidence of past intrusions.
Skill in the use of penetration testing tools and techniques.
Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality
Skill to develop insights about the context of an organization’s threat environment

ity, integrity, availability, authentication, non-repudiation).

its risk management posture.

nise.

f privileges, maintaining access, network exploitation, covering tracks).
onsored).

lity, integrity, availability, authentication, non-repudiation).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

nID, SAML, SPML).
and directory services.
iples (e.g., application of defense-in-depth).

).

OS, Android, and Windows operating systems.

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio

nerabilities.

, integrity, availability, authentication, non-repudiation).

ent version [ITIL]).

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

612 - Security Control Assessor

Ability to analyze test data.
Ability to answer questions in a clear and concise manner.
Ability to apply collaborative skills and strategies.
Ability to apply critical reading/thinking skills.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to ask clarifying questions.
Ability to collect, verify, and validate test data.
Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner t
Ability to communicate effectively when writing.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to design valid and reliable assessments.
Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
Ability to effectively collaborate via virtual teams.
Ability to ensure security practices are followed throughout the acquisition process.
Ability to evaluate information for reliability, validity, and relevance.
Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradi
Ability to exercise judgment when policies are not well-defined.
Ability to expand network access by conducting target analysis and collection to identify targets of interest.
Ability to facilitate small group discussions.
Ability to focus research efforts to meet the customer's decision-making needs.
Ability to function effectively in a dynamic, fast-paced environment.
Ability to function in a collaborative environment, seeking continuous consultation with other analysts and e
Ability to identify basic common coding flaws at a high level.
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to identify external partners with common cyber operations interests.
Ability to identify intelligence gaps.
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
Ability to identify/describe target vulnerability.
Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objecti
Ability to interpret and translate customer requirements into operational action.
Ability to interpret and understand complex and rapidly evolving concepts.
Ability to monitor advancements in information privacy technologies to ensure organizational adaptation ar
Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.
Ability to prepare and present briefings.
Ability to prioritize and allocate cybersecurity resources correctly and efficiently.
Ability to produce technical documentation.
Ability to recognize and mitigate cognitive biases which may affect analysis.
Ability to relate strategy, business, and technology in the context of organizational dynamics.
Ability to think critically.
Ability to translate data and test results into evaluative conclusions.
Ability to understand objectives and effects.
Ability to understand technology, management, and leadership issues related to organization processes and
Ability to understand the basic concepts and issues related to cyber and its organizational impact.
Ability to utilize multiple intelligence sources across all intelligence disciplines.

Ability to work across departments and business units to implement organization’s privacy principles and pr

Ability to work across departments and business units to implement organization’s privacy principles and pr

Knowledge of an organization's information classification program and procedures for information compron

Knowledge of applicable business processes and operations of customer organizations.

Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, exe

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Knowledge of application vulnerabilities.

Knowledge of authentication, authorization, and access control methods.

Knowledge of business continuity and disaster recovery continuity of operations plans.

Knowledge of capabilities and applications of network equipment including routers, switches, bridges, serve

Knowledge of communication methods, principles, and concepts that support the network infrastructure.

Knowledge of computer networking concepts and protocols, and network security methodologies.

Knowledge of controls related to the use, processing, storage, and transmission of data.

Knowledge of critical infrastructure systems with information communication technology that were designe

Knowledge of cryptography and cryptographic key management concepts

Knowledge of current industry methods for evaluating, implementing, and disseminating information techn

Knowledge of cyber defense and vulnerability assessment tools and their capabilities.

Knowledge of cyber threats and vulnerabilities.

Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential

Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, stora

Knowledge of cybersecurity and privacy principles.

Knowledge of data backup and recovery.

Knowledge of database systems.

Knowledge of embedded systems.

Knowledge of encryption algorithms

Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zone

Knowledge of information technology (IT) supply chain security and supply chain risk management policies,

Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.

Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope

Knowledge of network security architecture concepts including topology, protocols, components, and princi

Knowledge of new and emerging information technology (IT) and cybersecurity technologies.

Knowledge of organization's enterprise information security architecture.

Knowledge of organization's evaluation and validation requirements.

Knowledge of organization's Local and Wide Area Network connections.

Knowledge of Payment Card Industry (PCI) data security standards.

Knowledge of penetration testing principles, tools, and techniques.

Knowledge of Personal Health Information (PHI) data security standards.

Knowledge of Personally Identifiable Information (PII) data security standards.

Knowledge of Risk Management Framework (RMF) requirements.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, F

Knowledge of Security Assessment and Authorization process.

Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model

Knowledge of specific operational impacts of cybersecurity lapses.

Knowledge of structured analysis principles and methods.

Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)

Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of systems diagnostic tools and fault identification techniques.
Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organi
Knowledge of the enterprise information technology (IT) architecture.
Knowledge of the organization's enterprise information technology (IT) goals and objectives.
Knowledge of the organization's core business/mission processes.
Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

Skill in administrative planning activities, to include preparation of functional and specific support plans, pre
Skill in analyzing a target's communication networks.
Skill in analyzing traffic to identify network devices.
Skill in applying confidentiality, integrity, and availability principles.
Skill in applying secure coding techniques.
Skill in applying security controls.
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-5
Skill in assessing security systems designs.
Skill in conducting application vulnerability assessments.
Skill in conducting reviews of systems.
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Skill in determining how a security system should work (including its resilience and dependability capabilitie
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill in identifying intelligence gaps and limitations.
Skill in identifying language issues that may have an impact on organization objectives.
Skill in identifying leads for target development.
Skill in identifying measures or indicators of system performance and the actions needed to improve or corr
Skill in identifying non-target regional languages and dialects
Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.
Skill in identifying the devices that work at each level of protocol models.
Skill in identifying, locating, and tracking targets via geospatial analysis techniques
Skill in information prioritization as it relates to operations.
Skill in integrating and applying policies that meet system security objectives.
Skill in interfacing with customers.
Skill in interpreting compiled and interpretive programming languages.
Skill in interpreting metadata and content as applied by collection systems.
Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.
Skill in interpreting vulnerability scanner results to identify vulnerabilities.
Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).
Skill in managing client relationships, including determining client needs/requirements, managing client exp
Skill in managing test assets, test resources, and test personnel to ensure effective completion of test event
Skill in network systems management principles, models, methods (e.g., end-to-end systems performance n
Skill in performing impact/risk assessments.
Skill in performing root cause analysis.
Skill in performing target system analysis.
Skill in preparing and presenting briefings.
Skill in preparing plans and related correspondence.
Skill in preparing Test & Evaluation reports.
Skill in prioritizing target language material.
Skill in processing collected data for follow-on analysis.

Skill in providing analysis to aid writing phased after action reports.
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Skill in reviewing and editing assessment products.
Skill in reviewing and editing plans.
Skill in reviewing logs to identify evidence of past intrusions.
Skill in secure test plan design (e. g. unit, integration, system, acceptance).
Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
Skill in target development in direct support of collection operations.
Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementatio
Skill in technical writing.
Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution
Skill in using code analysis tools.
Skill in using manpower and personnel IT systems.
Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.
Skill in using security event correlation tools.
Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazo
Skill in utilizing feedback to improve processes, products, and services.
Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).
Skill to access information on current assets available, usage.
Skill to access the databases where plans/directives/guidance are maintained.
Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.
Skill to analyze target or threat sources of strength and morale.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality
Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information
Skill to evaluate requests for information to determine if response information exists.
Skill to extract information from available tools and applications associated with collection requirements an
Skill to identify cybersecurity and privacy issues that stem from connections with internal and external custo
Skill to use cyber defense Service Provider reporting structure and processes within one’s own organization.

ity, integrity, availability, authentication, non-repudiation).

hrough verbal, written, and/or visual means.

ctory) into high quality, fused targeting/intelligence products.

experts—both internal and external to the organization—to leverage analytical and technical expertise.

gned without system security considerations.

ves.

nd compliance.

l problem solving.

ograms, and align privacy objectives with security objectives.

ograms, and align privacy objectives with security objectives.

nise.

ecutive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

rs, transmission media, and related hardware.

d without system security considerations.

ology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standa

lity, integrity, availability, authentication, non-repudiation).

ge, and transmission of information or data.

s, encryption).

requirements, and procedures.

nID, SAML, SPML).

iples (e.g., application of defense-in-depth).

ederal Enterprise Architecture [FEA]).

).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio

ization.

paring and managing correspondence, and staffing procedures.

3, Cybersecurity Framework, etc.).

s) and how changes in conditions, operations, or the environment will affect these outcomes.

ect performance, relative to the goals of the system.

ectations, and demonstrating commitment to delivering quality results.
s.
nonitoring), and tools.

n of new technologies).

.

g., S/MIME email, SSL traffic).

n Elastic Compute Cloud, etc.).

, integrity, availability, authentication, non-repudiation).
n needed.

d collection operations management.
omers and partner organizations.

rds-based concepts and capabilities.

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

621 - Software Developer

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to develop secure software according to secure software deployment methodologies, tools, and prac
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to tailor code analysis for application-specific concerns.
Ability to use and understand complex mathematical concepts (e.g., discrete math).

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of computer programming principles
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cybersecurity and privacy principles and methods that apply to software development.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of embedded systems.
Knowledge of information technology (IT) risk management policies, requirements, and procedures.
Knowledge of interpreted and compiled computer languages.
Knowledge of local area and wide area networking principles and concepts including bandwidth manageme
Knowledge of low-level computer languages (e.g., assembly languages).
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of operating systems.
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of Privacy Impact Assessments.
Knowledge of programming language structures and logic.
Knowledge of root cause analysis techniques.
Knowledge of secure coding techniques.
Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guide
Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, F
Knowledge of software debugging principles.
Knowledge of software design tools, methods, and techniques.
Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
Knowledge of software engineering.
Knowledge of software quality assurance process.
Knowledge of software related information technology (IT) security principles and methods (e.g., moduliza
Knowledge of structured analysis principles and methods.
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of system design tools, methods, and techniques, including automated systems analysis and des
Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/poli
Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web serv

Skill in conducting software debugging.
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.

Skill in creating and utilizing mathematical or statistical models.
Skill in creating programs that validate and process multiple inputs including command line arguments, envi
Skill in designing countermeasures to identified security risks.
Skill in developing and applying security system access controls.
Skill in developing applications that can log and handle errors, exceptions, and application faults and logging
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill in performing root cause analysis.
Skill in secure test plan design (e. g. unit, integration, system, acceptance).
Skill in using code analysis tools.
Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g
Skill in writing code in a currently supported programming language (e.g., Java, C++).
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality

ity, integrity, availability, authentication, non-repudiation).
tices.
gned without system security considerations.

d without system security considerations.

lity, integrity, availability, authentication, non-repudiation).

nt.

and directory services.
iples (e.g., application of defense-in-depth).

es (STIGs), cybersecurity best practices on cisecurity.org).
Federal Enterprise Architecture [FEA]).

ation, layering, abstraction, data hiding, simplicity/minimization).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio
ign tools.
cy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, da
vice description language).

ronmental variables, and input streams.

g.

g., S/MIME email, SSL traffic).

, integrity, availability, authentication, non-repudiation).

ns, covert channel, replay, return-oriented attacks, malicious code).

ta loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

Click to return to TOC

622 - Secure Software Assessor

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to use and understand complex mathematical concepts (e.g., discrete math).

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of complex data structures.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of computer programming principles
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and methods that apply to software development.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of embedded systems.
Knowledge of information technology (IT) risk management policies, requirements, and procedures.
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of local area and wide area networking principles and concepts including bandwidth manageme
Knowledge of low-level computer languages (e.g., assembly languages).
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of operating systems.
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of Privacy Impact Assessments.
Knowledge of programming language structures and logic.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of root cause analysis techniques.
Knowledge of secure coding techniques.
Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guide
Knowledge of secure software deployment methodologies, tools, and practices.
Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, F
Knowledge of software debugging principles.
Knowledge of software design tools, methods, and techniques.
Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
Knowledge of software engineering.
Knowledge of software quality assurance process.
Knowledge of software related information technology (IT) security principles and methods (e.g., moduliza
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of structured analysis principles and methods.
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of system design tools, methods, and techniques, including automated systems analysis and des

Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/poli
Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web serv

Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Skill in designing countermeasures to identified security risks.
Skill in developing and applying security system access controls.
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill in integrating black box security testing tools into quality assurance process of software releases.
Skill in performing root cause analysis.
Skill in secure test plan design (e. g. unit, integration, system, acceptance).
Skill in using code analysis tools.
Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality

ity, integrity, availability, authentication, non-repudiation).
gned without system security considerations.

d without system security considerations.

lity, integrity, availability, authentication, non-repudiation).

nt.

iples (e.g., application of defense-in-depth).

es (STIGs), cybersecurity best practices on cisecurity.org).

Federal Enterprise Architecture [FEA]).

ation, layering, abstraction, data hiding, simplicity/minimization).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio
ign tools.

cy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, da
vice description language).

g., S/MIME email, SSL traffic).
, integrity, availability, authentication, non-repudiation).

ns, covert channel, replay, return-oriented attacks, malicious code).

ta loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

Click to return to TOC

631 - Information Systems Security Developer

Ability to analyze test data.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to apply network security architecture concepts including topology, protocols, components, and prin
Ability to apply secure system design tools, methods and techniques.
Ability to apply system design tools, methods, and techniques, including automated systems analysis and de
Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an orga
Ability to ask clarifying questions.
Ability to collaborate effectively with others.
Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner t
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to design architectures and frameworks.
Ability to ensure security practices are followed throughout the acquisition process.
Ability to function in a collaborative environment, seeking continuous consultation with other analysts and e
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.
Ability to produce technical documentation.
Ability to translate data and test results into evaluative conclusions.
Ability to understand objectives and effects.
Ability to understand the basic concepts and issues related to cyber and its organizational impact.

Knowledge of access authentication methods.
Knowledge of an organization's information classification program and procedures for information compron
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of countermeasure design for identified security risks.
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cryptology.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of database systems.
Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chi
Knowledge of embedded systems.
Knowledge of encryption algorithms
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of human-computer interaction principles.
Knowledge of information security systems engineering principles (NIST SP 800-160).
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zone
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and da
Knowledge of installation, integration, and optimization of system components.
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of local area and wide area networking principles and concepts including bandwidth manageme
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operationa

Knowledge of microprocessors.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network design processes, to include understanding of security objectives, operational object
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of operating systems.
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of parallel and distributed computing concepts.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of policy-based and risk adaptive access controls.
Knowledge of Privacy Impact Assessments.
Knowledge of process engineering concepts.
Knowledge of resiliency and redundancy.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guide
Knowledge of security management.
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
Knowledge of software engineering.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of structured analysis principles and methods.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of system design tools, methods, and techniques, including automated systems analysis and des
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.
Knowledge of systems testing and evaluation methods.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectr
Knowledge of the systems engineering process.

Skill in conducting audits or reviews of technical systems.
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
Skill in designing countermeasures to identified security risks.
Skill in designing security controls based on cybersecurity principles and tenets.
Skill in designing the integration of hardware and software solutions.
Skill in developing and applying security system access controls.
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill in evaluating the adequacy of security designs.
Skill in integrating and applying policies that meet system security objectives.
Skill in the use of design modeling (e.g., unified modeling language).
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality

ity, integrity, availability, authentication, non-repudiation).
ciples (e.g., application of defense-in-depth).

ɛsign tools.
anization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [T(

hrough verbal, written, and/or visual means.

experts—both internal and external to the organization—to leverage analytical and technical expertise.
gned without system security considerations.

nise.

d without system security considerations.

lity, integrity, availability, authentication, non-repudiation).

ips, and computer hardware).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

ɛs, encryption).
requirements, and procedures.
ta compression).

nt.
al analysis).

nID, SAML, SPML).
ives, and trade-offs.
and directory services.
iples (e.g., application of defense-in-depth).
nance monitoring), and tools.

es (STIGs), cybersecurity best practices on cisecurity.org).

).
ogy Infrastructure Library, current version [ITIL]).

ign tools.

g., International Organization for Standardization [ISO] guidelines) relating to system design.

al efficiency, Multiplexing).

, integrity, availability, authentication, non-repudiation).

OGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framewor

nt version [ITIL]).

·k [FEAF]).

Click to return to TOC

632 - Systems Developer

Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to identify critical infrastructure systems with information communication technology that were desi

Knowledge of access authentication methods.
Knowledge of an organization's information classification program and procedures for information compron
Knowledge of circuit analysis.
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of countermeasure design for identified security risks.
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cryptology.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of cybersecurity-enabled software products.
Knowledge of database systems.
Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chi
Knowledge of embedded systems.
Knowledge of encryption algorithms
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of human-computer interaction principles.
Knowledge of information security systems engineering principles (NIST SP 800-160).
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zone
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and da
Knowledge of installation, integration, and optimization of system components.
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of local area and wide area networking principles and concepts including bandwidth manageme
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operationa
Knowledge of microprocessors.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network design processes, to include understanding of security objectives, operational object
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of operating systems.
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of parallel and distributed computing concepts.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of policy-based and risk adaptive access controls.
Knowledge of Privacy Impact Assessments.
Knowledge of process engineering concepts.

Knowledge of resiliency and redundancy.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guide

Knowledge of security management.

Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model

Knowledge of service management concepts for networks and related standards (e.g., Information Technolo

Knowledge of software development models (e.g., Waterfall Model, Spiral Model).

Knowledge of software engineering.

Knowledge of specific operational impacts of cybersecurity lapses.

Knowledge of structured analysis principles and methods.

Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)

Knowledge of system design tools, methods, and techniques, including automated systems analysis and des

Knowledge of system life cycle management principles, including software security and usability.

Knowledge of system software and organizational design standards, policies, and authorized approaches (e.

Knowledge of systems testing and evaluation methods.

Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectr

Knowledge of the systems engineering process.

Knowledge of various types of computer architectures.

Skill in applying security controls.

Skill in conducting audits or reviews of technical systems.

Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU

Skill in creating policies that reflect system security objectives.

Skill in designing countermeasures to identified security risks.

Skill in designing security controls based on cybersecurity principles and tenets.

Skill in designing the integration of hardware and software solutions.

Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).

Skill in developing and applying security system access controls.

Skill in discerning the protection needs (i.e., security controls) of information systems and networks.

Skill in evaluating the adequacy of security designs.

Skill in integrating and applying policies that meet system security objectives.

Skill in network systems management principles, models, methods (e.g., end-to-end systems performance m

Skill in the use of design modeling (e.g., unified modeling language).

Skill in writing code in a currently supported programming language (e.g., Java, C++).

Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality

ity, integrity, availability, authentication, non-repudiation).
gned without system security considerations.

nise.

d without system security considerations.

lity, integrity, availability, authentication, non-repudiation).

ips, and computer hardware).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

es, encryption).
requirements, and procedures.
ta compression).

nt.
al analysis).

nID, SAML, SPML).
ives, and trade-offs.
and directory services.
iples (e.g., application of defense-in-depth).
nance monitoring), and tools.

es (STIGs), cybersecurity best practices on cisecurity.org).

).

ogy Infrastructure Library, current version [ITIL]).

ign tools.

g., International Organization for Standardization [ISO] guidelines) relating to system design.

al efficiency, Multiplexing).

specifications).

nonitoring), and tools.

, integrity, availability, authentication, non-repudiation).

:nt version [ITIL]).

Click to return to TOC

651 - Enterprise Architect

Ability to apply an organization's goals and objectives to develop and maintain architecture.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, a
Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's ent
Ability to build architectures and frameworks.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to execute technology integration processes.
Ability to identify critical infrastructure systems with information communication technology that were designed without
Ability to optimize systems to meet enterprise performance requirements.
Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrust

Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and
Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of circuit analysis.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of confidentiality, integrity, and availability requirements.
Knowledge of configuration management techniques.
Knowledge of critical infrastructure systems with information communication technology that were designed without syst
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity,
Knowledge of cybersecurity and privacy principles.
Knowledge of cybersecurity-enabled software products.
Knowledge of database systems.
Knowledge of demilitarized zones.
Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and comp
Knowledge of embedded systems.
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], O
Knowledge of industry-standard and organizationally accepted analysis principles and methods.
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compressio
Knowledge of installation, integration, and optimization of system components.
Knowledge of integrating the organization’s goals and objectives into the architecture.
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
Knowledge of multi-level security systems and cross domain solutions.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SP
Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trad
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory
Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., app
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monito
Knowledge of N-tiered typologies (e.g. including server and client operating systems).
Knowledge of operating systems.
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Mode
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of parallel and distributed computing concepts.

Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management polici
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of Security Assessment and Authorization process.
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
Knowledge of security system design tools, methods, and techniques.
Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastruct
Knowledge of software engineering.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system fault tolerance methodologies.
Knowledge of systems testing and evaluation methods.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, N
Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated desi
Knowledge of the Risk Management Framework Assessment Methodology.
Knowledge of the systems engineering process.
Knowledge of various types of computer architectures.

Skill in applying and incorporating information technologies into proposed solutions.
Skill in design modeling and building use cases (e.g., unified modeling language).
Skill in designing the integration of hardware and software solutions.
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how cha
Skill in the use of design methods.
Skill in writing code in a currently supported programming language (e.g., Java, C++).
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, ava
Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and part

ıework [FEAF]).

Click to return to TOC

652 - Security Architect

Ability to apply an organization's goals and objectives to develop and maintain architecture.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidential
Ability to apply network security architecture concepts including topology, protocols, components, and prin
Ability to apply secure system design tools, methods and techniques.
Ability to apply system design tools, methods, and techniques, including automated systems analysis and de
Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an orga
Ability to communicate effectively when writing.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to design architectures and frameworks.
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to optimize systems to meet enterprise performance requirements.
Ability to serve as the primary liaison between the enterprise architect and the systems security engineer ar
Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from
Ability, in close coordination with system security officers, advise authorizing officials, chief information offic

Knowledge of access authentication methods.
Knowledge of an organization's information classification program and procedures for information compron
Knowledge of applicable business processes and operations of customer organizations.
Knowledge of application vulnerabilities.
Knowledge of authentication, authorization, and access control methods.
Knowledge of business continuity and disaster recovery continuity of operations plans.
Knowledge of capabilities and applications of network equipment including routers, switches, bridges, serve
Knowledge of capabilities and requirements analysis.
Knowledge of communication methods, principles, and concepts that support the network infrastructure.
Knowledge of computer algorithms.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of confidentiality, integrity, and availability requirements.
Knowledge of configuration management techniques.
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cryptography and cryptographic key management concepts
Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidential
Knowledge of cybersecurity and privacy principles.
Knowledge of cybersecurity-enabled software products.
Knowledge of database systems.
Knowledge of demilitarized zones.
Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chi
Knowledge of embedded systems.
Knowledge of encryption algorithms
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of human-computer interaction principles.
Knowledge of industry-standard and organizationally accepted analysis principles and methods.
Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and da
Knowledge of installation, integration, and optimization of system components.

Knowledge of integrating the organization’s goals and objectives into the architecture.
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operationa
Knowledge of microprocessors.
Knowledge of multi-level security systems and cross domain solutions.
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, Ope
Knowledge of network design processes, to include understanding of security objectives, operational object
Knowledge of network hardware devices and functions.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of N-tiered typologies (e.g. including server and client operating systems).
Knowledge of operating systems.
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability N
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation criteria.
Knowledge of parallel and distributed computing concepts.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk mana
Knowledge of remote access technology concepts.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of Security Assessment and Authorization process.
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of software engineering.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system fault tolerance methodologies.
Knowledge of systems testing and evaluation methods.
Knowledge of technology integration processes.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectr
Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/poli
Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), a
Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline,
Knowledge of the Risk Management Framework Assessment Methodology.
Knowledge of the systems engineering process.
Knowledge of various types of computer architectures.

Skill in applying and incorporating information technologies into proposed solutions.
Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity mod
Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers,
Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus
Skill in design modeling and building use cases (e.g., unified modeling language).
Skill in designing countermeasures to identified security risks.
Skill in designing multi-level security/cross domain solutions.
Skill in designing the integration of hardware and software solutions.
Skill in determining how a security system should work (including its resilience and dependability capabilitie

Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from ot
Skill in the use of design methods.
Skill in translating operational requirements into protection needs (i.e., security controls).
Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g
Skill in using Virtual Private Network (VPN) devices and encryption.
Skill in writing test plans.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality
Skill to identify cybersecurity and privacy issues that stem from connections with internal and external custo

ity, integrity, availability, authentication, non-repudiation).
ciples (e.g., application of defense-in-depth).

esign tools.
anization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TC

gned without system security considerations.

nd coordinates with system owners, common control providers, and system security officers on the allocatio
other untrusted networks.
cers, senior information security officers, and the senior accountable official for risk management/risk execu

nise.

ers, transmission media, and related hardware.

d without system security considerations.

encryption) security features in databases (e.g. built-in cryptographic key management features).

lity, integrity, availability, authentication, non-repudiation).

ips, and computer hardware).

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

ta compression).

al analysis).

nID, SAML, SPML).
ives, and trade-offs.

and directory services.
nance monitoring), and tools.

Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).

agement policies, anti-tampering techniques, and requirements).

ogy Infrastructure Library, current version [ITIL]).

ral efficiency, Multiplexing).
cy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, da
nd how they interact to provide network communications.
validated design, and target architectures.)

el).
as appropriate).
software, anti-spyware).

s) and how changes in conditions, operations, or the environment will affect these outcomes.

:her untrusted networks.

g., S/MIME email, SSL traffic).

, integrity, availability, authentication, non-repudiation).
omers and partner organizations.

OGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framewor

n of security controls as system-specific, hybrid, or common controls.

tive (function), on a range of security-related issues (e.g. establishing system boundaries; assessing the sever

nt version [ITIL]).

ta loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

k [FEAF]).

rity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches

; security alerts; and potential adverse effects of identified vulnerabilities).

Click to return to TOC

661 - Research & Development Specialist

Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
Ability to prepare and present briefings.
Ability to produce technical documentation.

Knowledge of application vulnerabilities.
Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, r
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of covert communication techniques.
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of cryptography and cryptographic key management concepts
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of engineering concepts as applied to computer architecture and associated computer hardware
Knowledge of Extensible Markup Language (XML) schemas.
Knowledge of forensic footprint identification.
Knowledge of hacking methodologies.
Knowledge of hardware reverse engineering techniques.
Knowledge of industry standard security models.
Knowledge of industry technologies' potential cybersecurity vulnerabilities.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of middleware (e.g., enterprise service bus and message queuing).
Knowledge of mobile communications architecture.
Knowledge of network analysis tools used to identify software communications vulnerabilities.
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of networking protocols.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of operating system structures and internals (e.g., process management, directory structure, ins
Knowledge of operations security.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of software reverse engineering techniques.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/poli

Skill in applying and incorporating information technologies into proposed solutions.
Skill in applying secure coding techniques.
Skill in applying the systems engineering process.
Skill in creating and utilizing mathematical or statistical models.
Skill in designing the integration of technology processes and solutions, including legacy systems and moder
Skill in using scientific rules and methods to solve problems.

gned without system security considerations.

routers, switches, bridges, servers, transmission media, and related hardware.

d without system security considerations.

e/software.

requirements, and procedures.

iples (e.g., application of defense-in-depth).

talled applications).

cy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, da

n programming languages.

ta loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).

Click to return to TOC

671 - System Test and Evaluation Specialist

Ability to analyze test data.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, a
Ability to collect, verify, and validate test data.
Ability to translate data and test results into evaluative conclusions.

Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of critical infrastructure systems with information communication technology that were designed without syst
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, a
Knowledge of cybersecurity and privacy principles.
Knowledge of cybersecurity-enabled software products.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements,
Knowledge of interpreted and compiled computer languages.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of network hardware devices and functions.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., app
Knowledge of organization's enterprise information security architecture.
Knowledge of organization's evaluation and validation requirements.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterp
Knowledge of Security Assessment and Authorization process.
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of systems administration concepts.
Knowledge of systems testing and evaluation methods.
Knowledge of Test & Evaluation processes for learners.
Knowledge of the systems engineering process.

Skill in conducting test events.
Skill in conducting Test Readiness Reviews.
Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).
Skill in designing and documenting overall program Test & Evaluation strategies.
Skill in determining an appropriate level of test rigor for a given system.
Skill in developing operations-based testing scenarios.
Skill in evaluating test plans for applicability and completeness.
Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.
Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.
Skill in preparing Test & Evaluation reports.
Skill in providing Test & Evaluation resource estimate.
Skill in systems integration testing.

Skill in writing code in a currently supported programming language (e.g., Java, C++).
Skill in writing test plans.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, ava

Click to return to TOC

711 - Cyber Instructional Curriculum Developer

Ability to apply critical reading/thinking skills.
Ability to apply principles of adult learning.
Ability to apply the Instructional System Design (ISD) methodology.
Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner t
Ability to conduct training and education needs assessment.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to develop clear directions and instructional materials.
Ability to develop curriculum for use within a virtual environment.
Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
Ability to evaluate information for reliability, validity, and relevance.
Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
Ability to function in a collaborative environment, seeking continuous consultation with other analysts and e
Ability to monitor advancements in information privacy technologies to ensure organizational adaptation ar
Ability to operate common network tools (e.g., ping, traceroute, nslookup).
Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web foru
Ability to prepare and present briefings.
Ability to produce technical documentation.
Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
Ability to tailor technical and planning information to a customer's level of understanding.
Ability to think critically.
Ability to understand technology, management, and leadership issues related to organization processes and
Ability to understand the basic concepts and issues related to cyber and its organizational impact.

Knowledge of an organization's information classification program and procedures for information compron
Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulate
Knowledge of Learning Management Systems and their use in managing learning.
Knowledge of media production, communication, and dissemination techniques and methods, including alte
Knowledge of modes of learning (e.g., rote learning, observation).
Knowledge of organizational training and education policies, processes, and procedures.
Knowledge of principles and processes for conducting training and education needs assessment.
Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
Knowledge of Test & Evaluation processes for learners.
Knowledge of training and education principles and methods for curriculum design, teaching and instructior

Skill in applying technical delivery capabilities.
Skill in developing and executing technical training programs and curricula.
Skill in identifying gaps in technical capabilities.
Skill in identifying gaps in technical delivery capabilities.
Skill in talking to others to convey information effectively.
Skill in utilizing feedback to improve processes, products, and services.

hrough verbal, written, and/or visual means.

experts—both internal and external to the organization—to leverage analytical and technical expertise.

nd compliance.

ums, Direct Video Broadcasts).

problem solving.

nise.

ed, real-world situations.

ernative ways to inform via written, oral, and visual media.

for individuals and groups, and the measurement of training and education effects.

Click to return to TOC

712 - Cyber Instructor

Ability to apply critical reading/thinking skills.
Ability to apply principles of adult learning.
Ability to apply the Instructional System Design (ISD) methodology.
Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner t
Ability to conduct training and education needs assessment.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to develop clear directions and instructional materials.
Ability to develop curriculum for use within a virtual environment.
Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
Ability to evaluate information for reliability, validity, and relevance.
Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
Ability to function in a collaborative environment, seeking continuous consultation with other analysts and e
Ability to monitor advancements in information privacy technologies to ensure organizational adaptation ar
Ability to operate common network tools (e.g., ping, traceroute, nslookup).
Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web foru
Ability to prepare and present briefings.
Ability to produce technical documentation.
Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
Ability to tailor technical and planning information to a customer’s level of understanding.
Ability to think critically.
Ability to understand technology, management, and leadership issues related to organization processes and
Ability to understand the basic concepts and issues related to cyber and its organizational impact.

Knowledge of an organization's information classification program and procedures for information compron
Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulate
Knowledge of Learning Management Systems and their use in managing learning.
Knowledge of media production, communication, and dissemination techniques and methods, including alte
Knowledge of modes of learning (e.g., rote learning, observation).
Knowledge of organizational training and education policies, processes, and procedures.
Knowledge of principles and processes for conducting training and education needs assessment.
Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
Knowledge of Test & Evaluation processes for learners.
Knowledge of training and education principles and methods for curriculum design, teaching and instructior

Skill in applying technical delivery capabilities.
Skill in developing and executing technical training programs and curricula.
Skill in identifying gaps in technical capabilities.
Skill in identifying gaps in technical delivery capabilities.
Skill in talking to others to convey information effectively.
Skill in utilizing feedback to improve processes, products, and services.

hrough verbal, written, and/or visual means.

experts—both internal and external to the organization—to leverage analytical and technical expertise.

nd compliance.

ums, Direct Video Broadcasts).

problem solving.

nise.

ed, real-world situations.

ernative ways to inform via written, oral, and visual media.

for individuals and groups, and the measurement of training and education effects.

Click to return to TOC

722 - Information Systems Security Manager

Ability to apply techniques for detecting host and network-based intrusions using intrusion detection techno
Ability to identify critical infrastructure systems with information communication technology that were desi
Ability to integrate information security requirements into the acquisition process; using applicable baseline

Knowledge of an organization's information classification program and procedures for information compron
Knowledge of applicable business processes and operations of customer organizations.
Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, exe
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of business continuity and disaster recovery continuity of operations plans.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of controls related to the use, processing, storage, and transmission of data.
Knowledge of critical information technology (IT) procurement requirements.
Knowledge of critical infrastructure systems with information communication technology that were designe
Knowledge of current and emerging threats/threat vectors.
Knowledge of current industry methods for evaluating, implementing, and disseminating information techn
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, stora
Knowledge of cybersecurity and privacy principles.
Knowledge of data backup and recovery.
Knowledge of encryption algorithms
Knowledge of enterprise incident response program, roles, and responsibilities.
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet P
Knowledge of incident response and handling methodologies.
Knowledge of industry-standard and organizationally accepted analysis principles and methods.
Knowledge of information security program management and project management principles and techniqu
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intru
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of measures or indicators of system performance and availability.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS),
Knowledge of network security architecture concepts including topology, protocols, components, and princi
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems perforn
Knowledge of network traffic analysis methods.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of organization's risk tolerance and/or risk management approach.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of resource management principles and techniques.
Knowledge of Risk Management Framework (RMF) requirements.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, F
Knowledge of server administration and systems engineering theories, concepts, and methods.

Knowledge of server and client operating systems.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.
Knowledge of technology integration processes.
Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vul

Skill in creating policies that reflect system security objectives.
Skill in determining how a security system should work (including its resilience and dependability capabilitie
Skill in evaluating the trustworthiness of the supplier and/or product.

ologies.
gned without system security considerations.
: security controls as one of the sources for security requirements; ensuring a robust software quality contro

nise.

ecutive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

d without system security considerations.

ology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standa

ige, and transmission of information or data.

rotocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, curre

es.
requirements, and procedures.
usions.

and directory services.
iples (e.g., application of defense-in-depth).
nance monitoring), and tools.

Federal Enterprise Architecture [FEA]).

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio

g., International Organization for Standardization [ISO] guidelines) relating to system design.

nerabilities.

s) and how changes in conditions, operations, or the environment will affect these outcomes.

l process; and establishing multiple sources (e.g., delivery routes, for critical system elements).

rds-based concepts and capabilities.

ent version [ITIL]).

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

731 - Cyber Legal Advisor

Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.

Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engage
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of concepts and practices of processing digital forensic data.
Knowledge of cyber defense and information security policies, procedures, and regulations.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.
Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.
Knowledge of privacy disclosure statements based on current laws.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of specific operational impacts of cybersecurity lapses.

Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability,

Click to return to TOC

752 - Cyber Policy and Strategy Planner

Ability to determine the validity of technology trend data.
Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of org
Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cybe

Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of current and emerging cyber technologies.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of emerging technologies that have potential for exploitation.
Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Resea
Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).
Knowledge of industry indicators useful for identifying technology trends.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of strategic theory and practice.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scri
Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).
Knowledge of the organization's core business/mission processes.

Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and ma
Skill in preparing plans and related correspondence.

Click to return to TOC

802 - Program Manager/Acquisition

Ability to apply supply chain risk management standards.
Ability to ensure security practices are followed throughout the acquisition process.
Ability to evaluate/ensure the trustworthiness of the supplier and/or product.
Ability to oversee the development and update of the life cycle cost estimate.

Knowledge of Cloud-based knowledge management technologies and concepts related to security, governa
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of functionality, quality, and security requirements and how these will apply to specific items of
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized ac
Knowledge of how to leverage research and development centers, think tanks, academic research, and indu
Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supp
Knowledge of Import/Export Regulations related to cryptography and other security technologies.
Knowledge of information technology (IT) acquisition/procurement requirements.
Knowledge of information technology (IT) architectural concepts and frameworks.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability M
Knowledge of resource management principles and techniques.
Knowledge of Risk Management Framework (RMF) requirements.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of risk/threat assessment.
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of the acquisition/procurement life cycle process.
Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
Knowledge of the organization's core business/mission processes.

Skill in identifying measures or indicators of system performance and the actions needed to improve or corr
Skill to translate, track, and prioritize information needs and intelligence collection requirements across the

nce, procurement, and administration.

supply (i.e., elements and processes).
:ross the extended enterprise.
ıstry systems.
ɔly chain risk.

requirements, and procedures.

Λaturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).

ɔgy Infrastructure Library, current version [ITIL]).

ect performance, relative to the goals of the system.
extended enterprise.

Click to return to TOC

802 - IT Project Manager

Ability to apply supply chain risk management standards.
Ability to ensure security practices are followed throughout the acquisition process.
Ability to evaluate/ensure the trustworthiness of the supplier and/or product.
Ability to oversee the development and update of the life cycle cost estimate.

Knowledge of capabilities and requirements analysis.
Knowledge of Cloud-based knowledge management technologies and concepts related to security, governa
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of functionality, quality, and security requirements and how these will apply to specific items of
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized ac
Knowledge of how to leverage research and development centers, think tanks, academic research, and indu
Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supp
Knowledge of Import/Export Regulations related to cryptography and other security technologies.
Knowledge of industry-standard and organizationally accepted analysis principles and methods.
Knowledge of information technology (IT) acquisition/procurement requirements.
Knowledge of information technology (IT) architectural concepts and frameworks.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability N
Knowledge of resource management principles and techniques.
Knowledge of Risk Management Framework (RMF) requirements.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of risk/threat assessment.
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of the acquisition/procurement life cycle process.
Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
Knowledge of the organization's core business/mission processes.

Skill in identifying measures or indicators of system performance and the actions needed to improve or corr
Skill to translate, track, and prioritize information needs and intelligence collection requirements across the

nce, procurement, and administration.

supply (i.e., elements and processes).
cross the extended enterprise.
ıstry systems.
ɔly chain risk.

requirements, and procedures.

Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).

ɔgy Infrastructure Library, current version [ITIL]).

ect performance, relative to the goals of the system.
extended enterprise.

Click to return to TOC

901-Cyber Executive Leadership

Ability to apply critical reading/thinking skills.
Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in
Ability to ensure information security management processes are integrated with strategic and operational
Ability to ensure that senior officials within the organization provide information security for the informatio
Ability to exercise judgment when policies are not well-defined.
Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objecti
Ability to prioritize and allocate cybersecurity resources correctly and efficiently.
Ability to relate strategy, business, and technology in the context of organizational dynamics.
Ability to tailor technical and planning information to a customer’s level of understanding.
Ability to think critically.
Ability to understand technology, management, and leadership issues related to organization processes and
Ability to understand the basic concepts and issues related to cyber and its organizational impact.

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Knowledge of application vulnerabilities.
Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, r
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulate
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of emerging security issues, risks, and vulnerabilities.
Knowledge of industry technologies’ potential cybersecurity vulnerabilities.
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code
Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vul

Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, ap
Skill in creating policies that reflect system security objectives.
Skill to anticipate new security threats.
Skill to remain aware of evolving technical infrastructures.
Skill to use critical thinking to analyze organizational patterns and relationships.

support of organizational cyber activities.
planning processes.
n and systems that support the operations and assets under their control.

ves.

l problem solving.

routers, switches, bridges, servers, transmission media, and related hardware.

ed, real-world situations.

, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditio
nerabilities.

proachability, effective listening skills, appropriate use of style and language for the audience).

ns, covert channel, replay, return-oriented attacks, malicious code).

Click to return to TOC

801-COR

Ability to apply supply chain risk management standards.
Ability to ensure security practices are followed throughout the acquisition process.
Ability to evaluate/ensure the trustworthiness of the supplier and/or product.
Ability to oversee the development and update of the life cycle cost estimate.

Knowledge of Cloud-based knowledge management technologies and concepts related to security, governa
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of cyber threats and vulnerabilities.
Knowledge of cybersecurity and privacy principles.
Knowledge of functionality, quality, and security requirements and how these will apply to specific items of
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized ac
Knowledge of how to leverage research and development centers, think tanks, academic research, and indu
Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supp
Knowledge of Import/Export Regulations related to cryptography and other security technologies.
Knowledge of information technology (IT) acquisition/procurement requirements.
Knowledge of information technology (IT) architectural concepts and frameworks.
Knowledge of information technology (IT) supply chain security and supply chain risk management policies,
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability N
Knowledge of resource management principles and techniques.
Knowledge of Risk Management Framework (RMF) requirements.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of risk/threat assessment.
Knowledge of service management concepts for networks and related standards (e.g., Information Technolo
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Knowledge of supply chain risk management standards, processes, and practices.
Knowledge of system life cycle management principles, including software security and usability.
Knowledge of the acquisition/procurement life cycle process.
Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
Knowledge of the organization's core business/mission processes.

Skill in identifying measures or indicators of system performance and the actions needed to improve or corr
Skill to translate, track, and prioritize information needs and intelligence collection requirements across the

nce, procurement, and administration.

supply (i.e., elements and processes).
:ross the extended enterprise.
ıstry systems.
ɔly chain risk.

requirements, and procedures.

Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).

ɔgy Infrastructure Library, current version [ITIL]).

ect performance, relative to the goals of the system.
extended enterprise.