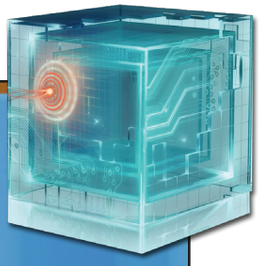


NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

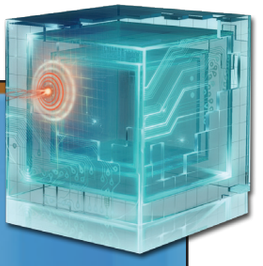
INTRODUCTION

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Two Executive Branch initiatives, in 2008 and 2010, founded the NICE.
[full text version]

DEFINING CYBERSECURITY

Defining the cybersecurity population in common terms is one of the major steps in building a robust workforce and providing meaningful training and professional development. NICE is working in collaboration with numerous federal government agencies, subject matter experts internal and external to the government, and industry partners.
[full text version]

CYBERSECURITY WORKFORCE FRAMEWORK



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

INTRODUCTION

PROTECTING OUR NATION'S DIGITAL INFRASTRUCTURE AGAINST THE GROWING THREAT OF CYBERCRIME AND STATE-SPONSORED INTRUSIONS AND OPERATIONS IS VITAL TO AMERICA'S CONTINUED SECURITY AND PROSPERITY.

Gen. Keith Alexander, Director of the National Security Agency and Commander of U.S. Cyber Command captured the scope of the issue in saying, "We now live in a world where a nation's security depends in no small part on the security awareness and practices of our agencies, firms, suppliers, schools, friends, neighbors, relatives and, well, all of us" (CSIS, 2010). Our nation's leaders recognize cybersecurity as a national imperative, and in 2010, President Obama established the National Initiative for Cybersecurity Education (NICE), which was formerly Initiative 8 under the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008).

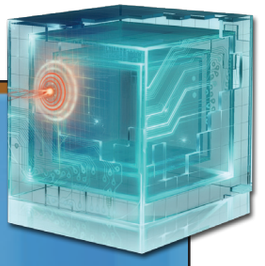
The NICE is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. It seeks to encourage and help build cybersecurity awareness and competence across the nation and to build an agile, highly skilled federal workforce capable of responding to a dynamic and rapidly developing array of threats.

Today, there is little consistency throughout the federal government and the nation in terms of how cybersecurity work is defined or described (e.g., there is significant variation in occupations, job titles, position description, and the Office of Personnel Management (OPM) series). This absence of a common language to discuss and understand the work and work requirements of cybersecurity hinders our nation's ability to understand the current baseline of capabilities and skills gaps, codify the pipeline of future talent, and collectively develop cybersecurity talent and workforces. Consequently, establishing and using a common lexicon, taxonomy, and other data standards for cybersecurity work and workers is not merely practical but vital for the NICE to achieve its mission.

This Cybersecurity Workforce Framework puts forth a working copy of such a framework that defines cybersecurity work and workers according to a common lexicon and taxonomy. It has been developed largely with input from the federal government, in particular the Intelligence Community and the Department of Defense. But that is not good enough; we need to ensure the Cybersecurity Workforce Framework can be adopted and used across America. In addition, it is currently based on the work requirements of cybersecurity as we know it today, but we need it to also address those skills and capabilities anticipated for the future. Therefore, we are seeking to refine and finalize the Cybersecurity Workforce Framework with input from every sector of our nation's cybersecurity stakeholders, including academia, cybersecurity organizations, and private industry. Your engagement is critical!

Please provide your ideas, suggestions, and specific feedback on the content of this document by following instructions at

http://csrc.nist.gov/nice/framework/



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

DEFINING THE CYBERSECURITY POPULATION

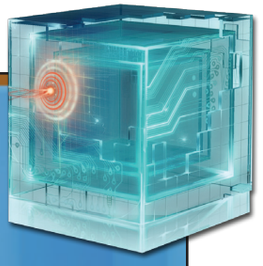
Defining the cybersecurity population in common terms is one of the major steps in building a robust workforce and providing meaningful training and professional development. NICE is working in collaboration with numerous federal government agencies, subject matter experts internal and external to the government, and industry partners. The intent of this work does not presume to get all federal agencies to change their organizational and occupational structures. It is recognized that such an effort would take many years, require significant resources, and not be needed to accomplish our goal of establishing a unified way to understand work and workers across a wide variety of organizations, both public and private. Instead, the taxonomy and lexicon being developed puts forth an overarching framework that can be overlaid onto any existing occupational structure, thereby helping achieve the goal of a healthy and prepared cybersecurity workforce.

The Defining Structure

The focus of this effort is on personnel whose primary job responsibilities require education and training in technical fields related to information technology, information assurance, and computer science. Consequently, with the exception of select critical support roles that allow cybersecurity professionals to effectively do their work, we did not include occupational specialties related to acquisition, physical security, oversight of critical infrastructure, electrical engineering, and so forth. Although these and other occupational specialties provide crucial support to federal government cybersecurity, the intent of this framework and the professional development program it informs was to develop a better understanding of how to train and equip the workforce with “cyber” skills.

To develop the cybersecurity framework, we adopted a “specialty area” construct. This simply groups work and workers according to the functions they share in common regardless of job titles, occupational series, or other organization-specific terms. Basically, specialty areas align work-related activities into groups that require similar competencies and may share comparable career paths. Within this definition, a single person may perform the tasks of more than one specialty area and multiple individuals may perform separate subsets of tasks from one specialty area. Because of the variety of jobs, occupations, and responsibilities within any given agency or organization, specialty areas serve as a framework that ties all those differences together under a common architecture. Specialty areas represent groupings of similar work at the task level. Within any given organization, the way these groupings are organized into jobs, career fields, or work roles depends on a number of factors including organizational characteristics (e.g., geographic location), constraints (e.g., limited personnel), and mission. Using this common lexicon and structure, we can begin to identify how seemingly variant jobs align across agencies.

The framework organizes specialty areas into seven high-level categories (as noted on the first page in colored boxes). The following paragraphs summarize each of these specialty areas.



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

DEFINING THE CYBERSECURITY POPULATION (CONTINUED)

Securely Provision consists of those specialty areas concerned with conceptualizing, designing, and building secure IT systems. In other words, each of the roles within the Securely Provision category is responsible for some aspect of the systems development process.

Operate and Maintain includes those specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Protect and Defend includes specialty areas primarily responsible for the identification, analysis, and mitigation of threats to IT systems and networks. Specialty areas in the Protect and Defend category are closely aligned to computer network defense service provider organizations and responsibilities.

Investigate specialty areas are responsible for the investigation of cyber events or crimes which occur within IT systems or networks, as well as the processing and use of digital evidence.

Operate and Collect includes specialty areas that have responsibility for the highly specialized collection of cybersecurity information that may be used to develop intelligence.

Analyze consists of specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. Although not part of the core set of specialty areas, there is also a category of specialty areas that have been determined critical to the support of the primary cybersecurity categories.

Support category includes specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

The following sections provide the cybersecurity workforce framework in its entirety. In addition to the information provided above, the full version of the framework includes the set of representative **Tasks and KSAs** for each of the specialty areas.

As you review, please take note of the sample job titles included within each specialty area. In working with multiple agencies, industry partners, and subject matter experts, we discovered that often different job titles were used for people who essentially performed the same work (i.e., same job tasks). Thus, in addition to the specialty area definitions, the sample job titles may help you understand where your organization's cybersecurity positions fall within this framework. When aligning specific positions to the framework, however, it is critical to use the specialty area definitions, tasks, and KSAs rather than similar job titles.

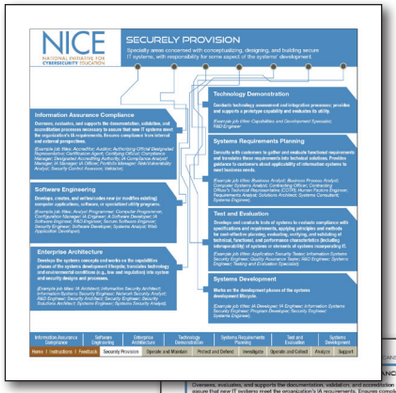
Call to Action

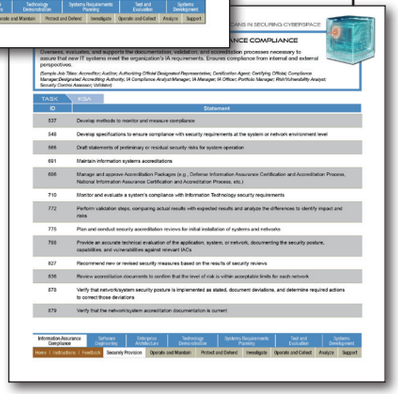
We hope organizations across the nation will begin to align their jobs and positions to this specialty area framework (and where this framework can be improved, please be sure to provide feedback to NICE). With a common structure and lexicon, we not only better understand the makeup of our cybersecurity population but also begin to identify the capabilities of those individuals. In doing so, we can begin to identify and develop the necessary workforce, training, and professional development opportunities to help address our growing cybersecurity concerns.

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

INSTRUCTIONS FOR USE





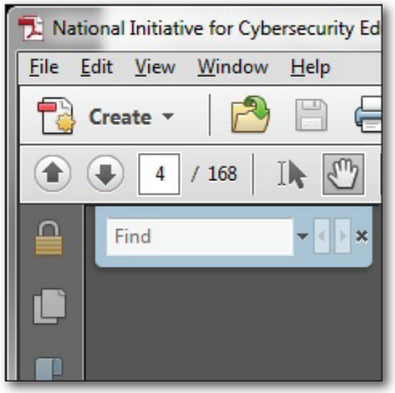
Access Guide Contents

To navigate to a particular category from the Home page, click on one of the seven category boxes or breadcrumb markers found at the bottom of the page. The breadcrumb markers appear on every page of the guide, allowing you to freely navigate the contents without the need to return to a specific point to further explore.

Once inside a category, you can select the specific specialty area you would like to further explore. Selecting a specialty area will bring up a detailed view of that specialty area featuring its associated tasks and KSAs as well as an additional set of specialty area-specific breadcrumb markers. You can switch between the tasks or KSAs at any time by selecting the "Task" or "KSA" tab above its list.

Search for Information

To conduct a search, press CTRL+F and type any keyword in the Find box of the Adobe Acrobat menu bar, then press Enter. The small arrow to the right of the Find box gives options for refining a search.



Provide Feedback

We are continually trying to improve this framework and we value your input. To provide feedback, please select the Feedback button below which will take you to **http://csrc.nist.gov/nice/framework/** which has a feedback form. That form can be submitted to **NICEFrameworkcomments@nist.gov**.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

SECURELY PROVISION

Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.

Technology Demonstration

Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

(Example job titles: Capabilities and Development Specialist; R&D Engineer

Information Assurance Compliance

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

(Example job titles: Accreditor; Auditor; Authorizing Official Designated Representative; Certification Agent; Certifying Official; Compliance Manager; Designated Accrediting Authority; IA Compliance Analyst/ Manager; IA Manager; IA Officer; Portfolio Manager; Risk/Vulnerability Analyst; Security Control Assessor; Validator).

Systems Requirements Planning

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

(Example job titles: Business Analyst; Business Process Analyst; Computer Systems Analyst; Contracting Officer; Contracting Officer's Technical Representative (COTR); Human Factors Engineer; Requirements Analyst; Solutions Architect; Systems Consultant; Systems Engineer).

Software Engineering

Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

(Example job titles: Analyst Programmer; Computer Programmer; Configuration Manager; IA Engineer; A Software Developer; IA Software Engineer; R&D Engineer; Secure Software Engineer; Security Engineer; Software Developer; Systems Analyst; Web Application Developer).

Test and Evaluation

Develops and conducts tests of systems to evaluate compliance with specifications and requirements, applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

(Example job titles: Application Security Tester; Information Systems Security Engineer; Quality Assurance Tester; R&D Engineer; Systems Engineer; Testing and Evaluation Specialist).

Enterprise Architecture

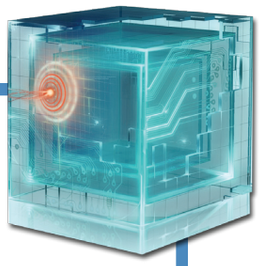
Develops the systems concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

(Example job titles: IA Architect; Information Security Architect; Information Systems Security Engineer; Network Security Analyst; R&D Engineer; Security Architect; Security Engineer; Security Solutions Architect; Systems Engineer; Systems Security Analyst).

Systems Development

Works on the development phases of the systems development lifecycle.

(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer).



SECURELY PROVISION

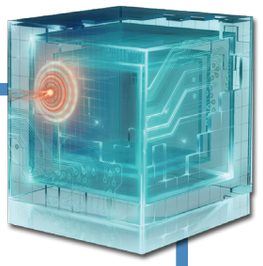
INFORMATION ASSURANCE COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

(Sample Job Titles: Accreditor; Auditor; Authorizing Official Designated Representative; Certification Agent; Certifying Official; Compliance Manager;Designated Accrediting Authority; IA Compliance Analyst/Manager; IA Manager; IA Officer; Portfolio Manager; Risk/Vulnerability Analyst; Security Control Assessor; Validator)

TASK | KSA

ID	Statement
537	Develop methods to monitor and measure compliance
548	Develop specifications to ensure compliance with security requirements at the system or network environment level
566	Draft statements of preliminary or residual security risks for system operation
691	Maintain information systems accreditations
696	Manage and approve Accreditation Packages (e.g., Defense Information Assurance Certification and Accreditation Process, National Information Assurance Certification and Accreditation Process, etc.)
710	Monitor and evaluate a system's compliance with Information Technology security requirements
772	Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks
775	Plan and conduct security accreditation reviews for initial installation of systems and networks
798	Provide an accurate technical evaluation of the application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant IACs
827	Recommend new or revised security measures based on the results of security reviews
836	Review accreditation documents to confirm that the level of risk is within acceptable limits for each network
878	Verify that network/system security posture is implemented as stated, document deviations, and determine required actions to correct those deviations
879	Verify that the network/system accreditation documentation is current



SECURELY PROVISION

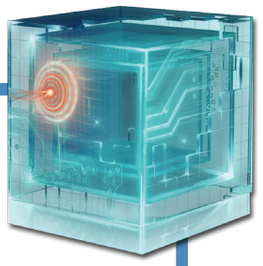
INFORMATION ASSURANCE COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

(Sample Job Titles: Accreditor; Auditor; Authorizing Official Designated Representative; Certification Agent; Certifying Official; Compliance Manager;Designated Accrediting Authority; IA Compliance Analyst/Manager; IA Manager; IA Officer; Portfolio Manager; Risk/Vulnerability Analyst; Security Control Assessor; Validator)

TASK / KSA

ID	Statement	Competency
58	Knowledge of identified vulnerabilities, alerts, and bulletins (IAVA, IAVB)	Information Systems/Network Security
69	Knowledge of IT security certification and accreditation requirements	Information Systems Security Certification
71	Knowledge of IT security principles and regulations	Information Systems Security Certification
77	Knowledge of methods for evaluating, implementing, and disseminating IT security tools and procedures	Information Systems/Network Security
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
97	Knowledge of pertinent government laws and information technology regulations	Legal, Government and Jurisprudence
121	Knowledge of structured analysis principles and methods	Logical Systems Design
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
143	Knowledge of the organization's enterprise IT goals and objectives	Enterprise Architecture
183	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system	Information Technology Performance Assessment



SECURELY PROVISION

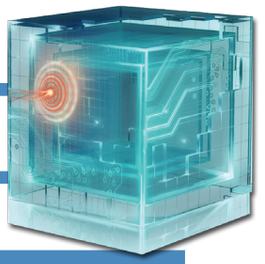
SOFTWARE ENGINEERING

Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Sample Job Titles: Analyst Programmer, Computer Programmer,Configuration Manager, IA Engineer, IA Software Developer, IA Software Engineer, R&D Engineer, Secure Software Engineer, Security Engineer, Software Developer, Systems Analyst, Web Application Developer

TASK | KSA

ID	Statement
408	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application
414	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints
417	Apply coding and testing standards, apply security testing tools (including "'fuzzing" static-analysis code scanning tools), and conduct code reviews
418	Apply secure code documentation
432	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules
446	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program
459	Conduct trial runs of programs and software applications to be sure they will produce the desired information and that the instructions are correct
461	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements and interfaces
465	Consult with customers about software system design and maintenance
467	Consult with engineering staff to evaluate interface between hardware and software
477	Correct errors by making appropriate changes and rechecking the program to ensure that the desired results are produced

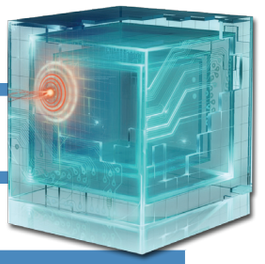


SECURELY PROVISION

SOFTWARE ENGINEERING

TASK | KSA

ID	Statement
506	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design
515	Develop and direct software system testing and validation procedures, programming, and documentation
543	Develop secure code and error messages
558	Direct software programming and development of documentation
602	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration
634	Identify basic common coding flaws at a high level
644	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development
645	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life
709	Modify existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance
756	Perform integrated QA testing for security functionality and resiliency attack
764	Perform secure programming and understand how to identify potential flaws in codes that will mitigate the possibility of vulnerabilities
770	Perform threat and vulnerability analysis whenever an application or system undergoes a major change
785	Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language
826	Recognize security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing

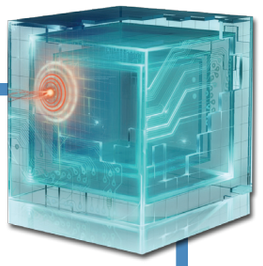


SECURELY PROVISION

SOFTWARE ENGINEERING

TASK | KSA

ID	Statement
850	Store, retrieve, and manipulate data for analysis of system capabilities and requirements
851	Supervise and assign work to programmers, designers, technologists,technicians, and other engineering and scientific personnel
865	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria



SECURELY PROVISION

SOFTWARE ENGINEERING

Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Sample Job Titles: Analyst Programmer, Computer Programmer,Configuration Manager, IA Engineer, IA Software Developer, IA Software Engineer, R&D Engineer, Secure Software Engineer, Security Engineer, Software Developer, Systems Analyst, Web Application Developer

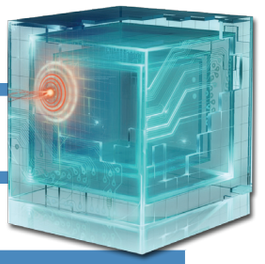
TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
6	Ability to use and understand mathematical concepts (e.g., discrete math)	Mathematical Reasoning
20	Knowledge of complex data structures	Object Technology
23	Knowledge of computer programming principles such as object-oriented design	Object Technology
38	Knowledge of agency IA architecture	Information Assurance
40	Knowledge of agency evaluation and validation requirements	Systems Testing and Evaluation
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
54	Knowledge of IA or IA-enabled software products	Information Assurance
56	Knowledge of IA principles and methods that apply to software development	Information Assurance
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
70	Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption	Information Systems/Network Security
72	Knowledge of local area and wide area networking principles and concepts including bandwidth management	Infrastructure Design
74	Knowledge of low-level computer languages (e.g., assembly languages)	Computer Languages

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SOFTWARE ENGINEERING

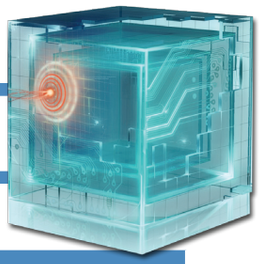
TASK | KSA

ID	Statement	Competency
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
91	Knowledge of networking architecture	Infrastructure Design
100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security
109	Knowledge of secure configuration management techniques	Configuration Management
116	Knowledge of software debugging principles	Software Development
117	Knowledge of software design tools, methods, and techniques	Software Development
118	Knowledge of software development models (waterfall model, spiral model, etc.)	Software Engineering
123	Knowledge of system and application security threats and vulnerabilities including buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, and malicious code	Vulnerabilities Assessment
149	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language	Web Technology
168	Skill in conducting software debugging	Software Development
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation
174	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams	Software Testing and Evaluation
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

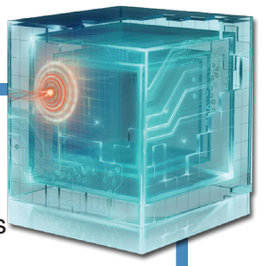


SECURELY PROVISION

SOFTWARE ENGINEERING

TASK | KSA

ID	Statement	Competency
185	Skill in developing applications that can log errors, exceptions, and application faults and logging	Software Development
191	Skill in developing and applying security system access controls	Identity Management
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages
904	Knowledge of interpreted and compiled computer languages	Computer Languages
905	Knowledge of secure coding techniques	Software Development
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment



SECURELY PROVISION

ENTERPRISE ARCHITECTURE

Develops the systems concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Sample Job Titles: IA Architect; Information Security Architect; Information Systems Security Engineer; Network Security Analyst; R&D Engineer; Security Architect; Security Engineer; Security Solutions Architect; Systems Engineer; Systems Security Analyst.

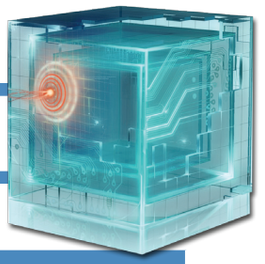
TASK | KSA

ID	Statement
413	Analyze user needs and requirements to plan system architecture
437	Collaborate with system developers to select appropriate design solutions or ensure the compatibility of system components
483	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event
484	Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration
502	Design system architecture or system components required to meet user needs
511	Develop a system security context and a preliminary system security concept of operations, and define baseline system security requirements in accordance with applicable IA requirements
561	Document and address agency information security, IA architecture and systems security engineering requirements throughout the acquisition lifecycle
563	Document design specifications, installation instructions, and other system-related information
569	Ensure all definition and architecture activities (system lifecycle support plans, concept of operations, operational procedures and maintenance training materials, etc.) are properly documented and updated as necessary
579	Ensure that acquired or developed system(s) and architecture(s) are consistent with agency IA architecture
601	Evaluate current or emerging technologies to consider factors such as cost, security, compatibility, or usability
603	Evaluate interface between hardware and software and operational and performance requirements of overall system

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

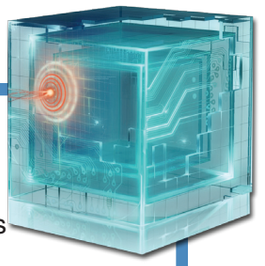


SECURELY PROVISION

ENTERPRISE ARCHITECTURE

TASK | KSA

ID	Statement
605	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents
646	Identify the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately
765	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan
797	Provide advice on project costs, design concepts, or design changes
807	Provide input on security requirements to be included in statements of work and other appropriate procurement documents
809	Provide input to the IA Certification and Accreditation (C&A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
849	Specify power supply requirements and configuration based on system performance expectations and design specifications
864	Translate proposed technical solutions into technical specifications
883	Write detailed functional specifications that document the architecture development process



SECURELY PROVISION

ENTERPRISE ARCHITECTURE

Develops the systems concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Sample Job Titles: IA Architect; Information Security Architect; Information Systems Security Engineer; Network Security Analyst; R&D Engineer; Security Architect; Security Engineer; Security Solutions Architect; Systems Engineer; Systems Security Analyst.

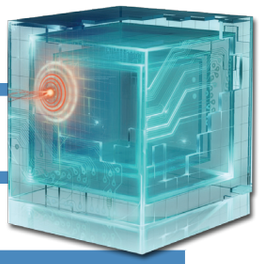
TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
18	Knowledge of circuit analysis	Computers and Electronics
21	Knowledge of computer algorithms	Mathematical Reasoning
22	Knowledge of computer networking fundamentals	Infrastructure Design
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of agency IA architecture	Information Assurance
39	Knowledge of agency confidentiality, integrity, and availability requirements	Information Assurance
40	Knowledge of agency evaluation and validation requirements	Systems Testing and Evaluation
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
43	Knowledge of embedded systems	Embedded Computers
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
46	Knowledge of fault tolerance	Information Assurance

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

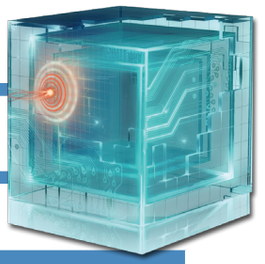
Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION — ENTERPRISE ARCHITECTURE

TASK | KSA

ID	Statement	Competency
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
53	Knowledge of IA Certification and Accreditation process	Information Assurance
54	Knowledge of IA or IA-enabled software products	Information Assurance
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
65	Knowledge of information theory	Mathematical Reasoning
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
84	Knowledge of network management principles, models, and tools	Network Management
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
90	Knowledge of operating systems	Operating Systems
92	Knowledge of Open System Interconnection model	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture

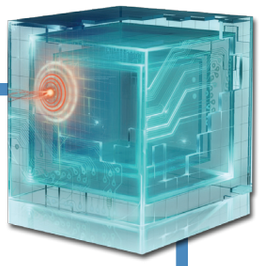


SECURELY PROVISION

ENTERPRISE ARCHITECTURE

TASK | KSA

ID	Statement	Competency
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
111	Knowledge of security system design tools, methods, and techniques	Information Systems/Network Security
119	Knowledge of software engineering	Software Engineering
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
147	Knowledge of various types of computer architectures	Information Technology Architecture
180	Skill in designing the integration of hardware and software solutions	Systems Integration
183	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment



SECURELY PROVISION

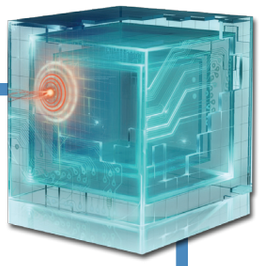
TECHNOLOGY DEMONSTRATION

Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

Sample Job Titles: - Capabilities and Development Specialist, R&D Engineer

TASK | KSA

ID	Statement
455	Conduct long-term analysis to identify network and system vulnerabilities
925	Research current technology to understand capabilities of required system or network
926	Identify and utilize reverse engineering tools to detect cyberspace vulnerabilities
927	Research and evaluate all available technologies and standards to meet customer requirements
928	Identify vulnerabilities based on target requirements
929	Develop data mining tools to analyze data collected through cyberspace systems to support analysts
934	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements



SECURELY PROVISION

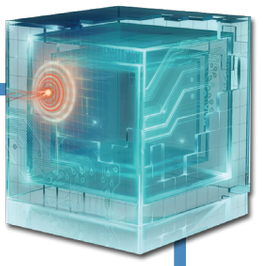
TECHNOLOGY DEMONSTRATION

Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

Sample Job Titles: - Capabilities and Development Specialist, R&D Engineer

TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
10	Knowledge of application vulnerabilities	Vulnerabilities Assessment
129	Knowledge of systems lifecycle management principles	Systems Life Cycle
321	Knowledge of products and nomenclature of major vendors (e.g., security suites; Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities	Technology Awareness



SECURELY PROVISION

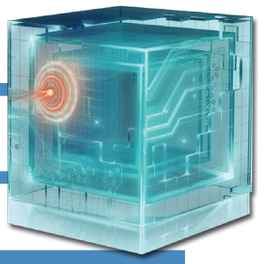
SYSTEMS REQUIREMENTS PLANNING

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Sample Job Titles: Business Analyst, Business Process Analyst, Computer Systems Analyst, Contracting Officer, Contracting Officer's Technical Representative (COTR), Human Factors Engineer, Requirements Analyst, Solutions Architect, Systems Consultant, Systems Engineer

TASK | KSA

ID	Statement
458	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications
466	Consult with customers to evaluate functional requirements
476	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions
487	Define project scope and objectives based on customer requirements
497	Design and document test procedures and quality standards
517	Develop and document requirements, capabilities, and constraints for design procedures and processes
528	Develop cost estimates for a newly acquired or modified system
560	Document a system context and preliminary system concept of operations (CONOPS)
630	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable)
669	Integrate and align information security and/or information assurance policies to ensure system analysis meets security requirements
700	Manage IT projects to ensure that developed solutions meet customer requirements
726	Oversee and make recommendations regarding configuration management
760	Perform needs analysis to determine opportunities for new and improved business process solutions

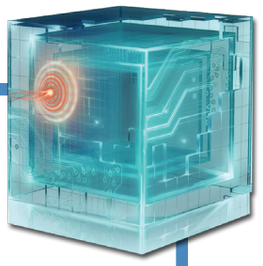


SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

TASK | KSA

ID	Statement
780	Plan system implementation to ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware)
789	Prepare use cases to justify the need for specific IT solutions
863	Translate functional requirements into design solutions



SECURELY PROVISION

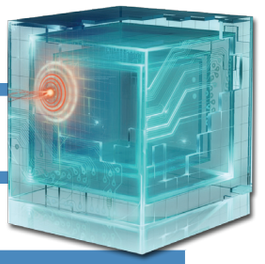
SYSTEMS REQUIREMENTS PLANNING

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Sample Job Titles: Business Analyst, Business Process Analyst, Computer Systems Analyst, Contracting Officer, Contracting Officer's Technical Representative (COTR), Human Factors Engineer, Requirements Analyst, Solutions Architect, Systems Consultant, Systems Engineer

TASK | KSA

ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
16	Knowledge of capabilities and requirements analysis	Requirements Analysis
22	Knowledge of computer networking fundamentals	Infrastructure Design
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
27	Knowledge of cryptology	Cryptography
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
53	Knowledge of IA Certification and Accreditation process	Information Assurance
55	Knowledge of IA principles	Information Assurance
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
65	Knowledge of information theory	Mathematical Reasoning
68	Knowledge of IT architectural concepts and frameworks	Information Technology Architecture
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics



SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

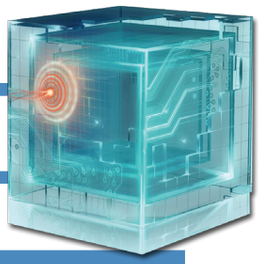
TASK | KSA

ID	Statement	Competency
79	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
84	Knowledge of network management principles, models, and tools	Network Management
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
90	Knowledge of operating systems	Operating Systems
92	Knowledge of Open System Interconnection model	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
101	Knowledge of process engineering concepts	Logical Systems Design
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design	Requirements Analysis
129	Knowledge of systems lifecycle management principles	Systems Life Cycle
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

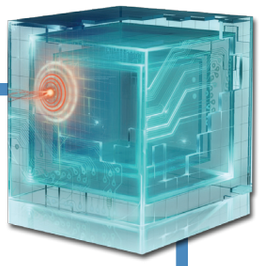


SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

TASK | KSA

ID	Statement	Competency
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating IT technologies into proposed solutions	Technology Awareness
156	Skill in applying confidentiality, integrity, and availability principles	Information Assurance
158	Skill in applying organization-specific systems analysis principles and techniques	Systems Testing and Evaluation
162	Skill in conducting capabilities and requirements analysis	Requirements Analysis
166	Skill in conducting queries and developing algorithms to analyze data structures	Database Management Systems
220	Skill in systems integration testing	Systems Testing and Evaluation
224	Skill in the use of design modeling (such as unified modeling language)	Modeling and Simulation
911	Ability to interpret and translate customer requirements into operational cyber actions	Requirements Analysis



SECURELY PROVISION

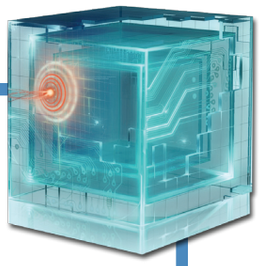
TEST AND EVALUATION

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

(Example job titles: Application Security Tester; Information Systems Security Engineer; Quality Assurance Tester; R&D Engineer; Systems Engineer; Testing and Evaluation Specialist).

TASK | KSA

ID	Statement
412	Analyze the results of software or hardware tests
508	Determine level of assurance of developed capabilities based on test results
550	Develop test plans to address specifications and requirements
694	Make recommendations based on test results
747	Perform conformance testing to assess whether a system complies with defined specifications or standards
748	Perform developmental testing on systems being concurrently developed
757	Perform joint interoperability testing on systems exchanging electronic information with systems of other services or nations
761	Perform operational testing to evaluate systems in the operational environment
773	Perform validation testing to ensure that requirements meet proposed specifications or standards and that correct specifications or standards are available
858	Test and verify hardware and support peripherals to ensure that they meet specifications and requirements by recording and analyzing test data



SECURELY PROVISION

TEST AND EVALUATION

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

(Example job titles: Application Security Tester; Information Systems Security Engineer; Quality Assurance Tester; R&D Engineer; Systems Engineer; Testing and Evaluation Specialist).

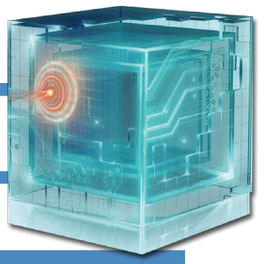
TASK | KSA

ID	Statement	Competency
38	Knowledge of agency IA architecture	Information Assurance
40	Knowledge of agency evaluation and validation requirements	Systems Testing and Evaluation
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
54	Knowledge of IA or IA-enabled software products	Information Assurance
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
83	Knowledge of network hardware devices and functions	Hardware
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
127	Knowledge of systems administration concepts	Operating Systems
144	Knowledge of the systems engineering process	Systems Life Cycle
169	Skill in conducting test events	Systems Testing and Evaluation
176	Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data)	Systems Testing and Evaluation
182	Skill in determining an appropriate level of test rigor for a given system	Systems Testing and Evaluation
190	Skill in developing operations-based testing scenarios	Systems Testing and Evaluation
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

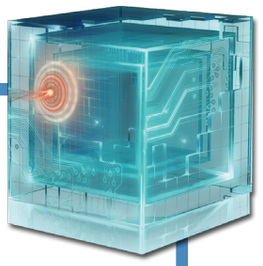


SECURELY PROVISION

TEST AND EVALUATION

TASK | KSA

ID	Statement	Competency
239	Skill in writing test plans	Systems Testing and Evaluation
904	Knowledge of interpreted and compiled computer languages	Computer Languages



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer)

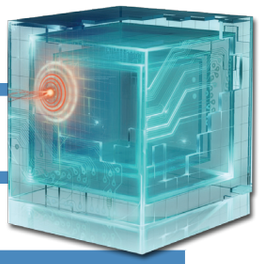
TASK | KSA

ID	Statement
399	Allocate information protection needs to systems
416	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support
419	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications
425	Assess the effectiveness of information protection measures utilized by system(s)
426	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile
431	Build, test, and modify product prototypes using working models or theoretical models
457	Conduct Privacy Impact Analysis of the application's security design for the appropriate security controls which protect the confidentiality and integrity of personally identifiable information (PII)
493	Design and develop Cross-Domain Solutions (CDS) including IA considerations for CDS
494	Design and develop IA or IA-enabled products
495	Design and develop secure interface specifications between interconnected systems
496	Design and develop system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation
500	Design hardware, operating systems, and software applications to adequately addresses IA security requirements
501	Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data
503	Design to minimum security requirements to ensure requirements are met for all systems and/or applications

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SYSTEMS DEVELOPMENT

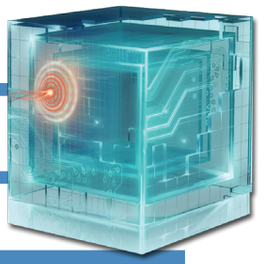
TASK | KSA

ID	Statement
516	Develop and direct system testing and validation procedures and documentation
527	Develop architectures or system components consistent with technical specifications
530	Develop detailed security design documentation for component and interface specifications to support system design and development
531	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure complete testing prior to systems entering a production environment
532	Develop IA designs for agency IS to include automated IS applications, networks, and special purpose environments with platform IT interconnectivity (e.g., weapons systems, sensors, medical technologies, or distribution systems)
533	Develop IA designs for agency IS with high integrity and availability requirements
534	Develop IA designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET)
535	Develop IA designs for systems processing Sensitive Compartmented Information (SCI)
542	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed
544	Develop security designs for new or existing system(s)
547	Develop specific IA countermeasures and risk mitigation strategies for systems and/or applications
549	Develop systems that provide adequate access controls
553	Develop/update security policies/requirements that meet the security objectives (confidentiality, integrity, and availability) of the system
562	Document application security design features, providing a functional description of their security implementation
568	Employ secure configuration management processes

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SYSTEMS DEVELOPMENT

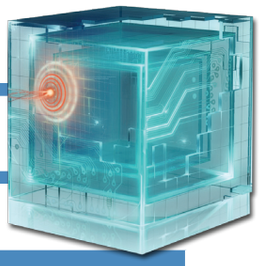
TASK | KSA

ID	Statement
575	Ensure IA design and development activities are properly documented and updated as necessary
626	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements
632	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability
648	Identify, assess, and recommend IA or IA-enabled products for use within a system and ensure recommended products are in compliance with agency evaluation and validation requirements
659	Implement security designs for new or existing system(s)
662	Incorporate IA vulnerability solutions into system designs (e.g., Information Assurance Vulnerability Alerts)
672	Integrate IA policies into system development
737	Perform an IS risk assessment and design security countermeasures to mitigate identified risks
766	Perform security reviews and identify security gaps in security architecture
770	Perform threat and vulnerability analysis whenever an application or system undergoes a major change
803	Provide guidelines for implementing developed systems to customers or installation teams
808	Provide input to implementation plans and standard operating procedures
809	Provide input to the IA Certification and Accreditation (C&A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
850	Store, retrieve, and manipulate data for analysis of system capabilities and requirements
856	Provide support to security/certification test and evaluation activities

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

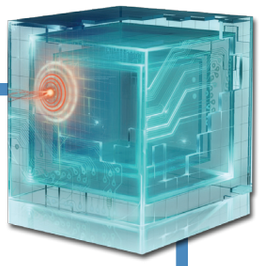
Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION — SYSTEMS DEVELOPMENT

TASK | KSA

ID	Statement
860	Trace all system security requirements to design components
874	Utilize models and simulations to analyze or predict system performance under different operating conditions
877	Verify stability, interoperability, portability, or scalability of system architecture



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer)

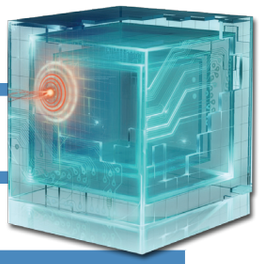
TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
18	Knowledge of circuit analysis	Computers and Electronics
21	Knowledge of computer algorithms	Mathematical Reasoning
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of agency IA architecture	Information Assurance
40	Knowledge of agency evaluation and validation requirements	Systems Testing and Evaluation
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
43	Knowledge of embedded systems	Embedded Computers
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
54	Knowledge of IA or IA-enabled software products	Information Assurance

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SYSTEMS DEVELOPMENT

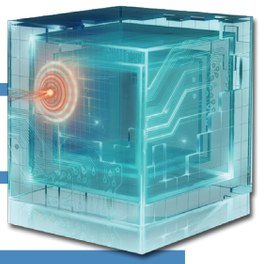
TASK | KSA

ID	Statement	Competency
64	Knowledge of Information Security Systems Engineering principles	Information Systems/Network Security
65	Knowledge of information theory	Mathematical Reasoning
70	Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption	Information Systems/Network Security
72	Knowledge of local area and wide area networking principles and concepts including bandwidth management	Infrastructure Design
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
84	Knowledge of network management principles, models, and tools	Network Management
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
90	Knowledge of operating systems	Operating Systems
92	Knowledge of Open System Interconnection model	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SYSTEMS DEVELOPMENT

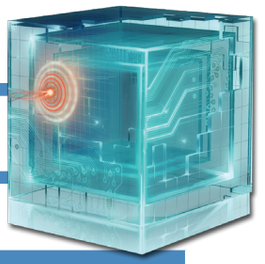
TASK | KSA

ID	Statement	Competency
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
119	Knowledge of software engineering	Software Engineering
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
147	Knowledge of various types of computer architectures	Information Technology Architecture
173	Skill in creating policies that reflect system security objectives	Information Systems Security Certification
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
179	Skill in designing security controls based on Information Assurance principles and tenets	Information Assurance
180	Skill in designing the integration of hardware and software solutions	Systems Integration
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
191	Skill in developing and applying security system access controls	Identity Management
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
199	Skill in evaluating the adequacy of security designs	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

Information Assurance Compliance | Software Engineering | Enterprise Architecture | Technology Demonstration | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SECURELY PROVISION | SYSTEMS DEVELOPMENT

TASK | KSA

ID	Statement	Competency
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

OPERATE AND MAINTAIN

Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Data Administration

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

(Example job titles: Content Staging Specialist; Data Architect; Data Manager; Data Warehouse Specialist; Database Administrator; Database Developer; Information Dissemination Manager; Systems Operations Personnel).

Information Systems Security Management

Oversees the information assurance program of an information system inside or outside the network environment; may include procurement duties (e.g., ISSO).

(Example job titles: Information Assurance Manager; Information Assurance Program Manager; Information Assurance Security Officer; Information Security Program Manager; Information Systems Security Officer (ISSO), Information Systems Security Manager).

Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

(Example job titles: Business Analyst; Business Intelligence Manager; Content Administrator; Document Steward; Freedom of Information Act Official; Information Manager; Information Owner; Information Resources Manager).

Customer Service and Technical Support

Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

(Example job titles: Computer Support Specialist; Customer Support; Help Desk Representative; Service Desk Operator; Systems Administrator; Technical Support Specialist).

Network Services

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

(Example job titles: Cabling Technician; Converged Network Engineer; Network Administrator; Network Analyst; Network Designer; Network Engineer; Network Systems and Data Communications Analyst; Telecommunications Engineer/Personnel/Specialist).

System Administration

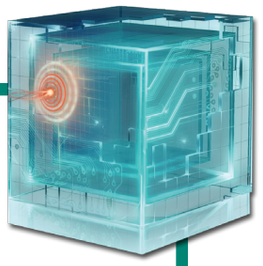
Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/ passwords/ account creation and administration.

(Example job titles: LAN Administrator; Platform Specialist; Security Administrator; Server Administrator; System Operations Personnel; Systems Administrator; Website Administrator).

Systems Security Analysis

Conducts the integration/testing, operations, and maintenance of systems security.

(Example job titles: IA Operational Engineer; Information Assurance Security Officer; Information Security Analyst/Administrator; Information Systems Security Manager; Information Systems Security Engineer; Platform Specialist; Security Administrator; Security Analyst; Security Control Assessor; Security Engineer).



OPERATE AND MAINTAIN

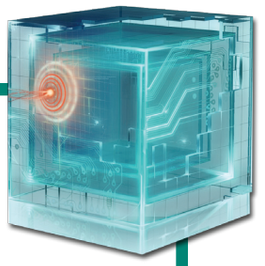
DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Sample Job Titles: Content Staging Specialist, Data Architect, Data Manager, Data Warehouse Specialist, Database Administrator, Database Developer, Information Dissemination Manager, Systems Operations Personnel

TASK | KSA

ID	Statement
400	Analyze and define data requirements and specifications
401	Analyze and plan for anticipated changes in data capacity requirements
498	Design and implement database systems
520	Develop and implement data mining and data warehousing programs
529	Develop data standards, policies, and procedures
664	Install and configure database management systems software
682	Maintain assured message delivery systems
684	Maintain database management systems software
688	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing
690	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required
702	Manage the compilation, cataloging, caching, distribution, and retrieval of data
712	Monitor and maintain databases to ensure optimal performance
740	Perform backup and recovery of databases to ensure data integrity
796	Provide a managed flow of relevant information (via web-based portals or other means) based on a mission requirements
815	Provide recommendations on new database technologies and architectures



OPERATE AND MAINTAIN

DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Sample Job Titles: Content Staging Specialist, Data Architect, Data Manager, Data Warehouse Specialist, Database Administrator, Database Developer, Information Dissemination Manager, Systems Operations Personnel

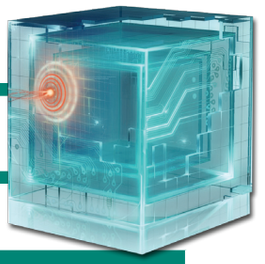
TASK | KSA

ID	Statement	Competency
28	Knowledge of data administration and data standardization policies and standards	Data Management
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
31	Knowledge of data mining and data warehousing principles	Data Management
32	Knowledge of database management systems, query languages, table relationships, and views	Database Management Systems
35	Knowledge of digital rights management	Encryption
41	Knowledge of agency LAN/WAN pathways	Infrastructure Design
44	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
79	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
90	Knowledge of operating systems	Operating Systems
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
104	Knowledge of query languages such as SQL (structured query language)	Database Management Systems
120	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
133	Knowledge of telecommunications concepts	Telecommunications
137	Knowledge of the characteristics of physical and virtual data storage media	Data Management

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

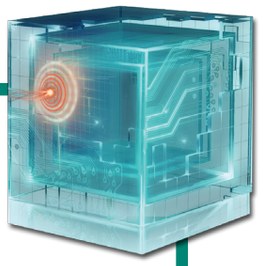


OPERATE AND MAINTAIN

DATA ADMINISTRATION

TASK | KSA

ID	Statement	Competency
152	Skill in allocating storage capacity in the design of data management systems	Database Administration
178	Skill in designing databases	Database Administration
186	Skill in developing data dictionaries	Data Management
187	Skill in developing data models	Modeling and Simulation
188	Skill in developing data repositories	Data Management
201	Skill in generating queries and reports	Database Management Systems
208	Skill in maintaining databases	Database Management Systems
213	Skill in optimizing database performance	Database Administration
910	Knowledge of database theory	Data Management



OPERATE AND MAINTAIN

INFORMATION SYSTEMS SECURITY MANAGEMENT

Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).

Sample Job Titles: Information Assurance Manager, Information Assurance Program Manager, Information Assurance Security Officer, Information Security Program Manager, Information Systems Security Manager, Information Systems Security Officer (ISSO)

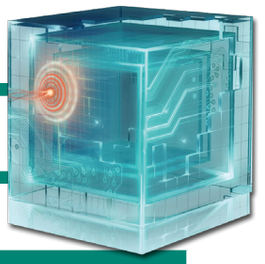
TASK | KSA

ID	Statement
397	Advise the DAA of changes affecting the enterprise's IA posture
405	Analyze identified security strategies and select the best approach or practice for the enterprise
415	Analyze, develop, approve, and issue enterprise IA policies
440	Collect and maintain data needed to meet system IA reporting
523	Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow IT and IA policies and procedures
536	Develop IT security requirements specific to an IT acquisition for inclusion in procurement documents
540	Develop procedures to ensure system users are aware of their IA responsibilities before granting access to agency's information systems
545	Develop security requirements for hardware, software, and services acquisitions
581	Ensure that compliance monitoring occurs, and review results of across the network environment
583	Ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate IT security configuration guidelines, policies, and procedures
584	Ensure that IA inspections, tests, and reviews are coordinated for the network environment
585	Ensure that IA requirements are integrated into the Continuity of Operations Plan (COOP) for that system or agency
586	Ensure that IA security requirements are appropriately identified in computer environment operation procedures
589	Ensure that IT information security recovery processes are monitored and that IA features and procedures are properly restored

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

INFORMATION SYSTEMS SECURITY MANAGEMENT

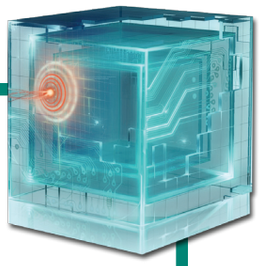
TASK | KSA

ID	Statement
590	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with agency- level IA architecture
591	Ensure that security related provisions of the system acquisition documents meet all identified security needs
592	Ensure that system security configuration guidelines are followed
598	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed
610	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents
625	Help prepare IA certification and accreditation documentation
719	Monitor system performance and review for compliance with IA security and privacy requirements within the computer environment
731	Participate in an information security risk assessment during the Certification and Accreditation process
733	Participate in the development or modification of the computer environment IA security program plans and requirements
790	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations
816	Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents
824	Recognize a possible security violation and take appropriate action to report the incident, as required
828	Recommend resource allocations required to securely operate and maintain an organization's IA requirements
852	Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered
853	Support and administer data retention and recovery within the computing environment
869	Use federal and organization-specific published documents to manage operations of their computing environment system(s)

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

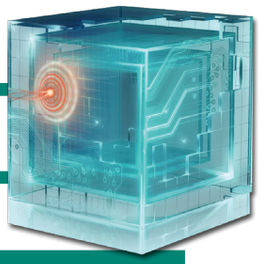
INFORMATION SYSTEMS SECURITY MANAGEMENT

Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).

Sample Job Titles: Information Assurance Manager, Information Assurance Program Manager, Information Assurance Security Officer, Information Security Program Manager, Information Systems Security Manager, Information Systems Security Officer (ISSO)

TASK | KSA

ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
37	Knowledge of disaster recovery continuity of operations plans	Incident Management
55	Knowledge of IA principles	Information Assurance
58	Knowledge of identified vulnerabilities, alerts, and bulletins (IAVA, IAVB)	Information Systems/Network Security
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
69	Knowledge of IT security certification and accreditation requirements	Information Systems Security Certification
71	Knowledge of IT security principles and regulations	Information Systems Security Certification
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
77	Knowledge of methods for evaluating, implementing, and disseminating IT security tools and procedures	Information Systems/Network Security
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
86	Knowledge of network systems management methods including end-to-end systems performance monitoring	Network Management



OPERATE AND MAINTAIN

INFORMATION SYSTEMS SECURITY MANAGEMENT

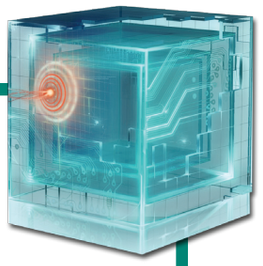
TASK | KSA

ID	Statement	Competency
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
97	Knowledge of pertinent government laws and information technology regulations	Legal, Government and Jurisprudence
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems
121	Knowledge of structured analysis principles and methods	Logical Systems Design
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design	Requirements Analysis
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
129	Knowledge of systems lifecycle management principles	Systems Life Cycle
143	Knowledge of the organization's enterprise IT goals and objectives	Enterprise Architecture
183	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system	Information Technology Performance Assessment
325	Knowledge of secure acquisitions (COTR, procurement, supply chain management).	Contracting/Procurement

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

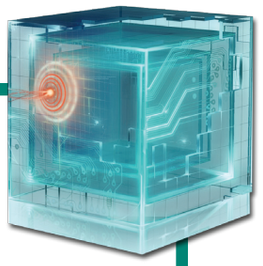
KNOWLEDGE MANAGEMENT

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Sample Job Titles: Business Analyst, Business Intelligence Manager, Content Administrator, Document Steward, Freedom of Information Act Official, Information Manager, Information Owner, Information Resources Manager

TASK | KSA

ID	Statement
394	Administer the indexing/cataloguing, storage, and access of organizational documents
464	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users
505	Design, build, implement, and maintain a knowledge management system that provides end-users access to the organization's intellectual capital
513	Develop an understanding of the needs and requirements of information end-users'
519	Develop and implement control procedures into the testing and development of core IT-based knowledge management systems
721	Monitor the usage of knowledge management assets
777	Plan and manage the delivery of knowledge management projects
794	Promote knowledge sharing through an organization's operational processes and systems by strengthening links between knowledge sharing and IT systems
814	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information



OPERATE AND MAINTAIN

KNOWLEDGE MANAGEMENT

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Sample Job Titles: Business Analyst, Business Intelligence Manager, Content Administrator, Document Steward, Freedom of Information Act Official, Information Manager, Information Owner, Information Resources Manager

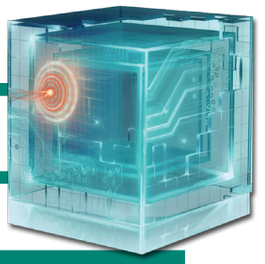
TASK | KSA

ID	Statement	Competency
5	Ability to match the appropriate knowledge repository technology for a given application or environment	Knowledge Management
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
56	Knowledge of IA principles and methods that apply to software development	Information Assurance
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
91	Knowledge of networking architecture	Infrastructure Design
134	Knowledge of the capabilities and functionality associated with various content creation technologies (wikis, social networking, blogs, etc.)	Technology Awareness
135	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines, etc.)	Data Management
136	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint, etc.)	Technology Awareness
163	Skill in conducting information searches	Computer Skills
164	Skill in conducting knowledge mapping (map of knowledge repositories)	Knowledge Management
189	Skill in developing expert directories that allow end-users to easily reach Subject Matter Experts	Data Management
223	Skill in the measuring and reporting of intellectual capital	Knowledge Management

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

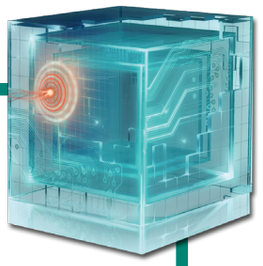


OPERATE AND MAINTAIN

KNOWLEDGE MANAGEMENT

TASK | KSA

ID	Statement	Competency
230	Skill in using knowledge management technologies	Knowledge Management
907	Skill in data mining techniques	Data Management
910	Knowledge of database theory	Data Management



OPERATE AND MAINTAIN

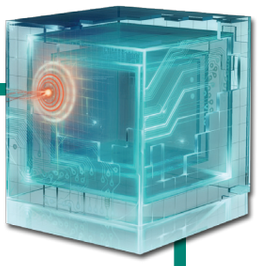
CUSTOMER SERVICE AND TECHNICAL SUPPORT

Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Sample Job Titles: Computer Support Specialist, Customer Support, Help Desk Representative, Service Desk Operator, Systems Administrator, Technical Support Specialist

TASK | KSA

ID	Statement
406	Analyze incident data for emerging trends
428	Assist in the execution of disaster recovery continuity of operations plans
514	Develop and deliver technical training to educate others or meet customer needs
554	Diagnose and resolve customer reported system incidents
639	Identify end-user requirements for software and hardware
665	Install and configure hardware, software, and peripheral equipment for system users
689	Maintain incident tracking and solution database
695	Manage accounts, network rights, and access to systems and equipment
698	Manage inventory of IT resources
714	Monitor client-level computer system performance
813	Provide recommendations for possible improvements and upgrades
830	Report emerging trend findings
859	Test computer system performance
866	Troubleshoot system hardware and software



OPERATE AND MAINTAIN

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Sample Job Titles: Computer Support Specialist, Customer Support, Help Desk Representative, Service Desk Operator, Systems Administrator, Technical Support Specialist

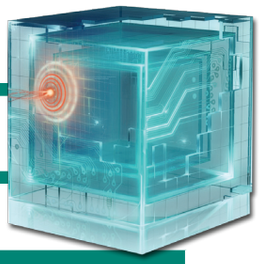
TASK | KSA

ID	Statement	Competency
7	Knowledge of "knowledge base" capabilities in identifying the solutions to less common and more complex system problems	Knowledge Management
33	Knowledge of database procedures used for documenting and querying reported incidents	Incident Management
37	Knowledge of disaster recovery continuity of operations plans	Incident Management
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
127	Knowledge of systems administration concepts	Operating Systems
142	Knowledge of the operations and processes for diagnosing common or recurring system problems	Systems Life Cycle
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly	Systems Life Cycle
165	Skill in conducting open source research for troubleshooting novel client-level problems	Knowledge Management
204	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation	Systems Life Cycle
221	Skill in testing and configuring network workstations and peripherals	Network Management

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

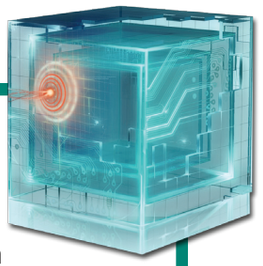


OPERATE AND MAINTAIN

CUSTOMER SERVICE AND TECHNICAL SUPPORT

TASK | KSA

ID	Statement	Competency
222	Skill in the basic operation of computers	Computer Skills
235	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system	Computers and Electronics



OPERATE AND MAINTAIN

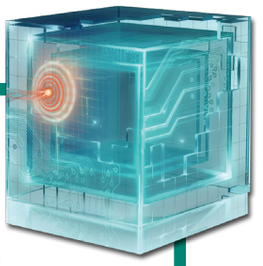
NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Sample Job Titles: Cabling Technician, Converged Network Engineer, Network Administrator, Network Analyst, Network Designer, Network Engineer, Network Systems and Data Communications Analyst, Telecommunications Engineer/Personnel/Specialist

TASK | KSA

ID	Statement
462	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling, etc.)
522	Develop and implement network backup and recovery procedures
555	Diagnose network connectivity problem
617	Expand or modify network infrastructure to serve new purposes or improve work flow
656	Implement new system design procedures, test procedures, and quality standards
666	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware, etc.)
667	Install or replace network hubs, routers, and switches
673	Integrate new systems into existing network architecture
718	Monitor network capacity and performance
736	Patch network vulnerabilities to ensure information is safeguarded against outside parties
802	Provide feedback on network requirements, including network architecture and infrastructure
829	Repair network connectivity problems
857	Test and maintain network infrastructure including software and hardware devices



OPERATE AND MAINTAIN

NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Sample Job Titles: Cabling Technician, Converged Network Engineer, Network Administrator, Network Analyst, Network Designer, Network Engineer, Network Systems and Data Communications Analyst, Telecommunications Engineer/Personnel/Specialist

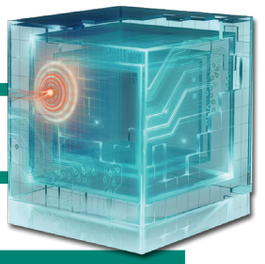
TASK | KSA

ID	Statement	Competency
12	Knowledge of basic communication methods, principles, and concepts (e.g., crypto, dual hubs, time multiplexers, etc.) that support the network infrastructure	Infrastructure Design
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware	Hardware
55	Knowledge of IA principles	Information Assurance
70	Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption	Information Systems/Network Security
72	Knowledge of local area and wide area networking principles and concepts including bandwidth management	Infrastructure Design
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
86	Knowledge of network systems management methods including end-to-end systems performance monitoring	Network Management
106	Knowledge of remote access technology concepts	Information Technology Architecture
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN | NETWORK SERVICES

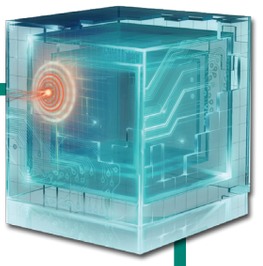
TASK | KSA

ID	Statement	Competency
127	Knowledge of systems administration concepts	Operating Systems
133	Knowledge of telecommunications concepts	Telecommunications
154	Skill in analyzing network traffic capacity and performance characteristics	Capacity Management
193	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans	Information Assurance
198	Skill in establishing a routing schema	Infrastructure Design
205	Skill in implementing, maintaining, and improving established security practices	Information Systems/Network Security
207	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches	Infrastructure Design
231	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)	Network Management
891	Skill in configuring and utilizing hardware-based computer protection tools (e.g., hardware firewalls, servers, routers)	Configuration Management
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)	Configuration Management
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Information Assurance
900	Knowledge of web filtering technologies	Web Technology
901	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts)	Network Management
902	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)	Network Management
903	Knowledge of wireless fidelity (WIFI)	Network Management

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Sample Job Titles: LAN Administrator, Platform Specialist, Security Administrator, Server Administrator, System Operations Personnel, Systems Administrator, Website Administrator

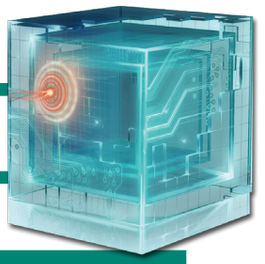
TASK | KSA

ID	Statement
434	Check server availability, functionality, integrity, and efficiency
452	Conduct functional and connectivity testing to ensure continuing operability
456	Conduct periodic server maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing
499	Design group policies and access control lists to ensure compatibility with agency standards
518	Develop and document systems administration standard operating procedures
521	Develop and implement local network usage policies and procedures
668	Install server fixes, updates, and enhancements
683	Maintain baseline system security per DISA Security Technical Implementation Guides (STIGs)
695	Manage accounts, network rights, and access to systems and equipment
701	Manage server resources including performance, capacity, availability, serviceability, and recoverability
713	Monitor and maintain server configuration
728	Oversee installation, implementation, configuration, and support of network components
763	Perform repairs on faulty server hardware
776	Plan and coordinate the installation of new or modified hardware, operating systems, and other baseline software
781	Plan, execute, and verify data redundancy and system recovery procedures

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

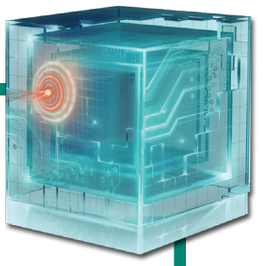


OPERATE AND MAINTAIN

SYSTEM ADMINISTRATION

TASK | KSA

ID	Statement
811	Provide ongoing optimization and problem solving support
835	Resolve hardware/software interface and interoperability problems



OPERATE AND MAINTAIN

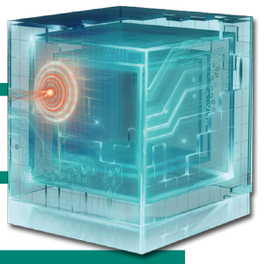
SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Sample Job Titles: LAN Administrator, Platform Specialist, Security Administrator, Server Administrator, System Operations Personnel, Systems Administrator, Website Administrator

TASK | KSA

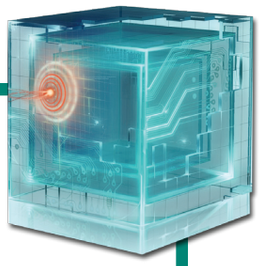
ID	Statement	Competency
70	Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption	Information Systems/Network Security
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
89	Knowledge of new technological developments in server administration	Technology Awareness
96	Knowledge of performance tuning tools and techniques	Information Technology Performance Assessment
99	Knowledge of principles and methods for integrating server components	Systems Integration
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques	Computer Forensics
127	Knowledge of systems administration concepts	Operating Systems
141	Knowledge of the enterprise IT architecture	Information Technology Architecture
167	Skill in conducting server planning, management, and maintenance	Network Management
170	Skill in configuring and optimizing software	Software Engineering



OPERATE AND MAINTAIN — SYSTEM ADMINISTRATION

TASK | KSA

ID	Statement	Competency
171	Skill in correcting physical and technical problems which impact server performance	Network Management
194	Skill in diagnosing connectivity problems	Network Management
195	Skill in diagnosing failed servers	Network Management
202	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems	Information Technology Performance Assessment
206	Skill in installing computer and server upgrades	Systems Life Cycle
209	Skill in maintaining directory services	Identity Management
211	Skill in monitoring and optimizing server performance	Information Technology Performance Assessment
216	Skill in recovering failed servers	Incident Management
891	Skill in configuring and utilizing hardware-based computer protection tools (e.g., hardware firewalls, servers, routers)	Configuration Management
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)	Configuration Management



OPERATE AND MAINTAIN

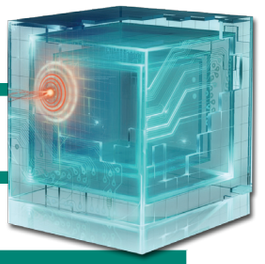
SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

Sample Job Titles: IA Operational Engineer, Information Assurance Security Officer, Information Security Analyst/Administrator, Information Systems Security Engineer, Information Systems Security Manager, Platform Specialist, Security Administrator, Security Analyst, Security Control Assessor, Security Engineer

TASK | KSA

ID	Statement
419	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications
420	Apply security policies to meet security objectives of the system
421	Apply service-oriented security architecture principles to meet agency confidentiality, integrity, and availability requirements
525	Develop and test system fail-over or system operations transfer to an alternate site based on system availability requirements
559	Discover organizational trends with regard to the security posture of systems
571	Ensure all operations and maintenance activities are properly documented and updated as necessary
572	Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment
576	Ensure IA-enabled products or other compensating security control technologies reduce identified risk to an acceptable level
593	Establish adequate access controls based on principles of least privilege and need-to-know
616	Exercise the system Disaster Recovery and Continuity Of Operations
651	Implement and manage an Information Assurance Program
652	Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines
653	Implement approaches to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed

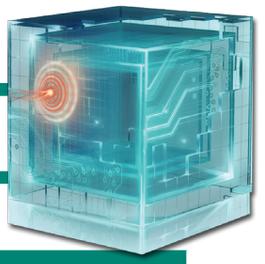


OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

TASK | KSA

ID	Statement
657	Implement security controls that ensure users can only perform actions for which they have authorization, based on principles of least privilege and separation of duty
658	Implement security designs and properly mitigate identified threats
660	Implement specific IA countermeasures for systems and/or applications
661	Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation
670	Integrate and/or implement Cross-Domain Solutions (CDS) in a secure environment
671	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system
708	Mitigate/correct security deficiencies identified during security/certification testing or identify risk acceptance for the appropriate DAA or authorized representative
717	Monitor information protection assurance mechanisms related to system implementation and testing practices
729	Oversee minimum security requirements are in place for all applications
754	Perform IA testing of developed applications and/or systems
767	Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy
782	Plan, and recommend modifications or adjustments based on exercise results or system environment; ensure Recovery and Continuity plans are executable in the system operational environment
795	Properly document all implementation,operations, and maintenance activities and update as necessary
806	Provide information assurance guidance to leadership

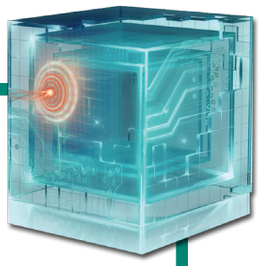


OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

TASK | KSA

ID	Statement
809	Provide input to the IA Certification and Accreditation (C&A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
876	Verify and update security documentation reflecting the application/system security design features
880	Work with others to resolve computer security incidents and vulnerability compliance



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

Sample Job Titles: IA Operational Engineer, Information Assurance Security Officer, Information Security Analyst/Administrator, Information Systems Security Engineer, Information Systems Security Manager, Platform Specialist, Security Administrator, Security Analyst, Security Control Assessor, Security Engineer

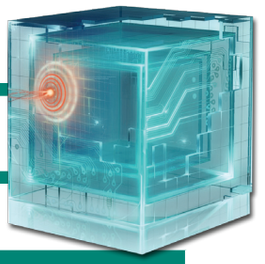
TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
18	Knowledge of circuit analysis	Computers and Electronics
21	Knowledge of computer algorithms	Mathematical Reasoning
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
43	Knowledge of embedded systems	Embedded Computers
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
65	Knowledge of information theory	Mathematical Reasoning

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

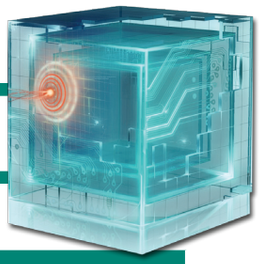
TASK | KSA

ID	Statement	Competency
70	Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption	Information Systems/Network Security
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
84	Knowledge of network management principles, models, and tools	Network Management
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
90	Knowledge of operating systems	Operating Systems
92	Knowledge of Open System Interconnection model	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
111	Knowledge of security system design tools, methods, and techniques	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE

Data Administration | Information Systems Security Management | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

TASK | KSA

ID	Statement	Competency
119	Knowledge of software engineering	Software Engineering
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
147	Knowledge of various types of computer architectures	Information Technology Architecture
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
180	Skill in designing the integration of hardware and software solutions	Systems Integration
183	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
191	Skill in developing and applying security system access controls	Identity Management
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

PROTECT AND DEFEND

Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

Computer Network Defense

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

(Example job titles: CND Analyst (Cryptologic); Cyber Security Intelligence Analyst; Focused Operations Analyst; Incident Analyst; Network Defense Technician; Security Analyst; Security Operator; Sensor Analyst)

Incident Response

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

(Example job titles: Computer Crime Investigator; Incident Handler; Incident Responder; Intrusion Analyst)

Computer Network Defense Infrastructure Support

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

(Example job titles: IDS Administrator; IDS Engineer; IDS Technician; Information Systems Security Engineer; Network Administrator; Network Analyst; Network Security Engineer/Specialist; Security Analyst; Security Engineer; Security Specialist)

Security Program Management

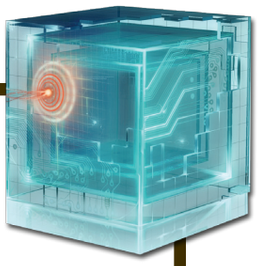
Manages relevant security (e.g., information security) implications within the organization, specific program,or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

(Example job titles: Chief Information Security Officer (CISO);Common Control Provider; Enterprise Security Officer; FacilitySecurity Officer; I Director; Principal Security Architect; Risk Executive; Senior Agency Information Security Officer)

Vulnerability Assessment and Management

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

(Example job titles: Blue Team Technician; Close Access Technician; CND Auditor; Compliance Manager; Ethical Hacker; Governance Manager; Internal Enterprise Auditor; Penetration Tester; Red Team Technician; Reverse Engineer; Risk/Vulnerability Analyst/Manager)



PROTECT AND DEFEND

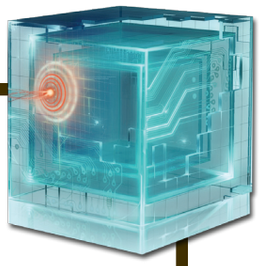
COMPUTER NETWORK DEFENSE

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Sample Job Titles: CND Analyst (Cryptologic), Cyber Security Intelligence Analyst, Focused Operations Analyst, Incident Analyst, Network Defense Technician, Security Analyst, Security Operator, Sensor Analyst

TASK | KSA

ID	Statement
427	Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
472	Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts
716	Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise
723	Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event's history, status, and potential impact for further action
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
800	Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Sample Job Titles: CND Analyst (Cryptologic), Cyber Security Intelligence Analyst, Focused Operations Analyst, Incident Analyst, Network Defense Technician, Security Analyst, Security Operator, Sensor Analyst

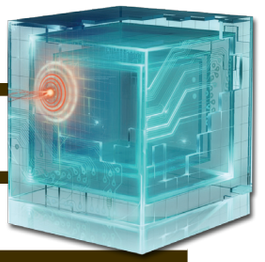
TASK | KSA

ID	Statement	Competency
8	Knowledge of access authentication methods	Identity Management
13	Knowledge of basic system, network, and operating system hardening techniques	Information Systems/Network Security
19	Knowledge of Computer Network Defense tools, including open source tools, and their capabilities	Computer Network Defense
26	Knowledge of cross-domain guards	Information Assurance
27	Knowledge of cryptology	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
66	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies	Computer Network Defense
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



PROTECT AND DEFEND | COMPUTER NETWORK DEFENSE

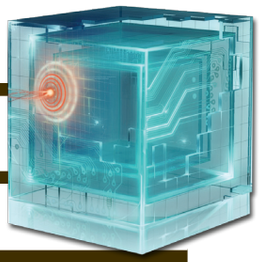
TASK | KSA

ID	Statement	Competency
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
87	Knowledge of network traffic analysis methods	Vulnerabilities Assessment
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
92	Knowledge of Open System Interconnection model	Infrastructure Design
95	Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)	Vulnerabilities Assessment
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
110	Knowledge of security management	Information Assurance
115	Knowledge of signature development	Computer Network Defense
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
138	Knowledge of the Computer Network Defense Service Provider reporting structure and processes within one's own agency or organization	Information Systems/Network Security
148	Knowledge of VPN security	Encryption
150	Knowledge of what constitutes a "threat" to a network	Information Systems/Network Security
175	Skill in developing and deploying signatures	Information Systems/Network Security
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
212	Skill in network mapping and recreating network topologies	Infrastructure Design

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

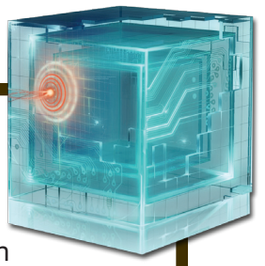
Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



PROTECT AND DEFEND | COMPUTER NETWORK DEFENSE

TASK | KSA

ID	Statement	Competency
214	Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)	Vulnerabilities Assessment
229	Skill in using incident handling methodologies	Incident Management
233	Skill in using protocol analyzers	Vulnerabilities Assessment
234	Skill in using sub-netting tools	Infrastructure Design
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup, etc.)	Infrastructure Design
278	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN, etc.)	Telecommunications
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip, etc.)	Operating Systems
342	Knowledge of unix command line (e.g., mkdir, mv, ls, passwd, grep, etc.)	Computer Languages
347	Knowledge of windows command line (e.g., ipconfig, netstat, dir, nbtstat, etc.)	Operating Systems
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
915	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection	Information Systems/Network Security
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment



PROTECT AND DEFEND

INCIDENT RESPONSE

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Sample Job Titles: Computer Crime Investigator, Incident Handler, Incident Responder, Intrusion Analyst

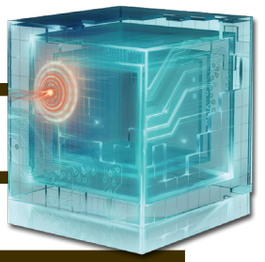
TASK | KSA

ID	Statement
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
474	Coordinate with intelligence analysts to correlate threat assessment data
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
686	Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission
716	Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
741	Perform command and control functions in response to incidents
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
745	Perform Computer Network Defense trend analysis and reporting
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

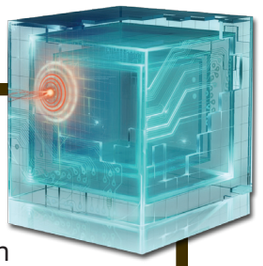
Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



PROTECT AND DEFEND | INCIDENT RESPONSE

TASK | KSA

ID	Statement
762	Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution
882	Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies



PROTECT AND DEFEND

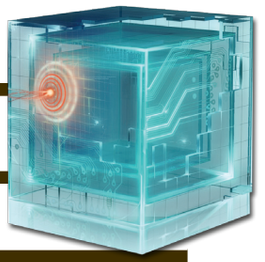
INCIDENT RESPONSE

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Sample Job Titles: Computer Crime Investigator, Incident Handler, Incident Responder, Intrusion Analyst

TASK | KSA

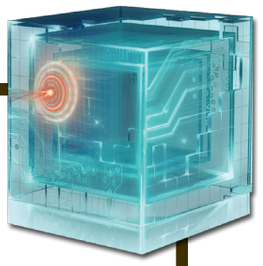
ID	Statement	Competency
13	Knowledge of basic system, network, and operating system hardening techniques	Information Systems/Network Security
24	Knowledge of concepts and practices of processing digital information	Data Management
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
36	Knowledge of Defense Information Systems Agency Security Technical Implementation Guides (STIGs)	Information Systems/Network Security
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
50	Knowledge of how network services and protocols interact to provide network communications	Infrastructure Design
60	Knowledge of incident categories, incident responses, and timelines for responses	Incident Management
61	Knowledge of incident response and handling methodologies	Incident Management
66	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies	Computer Network Defense
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design



PROTECT AND DEFEND | INCIDENT RESPONSE

TASK | KSA

ID	Statement	Competency
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
87	Knowledge of network traffic analysis methods	Vulnerabilities Assessment
92	Knowledge of Open System Interconnection model	Infrastructure Design
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
150	Knowledge of what constitutes a “threat” to a network	Information Systems/Network Security
153	Skill in analyzing malware	Vulnerabilities Assessment
217	Skill in seizing and preserving digital evidence	Computer Forensics
229	Skill in using incident handling methodologies	Incident Management
893	Skill in securing network communications	Information Assurance
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
896	Skill in protecting a network against malware	Information Assurance
897	Skill in performing damage assessments	Information Assurance
923	Knowledge of security event correlation tools	Information Systems/Network Security



PROTECT AND DEFEND

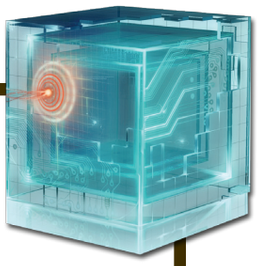
COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

Sample Job Titles: IDS Administrator, IDS Engineer, IDS Technician, Information Systems Security Engineer, Network Administrator, Network Analyst, Network Security Engineer, Network Security Specialist, Security Analyst, Security Engineer, Security Specialist, Systems Security Engineer

TASK | KSA

ID	Statement
393	Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service provider managed platforms
471	Coordinate with Computer Network Defense Analysts to manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized Computer Network Defense applications
481	Create, edit, and manage changes to network access control lists on specialized Computer Network Defense systems (e.g., firewalls and intrusion prevention systems)
643	Identify potential conflicts with implementation of any Computer Network Defense tools within the Computer Network Defense service provider area of responsibility (e.g., tool/signature testing and optimization)
654	Implement C&A requirements for specialized Computer Network Defense systems within the enterprise, and document and maintain records for them
769	Perform system administration on specialized Computer Network Defense applications and systems (e.g., anti-virus, Audit/Remediation, or VPN devices) to include installation, configuration, maintenance, and backup/restore
822	Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

Sample Job Titles: IDS Administrator, IDS Engineer, IDS Technician, Information Systems Security Engineer, Network Administrator, Network Analyst, Network Security Engineer, Network Security Specialist, Security Analyst, Security Engineer, Security Specialist, Systems Security Engineer

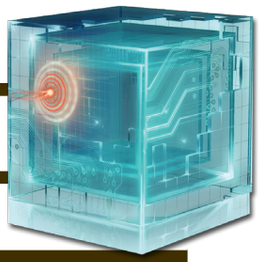
TASK | KSA

ID	Statement	Competency
13	Knowledge of basic system, network, and operating system hardening techniques	Information Systems/Network Security
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
59	Knowledge of IDS tools and applications	Computer Network Defense
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
87	Knowledge of network traffic analysis methods	Vulnerabilities Assessment
92	Knowledge of Open System Interconnection model	Infrastructure Design
93	Knowledge of packet-level analysis	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

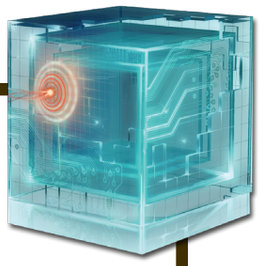


PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT

TASK | KSA

ID	Statement	Competency
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
146	Knowledge of the types of IDS hardware and software	Computer Network Defense
150	Knowledge of what constitutes a “threat” to a network	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
175	Skill in developing and deploying signatures	Information Systems/Network Security
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
219	Skill in system administration for Unix/Linux operating systems	Operating Systems
227	Skill in tuning sensors	Computer Network Defense
229	Skill in using incident handling methodologies	Incident Management
237	Skill in using VPN devices and encryption	Encryption
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Information Assurance
900	Knowledge of web filtering technologies	Web Technology



PROTECT AND DEFEND

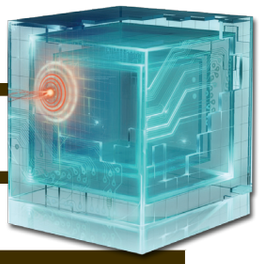
SECURITY PROGRAM MANAGEMENT

Manages relevant security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

Sample Job Titles: Chief Information Security Officer (CISO), Common Control Provider, Cyber Security Officer, Enterprise Security Officer, Facility Security Officer, IT Director, Principal Security Architect, Risk Executive, Security Domain Specialist, Senior Agency Information Security Officer (SAIS)

TASK | KSA

ID	Statement
391	Acquire and manage the necessary resources, including financial resources, to support IT security goals and objectives and reduce overall organizational risk
392	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program
395	Advise CIO on risk levels and security posture
396	Advise the CIO on cost/benefit analysis of information security programs, policies, processes, and systems
445	Communicate the value of IT security within the organization
468	Continuously validate the organization against additional mandates, as developed, to ensure full compliance
473	"Coordinate with information security, physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization"
475	Coordinate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance
574	Evaluate, monitor, and ensure compliance with data security policies and relevant legal and regulatory requirements
578	Ensure security improvement actions are implemented as required.
582	Ensure that data classification and data management policies and guidance are issue-updated
596	"Establish overall enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy"
600	Evaluate cost benefit, economic, and risk analysis in decision making process



PROTECT AND DEFEND | SECURITY PROGRAM MANAGEMENT

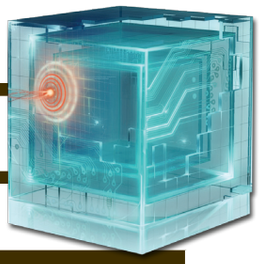
TASK | KSA

ID	Statement
604	Evaluate proposals to determine if proposed security solutions effectively address enterprise requirements, as detailed in solicitation documents
608	Evaluate the effectiveness of procurement function in addressing information security requirements through procurement activities, and recommend improvements
610	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents
628	Identify alternative functional IA security strategies to address organizational IT security concerns
631	Identify and prioritize critical business functions in collaboration with organizational stakeholders
640	Identify IT security program implications of new technologies or technology upgrades
650	Implement and enforce Computer Network Defense policies and procedures reflecting applicable laws, policies, procedures, and regulations (such as U.S. Codes 10 and 50)
674	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information
676	Interpret and/or approve security requirements relative to the capabilities of new information technologies
677	Interpret patterns of non compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's IA program
679	Lead and align IT security priorities with the organization's mission and vision
680	Lead and oversee information security budget, staffing, and contracting
705	Manage the monitoring of external Computer Network Defense data sources to maintain enterprise situational awareness
706	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs, etc.) for the enterprise constituency

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

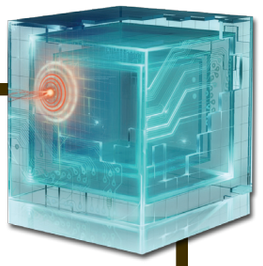


PROTECT AND DEFEND

SECURITY PROGRAM MANAGEMENT

TASK | KSA

ID	Statement
707	Manage threat or target analysis of Computer Network Defense information and production of threat information within the enterprise
711	Monitor and evaluate the effectiveness of the enterprise's IA security safeguards to ensure they provide the intended level of protection
730	Oversee the information security training and awareness program
801	Provide enterprise IA guidance for development of the Continuity of Operations Plans
810	Provide leadership and direction to IT personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities
818	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters
844	Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enterprise
848	Specify policy and coordinate review and approval
862	Track compliance of audit findings (Computer Network Defense findings), incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken



PROTECT AND DEFEND

SECURITY PROGRAM MANAGEMENT

Manages relevant security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

Sample Job Titles: Chief Information Security Officer (CISO), Common Control Provider, Cyber Security Officer, Enterprise Security Officer, Facility Security Officer, IT Director, Principal Security Architect, Risk Executive, Security Domain Specialist, Senior Agency Information Security Officer (SAIS)

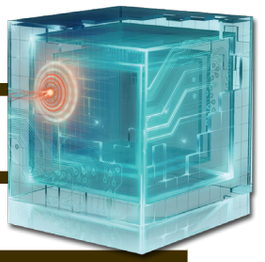
TASK | KSA

ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
37	Knowledge of disaster recovery continuity of operations plans	Incident Management
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
55	Knowledge of IA principles	Information Assurance
61	Knowledge of incident response and handling methodologies	Incident Management
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
66	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies	Computer Network Defense
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
84	Knowledge of network management principles, models, and tools	Network Management

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



PROTECT AND DEFEND | SECURITY PROGRAM MANAGEMENT

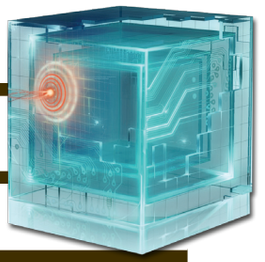
TASK | KSA

ID	Statement	Competency
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
86	Knowledge of network systems management methods including end-to-end systems performance monitoring	Network Management
87	Knowledge of network traffic analysis methods	Vulnerabilities Assessment
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
92	Knowledge of Open System Interconnection model	Infrastructure Design
95	Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)	Vulnerabilities Assessment
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
107	Knowledge of resource management principles and techniques	Project Management
110	Knowledge of security management	Information Assurance
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design	Requirements Analysis
129	Knowledge of systems lifecycle management principles	Systems Life Cycle

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

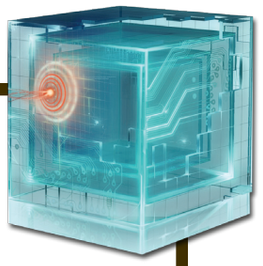


PROTECT AND DEFEND

SECURITY PROGRAM MANAGEMENT

TASK | KSA

ID	Statement	Competency
132	Knowledge of technology integration processes	Systems Integration
150	Knowledge of what constitutes a “threat” to a network	Information Systems/Network Security
299	Knowledge of information security program management and project management principles and techniques	Project Management
916	Skill in deconflicting cyber operations and activities	Political Savvy
919	Ability to promote awareness of security issues among management and ensure sound security principles are reflected in organizations' visions and goals	Political Savvy



PROTECT AND DEFEND

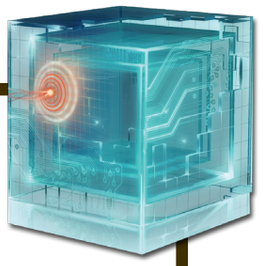
VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Sample Job Titles: Blue Team Technician, Close Access Technician, CND Auditor, Compliance Manager, Ethical Hacker, Governance Manager, Internal Enterprise Auditor, Penetration Tester, Red Team Technician, Reverse Engineer, Risk/Vulnerability Analyst, Vulnerability Manager

TASK | KSA

ID	Statement
411	Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives
448	Conduct authorized penetration testing of enterprise network assets
685	Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/ hardware) to support Computer Network Defense audit missions
692	Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing
744	Perform Computer Network Defense risk assessments within the enterprise
746	Perform Computer Network Defense vulnerability assessments within the enterprise
784	Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/ solutions



PROTECT AND DEFEND

VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Sample Job Titles: Blue Team Technician, Close Access Technician, CND Auditor, Compliance Manager, Ethical Hacker, Governance Manager, Internal Enterprise Auditor, Penetration Tester, Red Team Technician, Reverse Engineer, Risk/Vulnerability Analyst, Vulnerability Manager

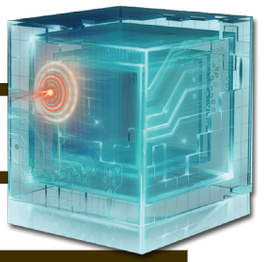
TASK | KSA

ID	Statement	Competency
3	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
10	Knowledge of application vulnerabilities	Vulnerabilities Assessment
13	Knowledge of basic system, network, and operating system hardening techniques	Information Systems/Network Security
17	Knowledge of certified ethical hacking principles and techniques	Vulnerabilities Assessment
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)	Information Assurance
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
85	Knowledge of network security architecture, including the application of Defense-In-Depth principles	Information Systems/Network Security
92	Knowledge of Open System Interconnection model	Infrastructure Design
95	Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense | Incident Response | Computer Network Defense Infrastructure Support | Security Program Management | Vulnerability Assessment and Management

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



PROTECT AND DEFEND

VULNERABILITY ASSESSMENT AND MANAGEMENT

TASK | KSA

ID	Statement	Competency
102	Knowledge of programming language structures and logic	Computer Languages
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
150	Knowledge of what constitutes a “threat” to a network	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
210	Skill in mimicking threat behaviors	Computer Network Defense
214	Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)	Vulnerabilities Assessment
225	Skill in the use of penetration testing tools and techniques	Vulnerabilities Assessment
226	Skill in the use of social engineering techniques	Human Factors
238	Skill in writing code in a modern programming language (e.g., Java, C++)	Computer Languages
897	Skill in performing damage assessments	Information Assurance
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

INVESTIGATE

Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

Investigation

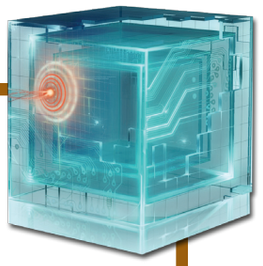
Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

(Example job titles: Computer Crime Investigator; Special Agent)

Digital Forensics

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

(Example job titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Forensic Analyst (Cryptologic); Forensic Technician; Network Forensic Examiner).



INVESTIGATE

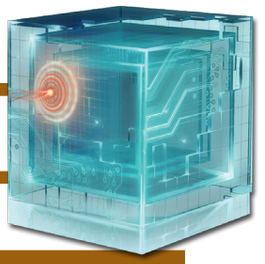
DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Sample Job Titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Forensic Analyst (Cryptologic); Forensic Technician; Network Forensic Examiner)

TASK | KSA

ID	Statement
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
447	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
463	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis
480	Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats
482	Decrypt seized data using technical means
541	Develop reports which organize and document recovered evidence and forensic processes used
564	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)
573	Ensure chain of custody is followed for all digital media acquired (e.g., indications, analysis, and warning standard operating procedures)
613	Examine recovered data for items of relevance to the issue at hand
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
686	Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission

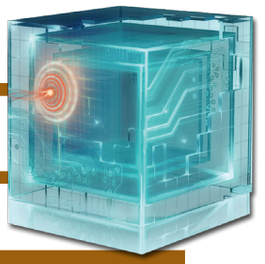


INVESTIGATE

DIGITAL FORENSICS

TASK | KSA

ID	Statement
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
749	Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment
752	Perform file signature analysis
753	Perform hash comparison against established database
758	Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)
759	Perform MAC timeline analysis on a file system
768	Perform static media analysis
771	Perform tier 1, 2, and 3 malware analysis
774	Perform Windows registry analysis
786	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures)
817	Provide technical assistance on digital evidence matters to appropriate personnel
825	Recognize and accurately report forensic artifacts indicative of a particular operating system
839	Review forensic images and other data sources for recovery of potentially relevant information
867	Update hash comparison databases from various libraries (e.g., National Software Reference Library, National Security Agency/Central Security Service Information Systems Incident Response Team)
868	Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis

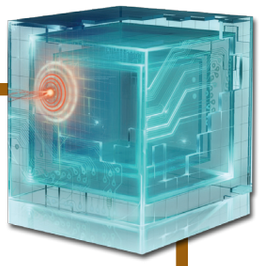


INVESTIGATE

DIGITAL FORENSICS

TASK | KSA

ID	Statement
870	Use network monitoring tools to capture real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis
871	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence
882	Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies
Tasks below are critical for law enforcement and counterintelligence cybersecurity specialty only	
429	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
620	Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
622	Formulate a strategy to insure chain of custody is maintained in such a way that the evidence is not altered (e.g., phones/ PDAs need a power source, hard drives need protection from shock)
799	Provide consultation to investigators and prosecuting attorneys regarding the findings of computer examinations
819	Provide testimony related to computer examinations
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
872	Use an array of specialized computer investigative techniques and programs to resolve the investigation



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Sample Job Titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Forensic Analyst (Cryptologic); Forensic Technician; Network Forensic Examiner)

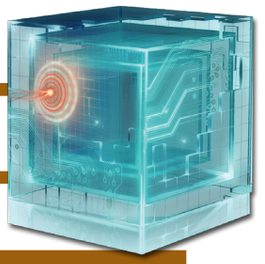
TASK | KSA

ID	Statement	Competency
24	Knowledge of concepts and practices of processing digital information	Data Management
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
61	Knowledge of incident response and handling methodologies	Incident Management
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
113	Knowledge of server and client operating systems	Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques	Computer Forensics
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems	Operating Systems
153	Skill in analyzing malware	Vulnerabilities Assessment
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)	Computers and Electronics

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



INVESTIGATE

DIGITAL FORENSICS

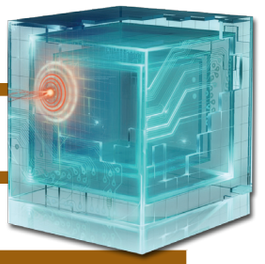
TASK | KSA

ID	Statement	Competency
268	Knowledge of binary analysis	Computer Forensics
287	Knowledge of file system implementations	Operating Systems
290	Knowledge of Forensic Chain of Evidence	Forensics
294	Knowledge of hacking methodologies in Windows or Unix/Linux environment	Surveillance
305	Knowledge of laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)	Forensics
316	Knowledge of processes for packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Criminal Law
340	Knowledge of types and collection of persistent data	Computer Forensics
345	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies	Web Technology
346	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files	Computer Forensics
350	Skill in analyzing memory dumps to extract information	Reasoning
364	Skill in identifying, modifying, and manipulating applicable system components (Window and/or Unix/Linux) (e.g., passwords, user accounts, files)	Operating Systems
369	Skill in processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Forensics
374	Skill in setting up a forensic workstation	Forensics
381	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK)	Computer Forensics
386	Skill in using virtual machines	Operating Systems

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

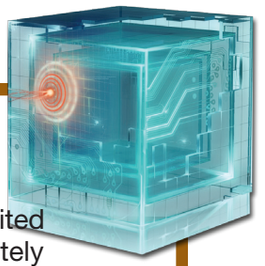


INVESTIGATE

DIGITAL FORENSICS

TASK | KSA

ID	Statement	Competency
389	Skill in disassembling PCs	Computers and Electronics
888	Knowledge of types of digital forensics data and how to recognize them	Computer Forensics
889	Knowledge of deployable forensics	Computer Forensics
890	Knowledge of forensics in multiple operating system environments	Computer Forensics
908	Ability to decrypt digital data collections	Computer Forensics
923	Knowledge of security event correlation tools	Information Systems/Network Security
KSAs below are critical for law enforcement and counterintelligence cybersecurity professionals only		
217	Skill in seizing and preserving digital evidence	Computer Forensics
310	Knowledge of legal governance related to admissibility (Federal Rules of Evidence)	Criminal Law
360	Skill in finding and extracting information of evidentiary value	Computer Forensics



INVESTIGATE

INVESTIGATION

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Sample Job Titles: Computer Crime Investigator, Special Agent

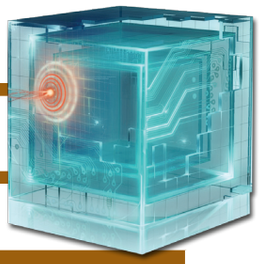
TASK | KSA

ID	Statement
402	Analyze computer-generated threats
429	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
447	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
454	Conduct interviews and interrogations of victims, witnesses, and suspects
507	Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion
512	Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet
564	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)
597	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
613	Examine recovered data for items of relevance to the issue at hand
620	Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
623	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations
633	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action
635	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

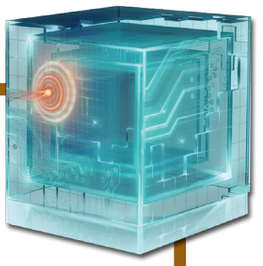


INVESTIGATE

INVESTIGATION

TASK | KSA

ID	Statement
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
637	Identify elements of the crime
642	Identify outside attackers accessing the system from Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges
649	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations
663	Independently conduct large-scale investigations of criminal activities involving complicated computer programs and networks
788	Prepare reports to document analysis
792	Process crime scenes
843	Secure the electronic device or information source
871	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence



INVESTIGATE

INVESTIGATION

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Sample Job Titles: Computer Crime Investigator, Special Agent

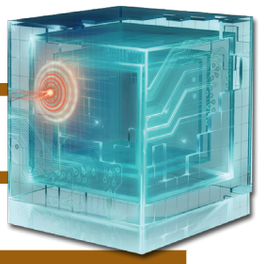
TASK | KSA

ID	Statement	Competency
97	Knowledge of pertinent government laws and information technology regulations	Legal, Government and Jurisprudence
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
217	Skill in seizing and preserving digital evidence	Computer Forensics
281	Knowledge of electronic devices such as computer systems and their components, access control devices, digital cameras, handheld devices, electronic organizers, hard drives, memory cards, modems, network components, connectors, pagers, printers, removable storage devices scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems, and other miscellaneous electronic items	Hardware
290	Knowledge of Forensic Chain of Evidence	Forensics
305	Knowledge of laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)	Forensics
310	Knowledge of legal governance related to admissibility (Federal Rules of Evidence)	Criminal Law
316	Knowledge of processes for packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Criminal Law
340	Knowledge of types and collection of persistent data	Computer Forensics
369	Skill in processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Forensics

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



INVESTIGATE

INVESTIGATION

TASK | KSA

ID	Statement	Competency
383	Skill in using scientific rules and methods to solve problems	Reasoning
917	Knowledge of social dynamics of computer attackers in a global context	External Awareness

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

OPERATE AND COLLECT

Specialty areas responsible for the highly specialized collection of cybersecurity information that may be used to develop intelligence.

Collection Operations

Executes collection using appropriate collection strategies and within the priorities established through the collection management process.

Cyber Operations

Uses automated tools to manage, monitor, and/or execute large-scale cyber operations in response to national and tactical requirements.

Cyber Operations Planning

Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

No Tasks or KSAs are available for these specialty areas

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

ANALYZE

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Cyber Threat Analysis

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

All Source Intelligence

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Exploitation Analysis

Analyzes collected information to identify vulnerabilities and potential for exploitation.

Targets

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

No Tasks or KSAs are available for these specialty areas

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

SUPPORT

Specialty areas providing support so that others may effectively conduct their cybersecurity work.

Legal Advice and Advocacy

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

(Example job titles: Legal Advisor/SJA)

Education and Training

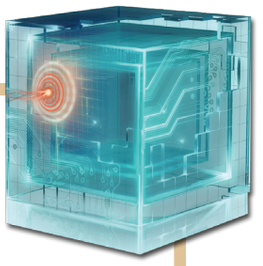
Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

(Example job titles: Cyber Trainer; Information Security Trainer; Security Training Coordinator)

Strategic Planning and Policy Development

Applies knowledge of priorities to define an entitys direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

(Example job titles: Chief Information Officer (CIO); Command IO;Information Security Policy Analyst; Information Security Policy Manager; Policy Writer and Strategist)



SUPPORT

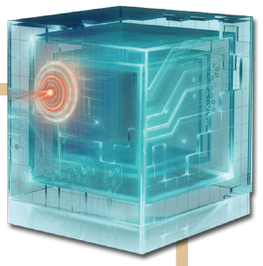
LEGAL ADVICE AND ADVOCACY

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Sample Job Titles: Legal Advisor/SJA

TASK | KSA

ID	Statement
390	Acquire and maintain a working knowledge of relevant laws, regulations, policies, standards, or procedures
398	Advocate organization's official position in legal and legislative proceedings
451	Conduct framing of allegations to determine proper identification of law, regulatory or policy/guidance of violation
539	Develop policy, programs, and guidelines for implementation
574	Evaluate, monitor, and ensure compliance with data security policies and relevant legal and regulatory requirements
599	Evaluate contracts to ensure compliance with funding, legal, and program requirements
607	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures
612	Evaluates the impact (for example, costs or benefits) of changes to laws, regulations, policies, standards, or procedures
618	Explain or provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients
655	Implement new or revised laws, regulations, executive orders, policies, standards, or procedures
675	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues
787	Prepare legal documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery)
834	Resolve conflicts in laws, regulations, policies, standards, or procedures



SUPPORT

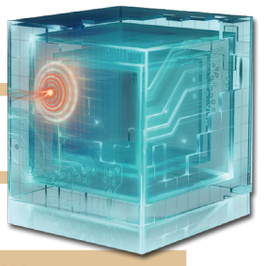
LEGAL ADVICE AND ADVOCACY

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Sample Job Titles: Legal Advisor/SJA

TASK | KSA

ID	Statement	Competency
27	Knowledge of cryptology	Cryptography
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
97	Knowledge of pertinent government laws and information technology regulations	Legal, Government and Jurisprudence
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
244	Ability to determine the validity of technology trend data	Technology Awareness
250	Knowledge of administrative/criminal legal cyber guidelines	Criminal Law
253	Knowledge of applicable statutes in Title 10 of the U.S. Code	Legal, Government and Jurisprudence
255	Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)	Legal, Government and Jurisprudence
257	Knowledge of applicable statutes in Title 32 of the U.S. Code	Legal, Government and Jurisprudence
259	Knowledge of applicable statutes in Title 50 of the U.S. Code (War and National Defense)	Legal, Government and Jurisprudence
279	Knowledge of Electronic Communications Privacy Act (ECPA)	Legal, Government and Jurisprudence
282	Knowledge of emerging computer-based technology that have potential for exploitation by adversaries	Technology Awareness

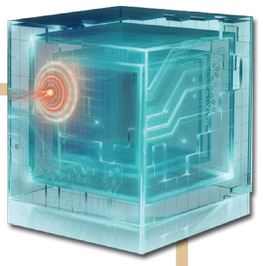


SUPPORT

LEGAL ADVICE AND ADVOCACY

TASK | KSA

ID	Statement	Competency
288	Knowledge of Foreign Intelligence Surveillance Act and Protect America Act laws and regulations associated with electronic surveillance	Legal, Government and Jurisprudence
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
300	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions	Organizational Awareness
318	Knowledge of Presidential Directives and executive branch guidelines that apply to cyber activities	Legal, Government and Jurisprudence
323	Knowledge of search and seizure laws	Criminal Investigation
333	Knowledge of the implications of the Bill of Rights (Amendments 1-10 of the U.S. Constitution) for cybersecurity	Legal, Government and Jurisprudence
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
339	Knowledge of the structure and intent of military operation plans, concept operation plans, orders, and standing rules of engagement	Organizational Awareness
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence



SUPPORT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

Sample Job Titles: Chief Information Officer (CIO), Command IO, Information Security Policy Analyst, Information Security Policy Manager, Policy Writer and Strategist

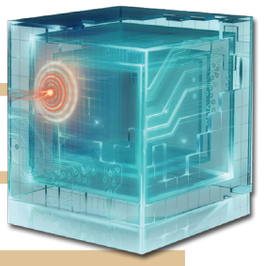
TASK | KSA

ID	Statement
410	Analyze organizational information security policy
424	Assess policy needs and collaborate with stakeholders to develop policies to govern IT activities
485	Define current and future business environments
492	Design a cybersecurity strategy that outlines the vision, mission, and goals that align with the organization's strategic plan
524	Develop and maintain strategic plans
539	Develop policy, programs, and guidelines for implementation
565	Draft and publish security policy
594	Establish and maintain communication channels with stakeholders
629	Identify and address IT workforce planning and management issues, such as recruitment, retention, and training
641	Identify organizational policy stakeholders
720	Monitor the rigorous application of information security/information assurance policies, principles, and practices in the delivery of planning and management services
724	Obtain consensus on proposed policy change from stakeholders
812	Provide policy guidance to IT management, staff, and users
838	Review existing and proposed policies with stakeholders
840	Review or conduct audits of IT programs and projects

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

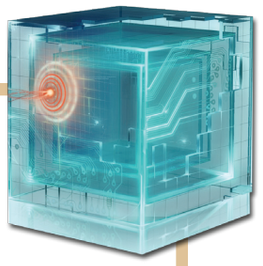


SUPPORT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

TASK | KSA

ID	Statement
847	Serve on agency and interagency policy boards
854	Support the CIO in the formulation of IT-related policies
884	Write Information Assurance (IA) policy and instructions.\



SUPPORT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

Sample Job Titles: Chief Information Officer (CIO), Command IO, Information Security Policy Analyst, Information Security Policy Manager, Policy Writer and Strategist

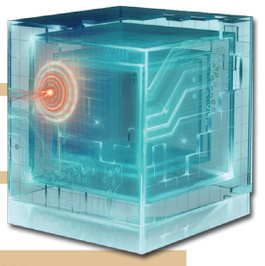
TASK | KSA

ID	Statement	Competency
27	Knowledge of cryptology	Cryptography
45	Knowledge of existing IA security principles, policies, and procedures	Information Assurance
88	Knowledge of new and emerging IT and information security technologies	Technology Awareness
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection	Legal, Government and Jurisprudence
244	Ability to determine the validity of technology trend data	Technology Awareness
250	Knowledge of administrative/criminal legal cyber guidelines	Criminal Law
253	Knowledge of applicable statutes in Title 10 of the U.S. Code	Legal, Government and Jurisprudence
255	Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)	Legal, Government and Jurisprudence
257	Knowledge of applicable statutes in Title 32 of the U.S. Code	Legal, Government and Jurisprudence
259	Knowledge of applicable statutes in Title 50 of the U.S. Code (War and National Defense)	Legal, Government and Jurisprudence
279	Knowledge of Electronic Communications Privacy Act (ECPA)	Legal, Government and Jurisprudence
282	Knowledge of emerging computer-based technology that have potential for exploitation by adversaries	Technology Awareness
288	Knowledge of Foreign Intelligence Surveillance Act and Protect America Act laws and regulations associated with electronic surveillance	Legal, Government and Jurisprudence

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

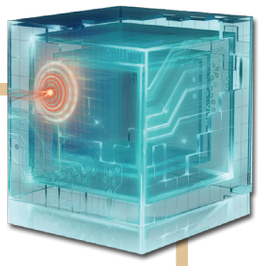


SUPPORT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

TASK | KSA

ID	Statement	Competency
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
300	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions	Organizational Awareness
318	Knowledge of Presidential Directives and executive branch guidelines that apply to cyber activities	Legal, Government and Jurisprudence
320	Knowledge of private-sector organizations and academic institutions dealing with cyber-security issues	External Awareness
323	Knowledge of search and seizure laws	Criminal Investigation
333	Knowledge of the implications of the Bill of Rights (Amendments 1-10 of the U.S. Constitution) for cybersecurity	Legal, Government and Jurisprudence
336	Knowledge of the nature and function of the National Information Infrastructure	Telecommunications
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence
887	Knowledge of human system integration principles including accessibility factors and standards	Human Factors
918	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures	Teaching Others
919	Ability to promote awareness of security issues among management and ensure sound security principles are reflected in organizations' visions and goals	Political Savvy



SUPPORT

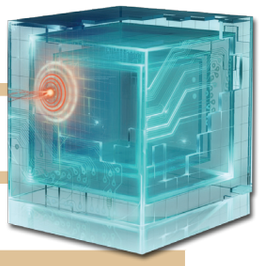
EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

Sample Job Titles: Cyber Trainer, Information Security Trainer, Security Training Coordinator

TASK | KSA

ID	Statement
453	Conduct interactive training exercises to create an effective learning environment
479	Correlate mission requirements to training
490	Deliver training courses tailored to the audience and physical environment
491	Demonstrate concepts, procedures, software, equipment, and technology applications to coworkers, subordinates, or others
504	Design training curriculum and course content
510	Determine training requirements (e.g., subject matter, format, location)
538	Develop new or identify existing awareness and training materials that are appropriate for intended audiences
551	Develop the goals and objectives for cybersecurity training, education, or awareness
567	Educate customers in established procedures and processes to ensure professional media standards are met
587	Ensure that information security personnel are receiving the appropriate level and type of training
588	Ensure that information security personnel can identify the limits of their capabilities (legally, technically, and skill) and the organization that may assist
606	Evaluate the effectiveness and comprehensiveness of existing training programs
624	Guide new and junior coworkers through career development and training choices
778	Plan classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment

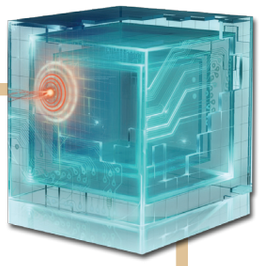


SUPPORT

EDUCATION AND TRAINING

TASK | KSA

ID	Statement
779	Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
833	Report tactical or strategic information derived from forensic processes through appropriate law enforcement/ counter-intelligence channels.
841	Review training documentation (e.g., Course Content Documents [COD], Lesson Plans, Student Texts, examinations, Schedules of Instruction [SOI], course descriptions)
842	Revise curriculum end course content based on feedback from previous training sessions
845	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media, cartography)
855	Support the design and execution of exercise scenarios
885	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce



SUPPORT

EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

Sample Job Titles: Cyber Trainer, Information Security Trainer, Security Training Coordinator

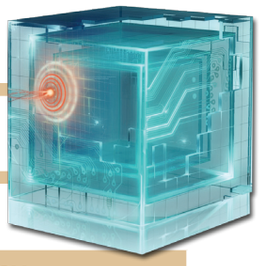
TASK | KSA

ID	Statement	Competency
80	Knowledge of network architecture concepts including topology, protocols, and components	Infrastructure Design
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
246	Knowledge and experience in the Instructional System Design methodology	Multimedia Technologies
252	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools, and laws/regulations	Computer Network Defense
253	Knowledge of applicable statutes in Title 10 of the U.S. Code	Legal, Government and Jurisprudence
255	Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)	Legal, Government and Jurisprudence
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)	Computers and Electronics
305	Knowledge of laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)	Forensics
314	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support



SUPPORT

EDUCATION AND TRAINING

TASK | KSA

ID	Statement	Competency
332	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience	Teaching Others
344	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems
359	Skill in developing and executing technical training programs and curricula	Computer Forensics
363	Skill in identifying gaps in technical capabilities	Teaching Others
376	Skill in talking to others to convey information effectively	Oral Communication
918	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures	Teaching Others