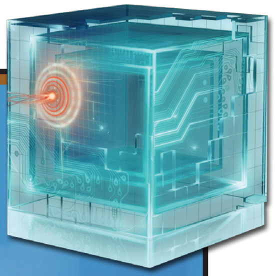
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a diverse, qualified cybersecurity workforce is vital to our nation's security and prosperity.
[full text version]

DEFINING CYBERSECURITY

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.
[full text version]

THE CALL TO ACTION

Only in the universal adoption of the *National Cybersecurity Workforce Framework* can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.
[full text version]

OPERATE AND MAINTAIN

SECURELY PROVISION

PROTECT AND DEFEND

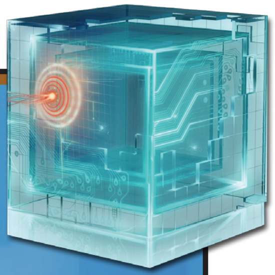
OVERSIGHT AND DEVELOPMENT

ANALYZE

INVESTIGATE

COLLECT AND OPERATE

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce is vital to our nation's security and prosperity.

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 descriptions, and the Office of Personnel Management [OPM] series). This absence of a common language to describe and understand cybersecurity work and requirements hinders our nation's ability to establish a baseline of capabilities, identify skills gaps, ensure an adequate pipeline of future talent, and continuously develop a highly-qualified cybersecurity workforce. Consequently, establishing and using a common lexicon, taxonomy, and other data standards for cybersecurity work and requirements is not merely desirable, it is vital.

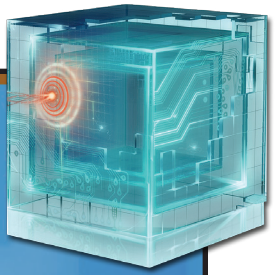
The compelling need for enhanced public and private cybersecurity capabilities and a more enlightened public has been documented repeatedly over the last twenty years. Unfortunately, many of these issues have persisted over time and, by virtue of not improving, have become more acute. A National Research Council report lamented this problem in 2002:

> ***The unfortunate reality is that relative to the magnitude of the threat, our ability and willingness to deal with threats have, on balance, changed for the worse, making many of the analyses, findings, and recommendations of these reports all the more relevant, timely, and applicable today. (National Research Council Computer Science and Telecommunications Board, 2002).***

These challenges are exacerbated by the unique aspects of cybersecurity work. For example, the cybersecurity workforce must keep up with emerging risks, threats, vulnerabilities, and associated technologies that may require more rapid skill and knowledge acquisition than other functional areas. In fact, this requirement makes a compelling case for the need for innovative, robust private-public partnerships, and the capacity for cybersecurity talent to move more easily between public and private sector jobs and in and out of academia to maintain and develop skills and advance the collective knowledge base for future capabilities.

In recognition of the criticality of these issues, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The workforce aspect of the CNCI was specifically emphasized and reinforced in 2010 when President Obama established the National Initiative for Cybersecurity Education (NICE), which was formerly CNCI Initiative 8. The NICE is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Its goals are to encourage and help increase cybersecurity awareness and competence across the nation and to build an agile, highly skilled cybersecurity workforce capable of responding to a dynamic and rapidly evolving array of threats.

More information about the National Initiative for Cybersecurity Education can be found at **http://csrc.nist.gov/nice/**. This document is available online at **http://csrc.nist.gov/nice/framework/**



DEFINING THE CYBERSECURITY WORKFORCE

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The NICE, in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.

The *National Cybersecurity Workforce Framework* establishes the common taxonomy and lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The Framework is intended to be applied in the public, private, and academic sectors. Use of the Framework does not require that organizations change organizational or occupational structures. In fact, the Framework was developed because requiring such changes would be costly, impractical, ineffective, and inefficient.

The Framework is agnostic to the particulars of a given organization and is overarching by design so that it can be overlaid onto any existing occupational structure to facilitate achieving an agile, highly-qualified cybersecurity workforce.

The Framework consists of thirty-one specialty areas organized into seven categories. These categories, serving as an overarching structure for the Framework, group related specialty areas together. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided.

This interactive document provides the Framework in its entirety.

The seven categories and a description of the types of specialty areas included in each are below

SECURELY PROVISION - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

OPERATE AND MAINTAIN - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

PROTECT AND DEFEND - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

INVESTIGATE - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

COLLECT AND OPERATE - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

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

OVERSIGHT AND DEVELOPMENT - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

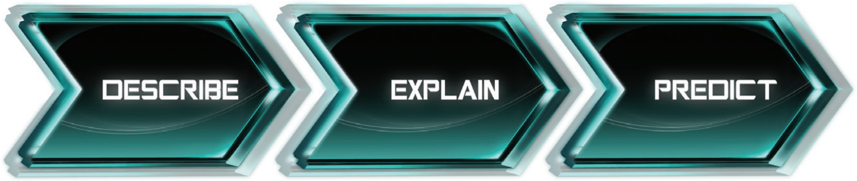
THE CALL TO ACTION

Only in the universal adoption of the National Cybersecurity Workforce Framework can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.

The Framework is at the core of this vital capability as it enables all organizations to describe their cybersecurity work and workforces with an unprecedented level of consistency, detail, and quality. It is only with this understanding that organizations can analyze and explain the factors and dynamics that influence the workforce and work requirements. This in turn supports maturing to a predictive model that will anticipate requirements, gaps, needs, and other critical strategic and operational workforce issues.

For example, initially an organization may only know the attrition rates for a segment of the cybersecurity population. As it collects and analyzes the data and other information consistent with the Framework, it will mature in its understanding of cybersecurity retention issues, be able to identify root causes, know the extent of the potential impact of the attrition, and take appropriate action to prevent continued attrition. Finally, the desired end state is to predict workforce retention issues in advance and take actions to preempt them.

This approach is depicted in the figure below.

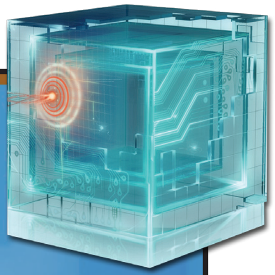


To achieve these goals, the Framework's specified labels and definitions should be used when describing the corresponding work or workers; otherwise the inability to truly understand the cybersecurity workforce will persist and the nation will be unnecessarily vulnerable to risk.

While fidelity to the Framework labels and definitions is essential, the Framework is flexible by design and is intended to accommodate existing organizational structures. ***The key is describing similar cybersecurity work, work requirements, and related skills using this common lexicon.***

Once organizations standardize their cybersecurity workforce information according to the Framework, the following initiatives can proceed in a meaningful, coherent, and cost-effective way across all sectors of the economy:

Collect and Analyze Data	Capture cybersecurity workforce and training data to understand capabilities and needs.
Recruit and Retain	Incentivize the hiring and retention of highly skilled and adaptive professionals needed for a secure digital nation.
Educate, Train, and Develop	Expand the pipeline for and deliberately develop an unrivaled cybersecurity workforce.
Engage	Educate and energize all cybersecurity workforces and the American public to strengthen the nation's front lines of cybersecurity.



SAMPLE JOB TITLES

The Framework is designed to be useful across all cybersecurity functions and organizations. The following list of sample job titles may be helpful as organizations adopt and prepare to use the Framework. It is important to note that this list is illustrative only and represents job titles that are frequently aligned with the indicated specialty area. A similar determination in any organization should be made based on a review of the work performed and the Framework.

The sample job titles are organized by specialty area in each category. Please note that no sample job titles are provided for the "Analyze" and "Collect and Operate" specialty areas in this document due to the unique and highly specialized nature of that work.

Securely Provision - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

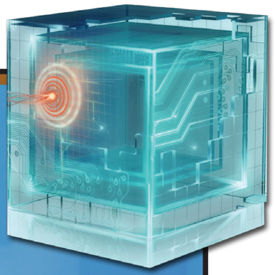
Information Assurance (IA) Compliance - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

- Accreditor
- Auditor
- Authorizing Official Designated Representative
- Certification Agent
- Certifying Official
- Compliance Manager
- Designated Accrediting Authority
- Information Assurance (IA) Auditor
- Information Assurance (IA) Compliance Analyst/Manager
- Information Assurance (IA) Manager
- Information Assurance (IA) Officer
- Portfolio Manager
- Quality Assurance (QA) Specialist
- Risk/Vulnerability Analyst
- Security Control Assessor
- Systems Analyst
- Validator

Software Assurance and Security Engineering - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

- Analyst Programmer
- Computer Programmer
- Configuration Manager
- Database Developer/Engineer/Architect
- Information Assurance (IA) Engineer
- Information Assurance (IA) Software Developer
- Information Assurance (IA) Software Engineer
- Research & Development Engineer
- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer

NEXT PAGE | PREVIOUS PAGE



SAMPLE JOB TITLES (CONTINUED)

Systems Security Architecture - Develops system 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.

- Information Assurance (IA) Architect
- Information Security Architect
- Information Systems Security Engineer
- Network Security Analyst
- Research & Development Engineer
- Security Architect
- Security Engineer
- Security Solutions Architect
- Systems Engineer
- Systems Security Analyst

Technology Research and Development - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

- Capabilities and Development Specialist
- Chief Engineer
- Research & Development Engineer

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.

- Business Analyst
- Business Process Analyst
- Computer Systems Analyst
- Human Factors Engineer
- Requirements Analyst
- Solutions Architect
- Systems Consultant
- Systems Engineer

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 information technology (IT).

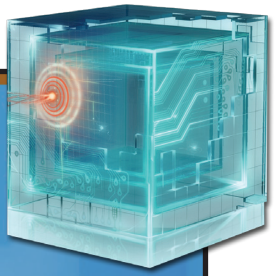
- Application Security Tester
- Information Systems Security Engineer
- Quality Assurance (QA) Tester
- Research & Development Engineer
- Research & Development Research Engineer
- Security Systems Engineer
- Software Quality Assurance (QA) Engineer
- Software Quality Engineer
- Systems Engineer
- Testing and Evaluation Specialist

Systems Development - Works on the development phases of the systems development lifecycle.

- Firewall Engineer
- Information Assurance (IA) Developer
- Information Assurance (IA) Engineer
- Information Assurance (IA) Software Engineer
- Information Systems Security Engineer
- Program Developer
- Security Engineer
- Systems Engineer
- Systems Security Engineer

NEXT PAGE | PREVIOUS PAGE

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SAMPLE JOB TITLES (CONTINUED)

Operate and Maintain - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (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.

- Content Staging Specialist
- Data Architect
- Data Custodian
- Data Manager
- Data Warehouse Specialist
- Database Administrator
- Database Developer
- Database Engineer/Architect
- Information Dissemination Manager
- Systems Operations Personnel

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

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

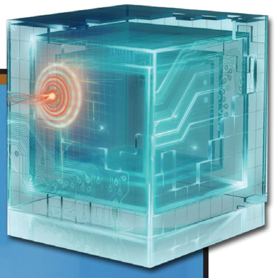
- Computer Support Specialist
- Customer Support
- Help Desk Representative
- Service Desk Operator
- Systems Administrator
- Technical Support Specialist
- User Support Specialist

Network Services - Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

- Cabling Technician
- Converged Network Engineer
- Network Administrator
- Network Analyst
- Network Designer
- Network Engineer
- Network Systems and Data Communications Analyst
- Network Systems Engineer
- Systems Engineer
- Telecommunications Engineer/Personnel/Specialist

NEXT PAGE | PREVIOUS PAGE

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SAMPLE JOB TITLES (CONTINUED)

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.

- Local Area Network (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.

- Information Assurance (IA) Operational Engineer
- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager
- Information Security Specialist
- Information Systems Security Engineer
- Information Systems Security Manager (ISSM)
- Platform Specialist
- Security Administrator
- Security Analyst
- Security Control Assessor
- Security Engineer

Protect and Defend - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

Computer Network Defense (CND) Analysis - 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.

- Computer Network Defense (CND) Analyst (Cryptologic)
- Cybersecurity Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- 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.

- Computer Crime Investigator
- Incident Handler
- Incident Responder
- Incident Response Analyst
- Incident Response Coordinator
- Intrusion Analyst

NEXT PAGE | PREVIOUS PAGE

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

SAMPLE JOB TITLES (CONTINUED)

Computer Network Defense (CND) Infrastructure Support - Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

- Information Systems Security Engineer
- Intrusion Detection System (IDS) Administrator
- Intrusion Detection System (IDS) Engineer
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Analyst
- Network Security Engineer
- Network Security Specialist
- Security Analyst
- Security Engineer
- Security Specialist
- Systems Security Engineer

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

- Blue Team Technician
- Certified TEMPEST[1] Professional
- Certified TEMPEST[1] Technical Authority
- Close Access Technician
- Computer Network Defense (CND) Auditor
- Compliance Manager
- Ethical Hacker
- Governance Manager
- Information Security Engineer
- Internal Enterprise Auditor
- Penetration Tester
- Red Team Technician
- Reverse Engineer
- Risk/Vulnerability Analyst
- Technical Surveillance Countermeasures Technician
- Vulnerability Manager

Investigate - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

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.

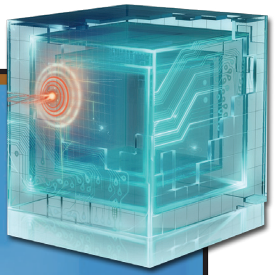
- Computer Forensic Analyst
- Computer Network Defense (CND) Forensic Analyst
- Digital Forensic Examiner
- Digital Media Collector
- Forensic Analyst
- Forensic Analyst (Cryptologic)
- Forensic Technician
- Network Forensic Examiner

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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

- Computer Crime Investigator
- Special Agent

[1] TEMPEST is a codename and not an acronym

NEXT PAGE | PREVIOUS PAGE



SAMPLE JOB TITLES (CONTINUED)

Oversight and Development - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Education and Training - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

- Cyber Trainer
- Information Security Trainer
- Security Training Coordinator

Information Systems Security Operations (Information Systems Security Officer [ISSO]) - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

- Contracting Officer (CO)
- Contracting Officer Technical Representative (COTR)
- Information Assurance (IA) Manager
- Information Assurance (IA) Program Manager
- Information Assurance (IA) Security Officer
- Information Security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Information Systems Security Operator

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.

- Legal Advisor/Staff Judge Advocate (SJA)
- Paralegal

Security Program Management (Chief Information Security Officer [CISO]) - Manages 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.

- Chief Information Security Officer (CISO)
- Common Control Provider
- Cyber Security Officer
- Enterprise Security Officer
- Facility Security Officer
- Information Systems Security Manager (ISSM)
- Information Technology (IT) Director
- Principal Security Architect
- Risk Executive
- Security Domain Specialist
- Senior Agency Information Security (SAIS) Officer

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.

- Chief Information Officer (CIO)
- Command Information Officer
- Information Security Policy Analyst
- Information Security Policy Manager
- Policy Writer and Strategist

NEXT PAGE | PREVIOUS PAGE

USING THIS DOCUMENT

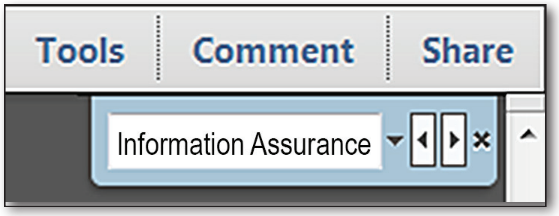
Navigating the Framework

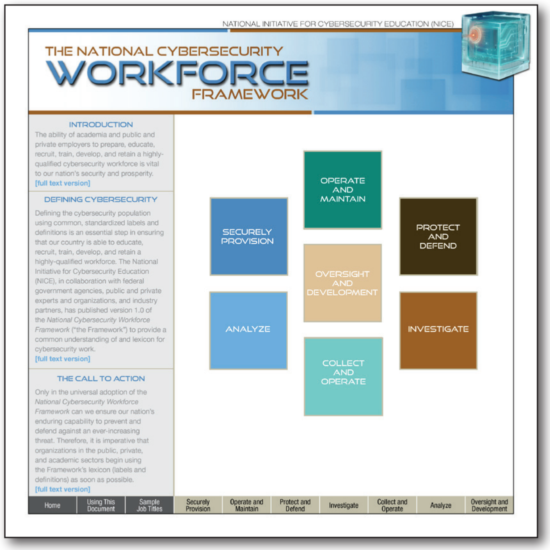
To navigate to a particular Framework category from the Home page, click on one of the seven large category boxes or the smaller tabs at the bottom of the page. Tabs appear on every page, allowing you to easily navigate the Framework.

Once inside a Framework category, select a specific specialty area to explore it further. Selecting a specialty area will display a detailed view of that specialty area including associated tasks and KSAs. You can switch between the specialty area tasks or KSAs at any time by selecting the "Task" or "KSA" tab at the top of the list.

Searching the Framework

To search for a particular word or term, press "CTRL+F" and type the word or term in the "Find" box of the Adobe® Reader menu bar (typically in the upper right corner of the screen). Then press "Enter." The small down arrow to the right of the "Find" box gives options for refining a search. The small left and right arrows search backwards and forwards in the document.





NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce is vital to our nation's security and prosperity. [full text version]

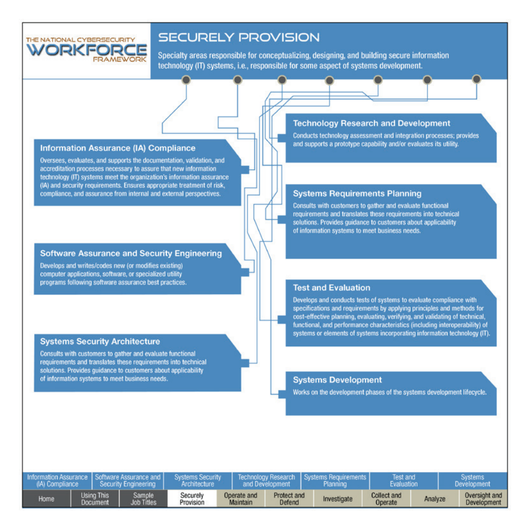
DEFINING CYBERSECURITY

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work. [full text version]

THE CALL TO ACTION

Only in the universal adoption of the *National Cybersecurity Workforce Framework* can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible. [full text version]

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE
Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SECURELY PROVISION

Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, i.e., responsible for some aspect of systems development.

Information Assurance (IA) Compliance Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Software Assurance and Security Engineering Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Systems Security Architecture 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.

Technology Research and Development Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

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.

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 information technology (IT).

Systems Development Works on the development phases of the systems development lifecycle.

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development
Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

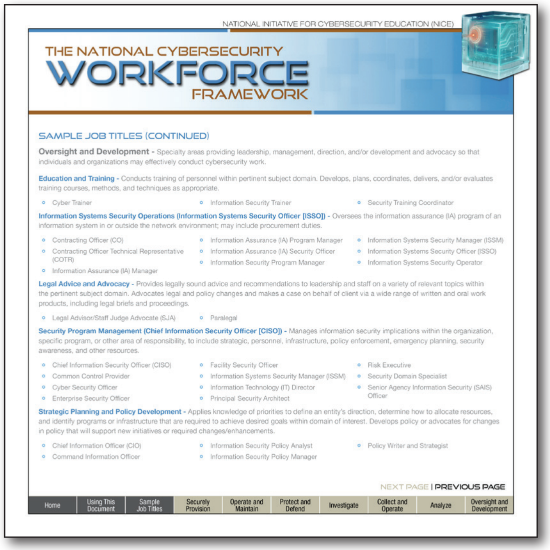
SECURELY PROVISION | INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK | KSA

ID	Statement
537	Develop methods to monitor and measure risk, compliance, and assurance efforts
548	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level
566	Draft statements of preliminary or residual security risks for system operation
691	Maintain information systems assurance and accreditation materials
696	Manage and approve Accreditation Packages (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 15026-2)
710	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability 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 authorization reviews and assurance case development for initial installation of software applications, systems, and networks
798	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant information assurance (IA) compliances
827	Recommend new or revised security, resilience, and dependability measures based on the results of reviews
836	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network
878	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations
879	Verify that the software application/network/system accreditation and assurance documentation is current
936	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers)
937	Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development
Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

Oversight and Development - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Education and Training - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

- Cyber Trainer
- Information Security Trainer
- Security Training Coordinator

Information Systems Security Operations (Information Systems Security Officer [ISSO]) - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

- Contracting Officer (CO)
- Contracting Officer Technical Representative (COTR)
- Information Assurance (IA) Manager
- Information Assurance (IA) Program Manager
- Information Assurance (IA) Security Officer
- Information Security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Information Systems Security Operator

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.

- Legal Advisor/Staff Judge Advocate (SJA)
- Paralegal

Security Program Management (Chief Information Security Officer [CISO]) - Manages 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.

- Chief Information Security Officer (CISO)
- Common Control Provider
- Cyber Security Officer
- Enterprise Security Officer
- Facility Security Officer
- Information Systems Security Manager (ISSM)
- Information Technology (IT) Director
- Principal Security Architect
- Risk Executive
- Security Domain Specialist
- Senior Agency Information Security (SAIS) Officer

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.

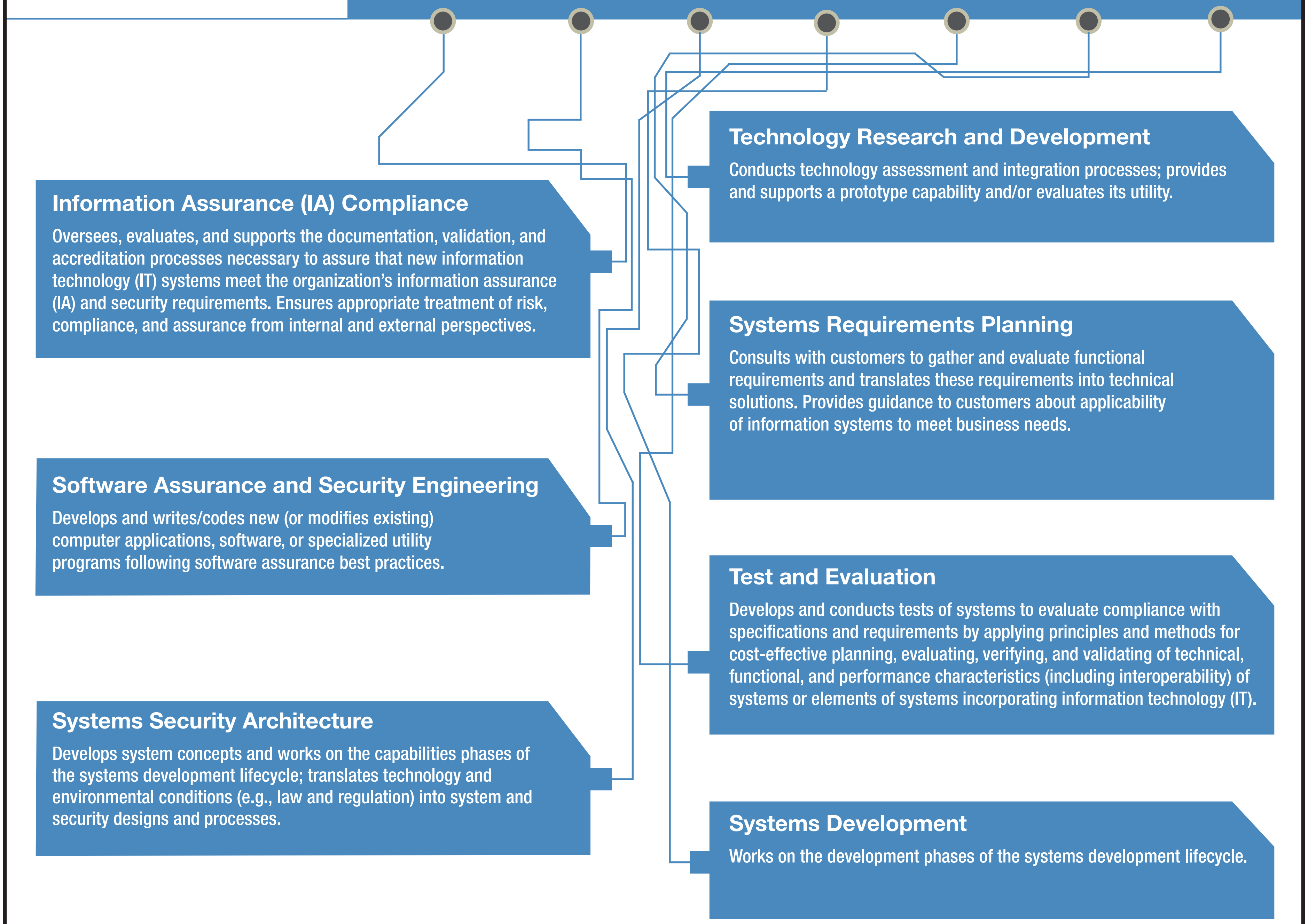
- Chief Information Officer (CIO)
- Command Information Officer
- Information Security Policy Analyst
- Information Security Policy Manager
- Policy Writer and Strategist

NEXT PAGE | PREVIOUS PAGE

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SECURELY PROVISION

Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, i.e., responsible for some aspect of systems development.



Information Assurance (IA) Compliance

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Software Assurance and Security Engineering

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Systems Security Architecture

Develops system 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.

Technology Research and Development

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

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.

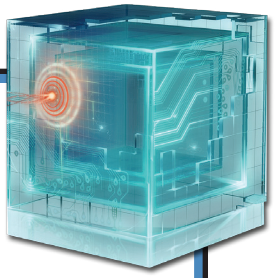
Test and Evaluation

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 information technology (IT).

Systems Development

Works on the development phases of the systems development lifecycle.

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development



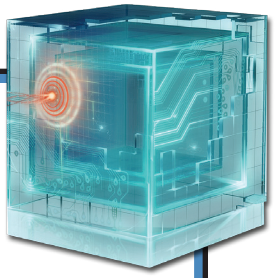
SECURELY PROVISION

INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK KSA

ID	Statement
537	Develop methods to monitor and measure risk, compliance, and assurance efforts
548	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level
566	Draft statements of preliminary or residual security risks for system operation
691	Maintain information systems assurance and accreditation materials
696	Manage and approve Accreditation Packages (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 15026-2)
710	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability 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 authorization reviews and assurance case development for initial installation of software applications, systems, and networks
798	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant information assurance (IA) compliances
827	Recommend new or revised security, resilience, and dependability measures based on the results of reviews
836	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network
878	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations
879	Verify that the software application/network/system accreditation and assurance documentation is current
936	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers)
937	Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system



SECURELY PROVISION

INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

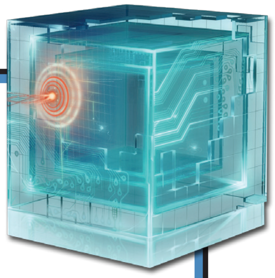
TASK | KSA

ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
77	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
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 information technology (IT) goals and objectives	Enterprise Architecture
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	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
942	Knowledge of the organization's core business/mission processes	Organizational Awareness

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

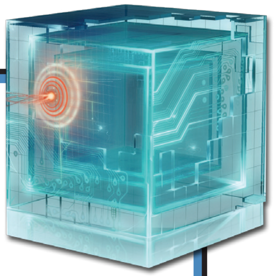
TASK | KSA

ID	Statement	Competency
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

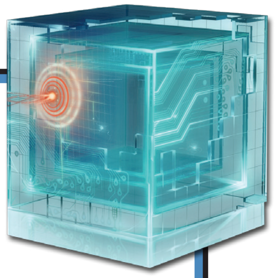
TASK | KSA

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 applications and to obtain information on project limitations and capabilities, performance requirements, and interfaces
465	Develop threat model based on customer interviews and requirements
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
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
602	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

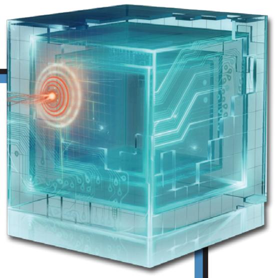
SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK | KSA

ID	Statement
634	Identify basic common coding flaws at a high level
644	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's 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 quality assurance testing for security functionality and resiliency from attacks
764	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities
770	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) 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
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
969	Perform penetration testing as required for new or updated applications
970	Apply defensive functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities of supply chain vulnerabilities
971	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements
972	Determine and document critical numbers of software patches or the extent of releases that would leave software vulnerable

NEXT PAGE | PREVIOUS PAGE



SECURELY PROVISION

SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

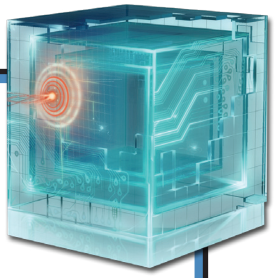
TASK KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
20	Knowledge of complex data structures	Object Technology
23	Knowledge of computer programming principles such as object-oriented design	Object Technology
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
43	Knowledge of embedded systems	Embedded Computers
56	Knowledge of information assurance (IA) principles and methods that apply to software development	Information Assurance
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
74	Knowledge of low-level computer languages (e.g., assembly languages)	Computer Languages
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
102	Knowledge of programming language structures and logic	Computer Languages

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

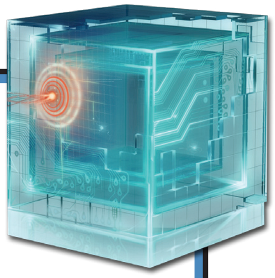
TASK | KSA

ID	Statement	Competency
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 (e.g., waterfall model, spiral model)	Software Engineering
119	Knowledge of software engineering	Software Engineering
121	Knowledge of structured analysis principles and methods	Logical Systems Design
123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
149	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol (SOAP), 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
185	Skill in developing applications that can log errors, exceptions, and application faults and logging	Software Development

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

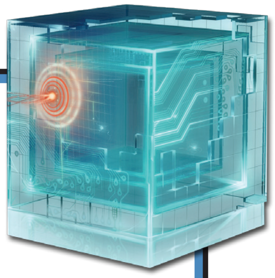
TASK KSA

ID	Statement	Competency
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 that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) 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	Computer Languages
968	Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization)	Information Systems/Network Security
973	Skill in using code analysis tools to eradicate bugs	Software Development
974	Ability to tailor code analysis for application-specific concerns	Software Testing and Evaluation
975	Skill in integrating black box security testing tools into quality assurance process of software releases	Quality Assurance
976	Knowledge of software quality assurance process	Software Engineering
978	Knowledge of root cause analysis for incidents	Incident Management
979	Knowledge of supply chain risk management processes and practices	Risk Management
980	Skill in performing root cause analysis for incidents	Incident Management
1020	Skill in secure test plan design (i.e., unit, integration, system, acceptance)	Systems Testing and Evaluation

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

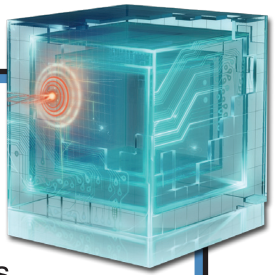
SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK KSA

ID	Statement	Competency
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1071	Knowledge of secure software deployment methodologies, tools, and practices	Software Engineering
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

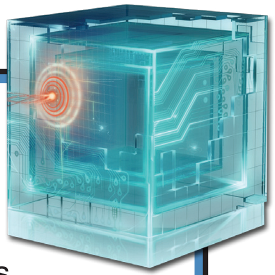
TASK | KSA

ID	Statement
413	Analyze user needs and requirements to plan system architecture
437	Collaborate with system developers and users 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 recovery/restoration
502	Design system architecture or system components required to meet user needs
534	Develop information assurance (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)
561	Document and address organization's information security, information assurance (IA) architecture, and systems security engineering requirements throughout the acquisition lifecycle
563	Document design specifications, installation instructions, and other system-related information
568	Employ secure configuration management processes
569	Ensure all definition and architecture activities (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials) are properly documented and updated as necessary
579	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's information assurance (IA) architecture guidelines
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
631	Identify and prioritize critical business functions in collaboration with organizational stakeholders
646	Identify the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

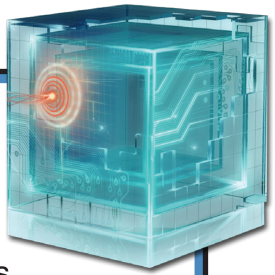
TASK | KSA

ID	Statement
765	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan
780	Plan system implementation to ensure that all system components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware)
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 Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
849	Specify power supply and heating, ventilation, and air conditioning (HVAC) requirements and configuration based on system performance expectations and design specifications
864	Translate proposed technical solutions into technical specifications
994	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment
995	Document and manage an enterprise technical risk register, prioritizing and managing technical risks throughout the system lifecycle
996	Assess and design key management functions (as related to information assurance [IA])

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

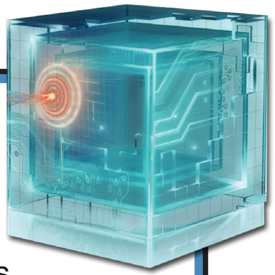
TASK | KSA

ID	Statement	Competency
8	Knowledge of access authentication methods	Identity Management
21	Knowledge of computer algorithms	Mathematical Reasoning
22	Knowledge of computer networking fundamentals	Infrastructure Design
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
43	Knowledge of embedded systems	Embedded Computers
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
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

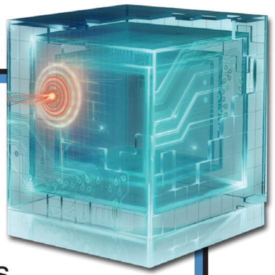
SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

TASK | KSA

ID	Statement	Competency
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
65	Knowledge of information theory	Mathematical Reasoning
68	Knowledge of information technology (IT) architectural concepts and frameworks	Information Technology Architecture
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	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

NEXT PAGE | PREVIOUS PAGE



SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

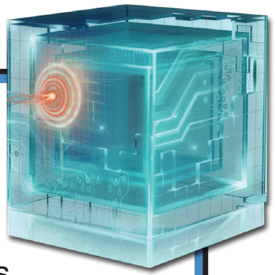
TASK | KSA

ID	Statement	Competency
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
113	Knowledge of server and client operating systems	Operating Systems
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
132	Knowledge of technology integration processes	Systems Integration
133	Knowledge of telecommunications concepts	Telecommunications
141	Knowledge of the enterprise information technology (IT) architecture	Information Technology Architecture
143	Knowledge of the organization’s enterprise information technology (IT) goals and objectives	Enterprise Architecture
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
180	Skill in designing the integration of hardware and software solutions	Systems Integration

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SYSTEMS SECURITY ARCHITECTURE

Develops system 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.

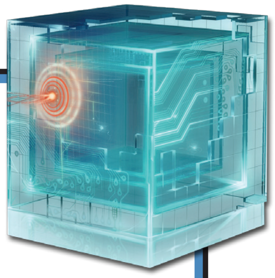
TASK | KSA

ID	Statement	Competency
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
904	Knowledge of interpreted and compiled computer languages	Computer Languages
993	Knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DODAF], Federal Enterprise Architecture Framework [FEAF])	Enterprise Architecture
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



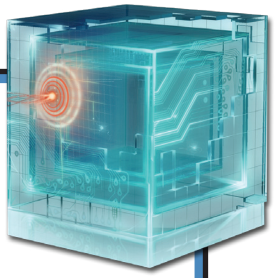
SECURELY PROVISION

TECHNOLOGY RESEARCH AND DEVELOPMENT

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

TASK KSA

ID	Statement
455	Conduct continuous analysis to identify network and system vulnerabilities
520	Develop and implement data mining and data warehousing programs
925	Research current technology to understand capabilities of required system or network
927	Research and evaluate all available technologies and standards to meet customer requirements
934	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements
1076	Collaborate with stakeholders to identify and/or develop appropriate solutions technology
1077	Design and develop new tools/technologies
1078	Troubleshoot prototype design and process issues throughout the product design, development, and post-launch phases
1079	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate cyberspace vulnerabilities
1080	Identify and/or develop reverse engineering tools to detect cyberspace vulnerabilities



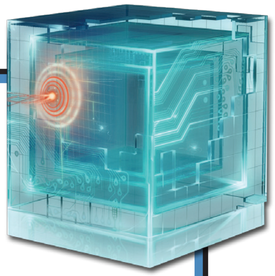
TECHNOLOGY RESEARCH AND DEVELOPMENT

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

TASK | KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing 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
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware	Hardware
27	Knowledge of cryptology	Cryptography
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
132	Knowledge of technology integration processes	Systems Integration
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation

NEXT PAGE | PREVIOUS PAGE



SECURELY PROVISION

TECHNOLOGY RESEARCH AND DEVELOPMENT

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

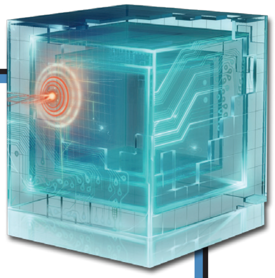
TASK | KSA

ID	Statement	Competency
180	Skill in designing the integration of hardware and software solutions	Systems Integration
238	Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) in a modern programming language (e.g., Java, C++)	Computer Languages
321	Knowledge of products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky) and how differences affect exploitation/ vulnerabilities	Technology Awareness
371	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [VBS]) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data)	Operating Systems
905	Knowledge of secure coding techniques	Computer Languages
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1042	Ability to apply network programming towards client/server model	Requirements Analysis
1044	Skill in identifying forensic footprints	Computer Forensics
1047	Skill in writing kernel level applications	Software Development
1052	Knowledge of Global Systems for Mobile Communications (GSM) architecture	Telecommunications

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



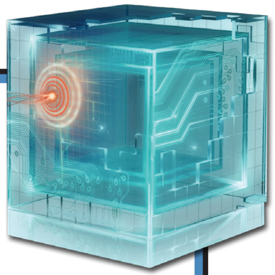
TECHNOLOGY RESEARCH AND DEVELOPMENT

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

TASK | KSA

ID	Statement	Competency
1054	Knowledge of hardware reverse engineering techniques	Vulnerabilities Assessment
1055	Knowledge of middleware	Software Development
1056	Knowledge of operations security	Public Safety and Security
1059	Knowledge of networking protocols	Infrastructure Design
1061	Knowledge of the lifecycle process	Systems Life Cycle
1062	Knowledge of software reverse engineering techniques	Vulnerabilities Assessment
1063	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications)	Operating Systems
1064	Knowledge of Extensible Markup Language (XML) schemas	Infrastructure Design
1066	Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (penetration and testing)	Vulnerabilities Assessment
1067	Skill in utilizing network analysis tools to identify software communications vulnerabilities	Vulnerabilities Assessment
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



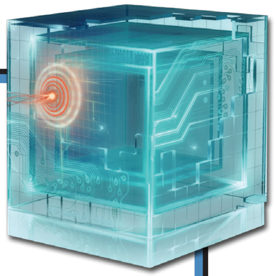
SECURELY PROVISION

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.

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
511	Develop an enterprise system security context, a preliminary system security concept of operations, and define baseline system security requirements in accordance with applicable information assurance (IA) requirements
517	Develop and document requirements, capabilities, and constraints for design procedures and processes
528	Develop cost estimates for future new or modified system(s)
669	Integrate and align information security and/or information assurance (IA) policies to ensure system analysis meets security requirements
700	Manage information technology (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
789	Prepare use cases to justify the need for specific information technology (IT) solutions
863	Translate functional requirements into technical solutions
1003	Develop and document supply chain risks for critical system elements, as appropriate



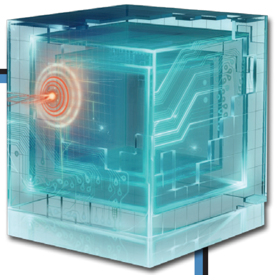
SYSTEMS REQUIREMENTS PLANNING

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.

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 encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	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 the Security Assessment and Authorization (SA&A) process	Information Assurance
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
64	Knowledge of information security systems engineering principles	Information Systems/Network Security
65	Knowledge of information theory	Mathematical Reasoning

NEXT PAGE | PREVIOUS PAGE



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.

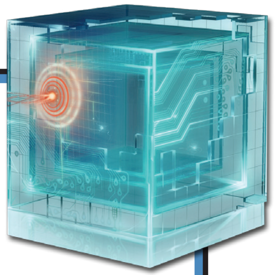
TASK | KSA

ID	Statement	Competency
68	Knowledge of information technology (IT) architectural concepts and frameworks	Information Technology Architecture
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
101	Knowledge of process engineering concepts	Logical Systems Design
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

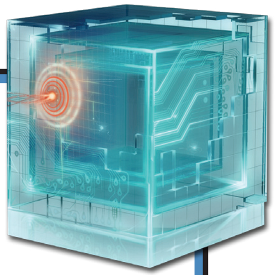
TASK | KSA

ID	Statement	Competency
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., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
143	Knowledge of the organization’s enterprise information technology (IT) goals and objectives	Enterprise Architecture
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information 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
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
229	Skill in using incident handling methodologies	Incident Management

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

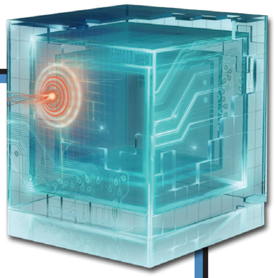
TASK | KSA

ID	Statement	Competency
911	Ability to interpret and translate customer requirements into operational cyber actions	Requirements Analysis
1002	Skill in conducting audits or reviews of technical systems	Information Technology Performance Assessment
1004	Knowledge of critical information technology (IT) procurement requirements	Contracting/Procurement
1005	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)	Contracting/Procurement
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



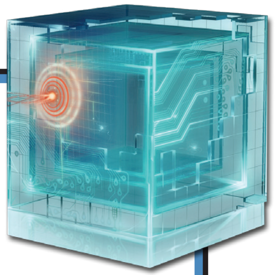
SECURELY PROVISION

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 information technology (IT).

TASK KSA

ID	Statement
412	Analyze the results of end-to-end testing (e.g., software, hardware, transport, seams, interfaces)
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 interoperability testing on systems exchanging electronic information with systems of other organizations
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
951	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated
1006	Create auditable evidence of security measures



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 information technology (IT).

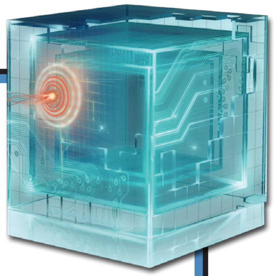
TASK | KSA

ID	Statement	Competency
22	Knowledge of computer networking fundamentals	Infrastructure Design
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
83	Knowledge of network hardware devices and functions	Hardware
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 the 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
220	Skill in systems integration testing	Systems Testing and Evaluation
239	Skill in writing test plans	Systems Testing and Evaluation
904	Knowledge of interpreted and compiled computer languages	Computer Languages

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



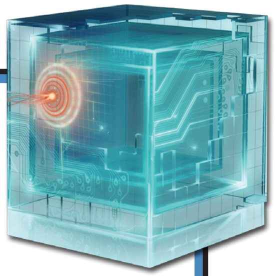
SECURELY PROVISION

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 information technology (IT).

TASK KSA

ID	Statement	Competency
950	Skill in evaluating test plans for applicability and completeness	Systems Testing and Evaluation
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

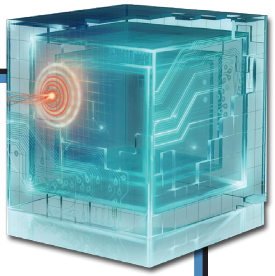
TASK | KSA

ID	Statement
416	Analyze design constraints, trade-offs, and detailed system and security designs to identify necessary 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 or theoretical models
457	Conduct Privacy Impact Assessments (PIA) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII)
494	Design and develop information assurance (IA) or IA-enabled products
495	Design and develop secure interface specifications between interconnected systems
496	Design, develop, integrate, and update system security measures (including policies and requirements) that provide confidentiality, integrity, availability, authentication, and non-repudiation
500	Design hardware, operating systems, and software applications to adequately address information assurance (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
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 testing prior to systems entering a production environment

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

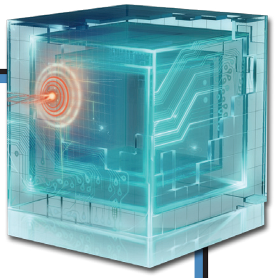
TASK | KSA

ID	Statement
542	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed
547	Develop specific information assurance (IA) countermeasures and risk mitigation strategies for systems and/or applications
626	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements
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)
632	Identify and prioritize essential system functions or sub-systems, as may be necessary to support essential capabilities or business functions; in the event of system failure or system recovery, observe and adhere to overall system requirements for continuity and availability
648	Identify, assess, and recommend information assurance (IA) or IA-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements
659	Implement security designs for new or existing system(s)
662	Incorporate information assurance (IA) vulnerability solutions into system designs (e.g., IA vulnerability alerts)
737	Perform an information security risk assessment and design security countermeasures to mitigate identified risks
766	Perform security reviews and identify security gaps in security architecture
770	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) 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 Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



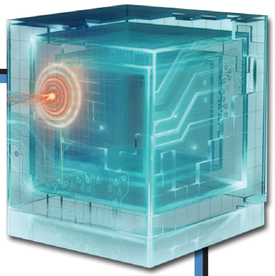
SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK | KSA

ID	Statement
850	Store, retrieve, and manipulate data for analysis of system capabilities and requirements
856	Provide support to security/certification test and evaluation activities
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
997	Design and develop key management functions (as related to information assurance [IA])
998	Analyze user needs and requirements to plan and conduct system security development
999	Develop information assurance (IA) designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information [SCI])
1000	Ensure that security design and information assurance (IA) development activities are properly documented, providing a functional description of security implementation, and updated as necessary



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

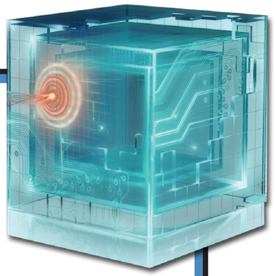
TASK | KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
8	Knowledge of access authentication methods	Identity Management
21	Knowledge of computer algorithms	Mathematical Reasoning
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's 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
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 (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
64	Knowledge of information security systems engineering principles	Information Systems/Network Security
65	Knowledge of information theory	Mathematical Reasoning

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURELY PROVISION

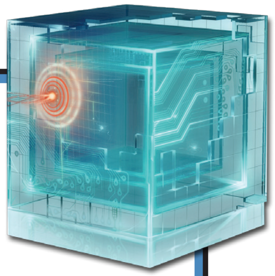
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK | KSA

ID	Statement	Competency
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) 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, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
101	Knowledge of process engineering concepts	Logical Systems Design

NEXT PAGE | PREVIOUS PAGE



SECURELY PROVISION

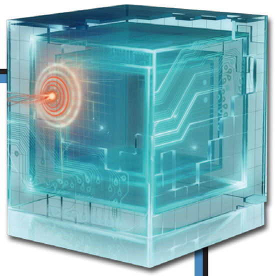
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK KSA

ID	Statement	Competency
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
118	Knowledge of software development models (e.g., waterfall model, spiral model)	Software Engineering
119	Knowledge of software engineering	Software Engineering
121	Knowledge of structured analysis principles and methods	Logical Systems Design
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., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
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
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 (IA) principles and tenets	Information Assurance
180	Skill in designing the integration of hardware and software solutions	Systems Integration
191	Skill in developing and applying security system access controls	Identity Management

NEXT PAGE | PREVIOUS PAGE



SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK | KSA

ID	Statement	Competency
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
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
904	Knowledge of interpreted and compiled computer languages	Computer Languages
1002	Skill in conducting audits or reviews of technical systems	Information Technology Performance Assessment
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

NEXT PAGE | PREVIOUS PAGE

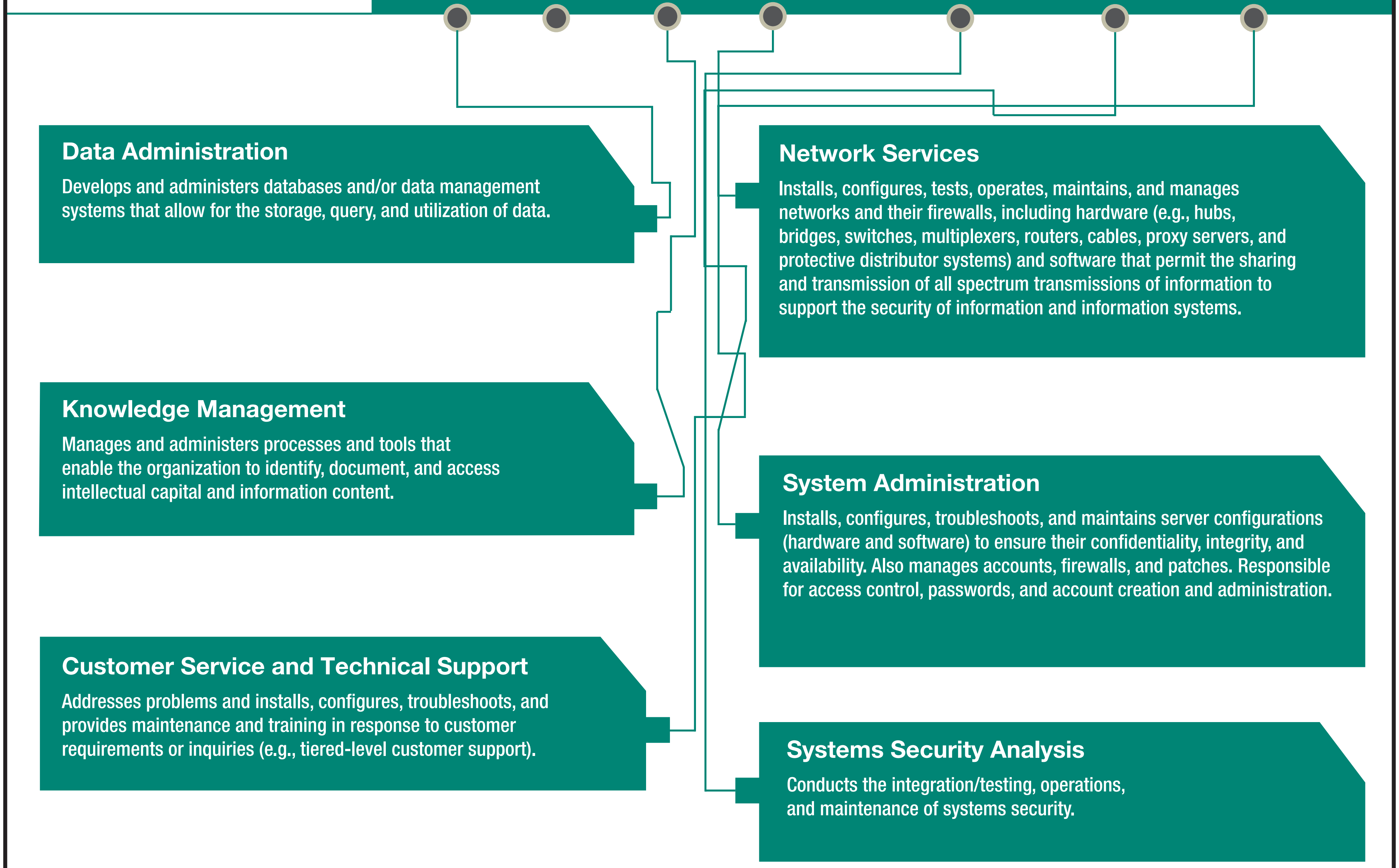
Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

OPERATE AND MAINTAIN

Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (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.

Knowledge Management

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

Customer Service and Technical Support

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

Network Services

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

System Administration

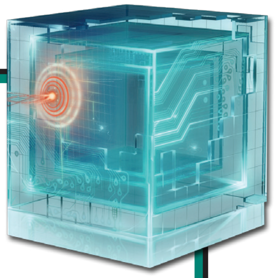
Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Systems Security Analysis

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

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



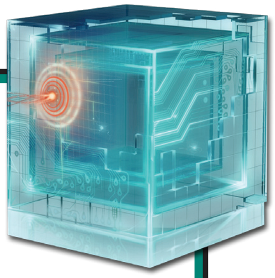
OPERATE AND MAINTAIN

DATA ADMINISTRATION

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

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
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 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.

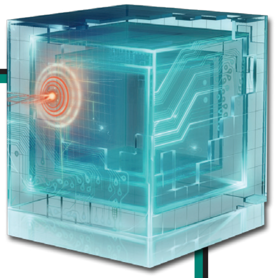
TASK | KSA

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
44	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	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 Structured Query Language (SQL)	Database Management Systems
120	Knowledge of sources, characteristics, and uses of the organization’s data assets	Data Management
137	Knowledge of the characteristics of physical and virtual data storage media	Data Management
152	Skill in allocating storage capacity in the design of data management systems	Database Administration
166	Skill in conducting queries and developing algorithms to analyze data structures	Database Management Systems
178	Skill in designing databases	Database Administration
186	Skill in developing data dictionaries	Data Management
187	Skill in developing data models	Modeling and Simulation

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

DATA ADMINISTRATION

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

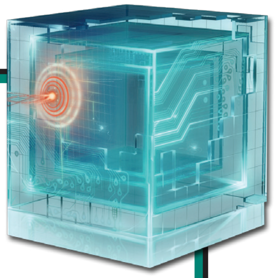
TASK KSA

ID	Statement	Competency
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
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

KNOWLEDGE MANAGEMENT

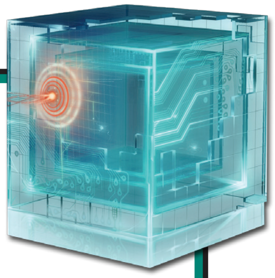
Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

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 information technology (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 information technology (IT) systems
814	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

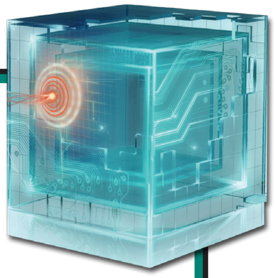
TASK | KSA

ID	Statement	Competency
5	Ability to match the appropriate knowledge repository technology for a given application or environment	Knowledge Management
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
77	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
134	Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs)	Technology Awareness
135	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines)	Data Management
136	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint)	Technology Awareness
163	Skill in conducting information searches	Computer Skills
164	Skill in conducting knowledge mapping (i.e., map of knowledge repositories)	Knowledge Management
223	Skill in the measuring and reporting of intellectual capital	Knowledge Management
230	Skill in using knowledge management technologies	Knowledge Management
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
907	Skill in data mining techniques	Data Management
910	Knowledge of database theory	Data Management

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

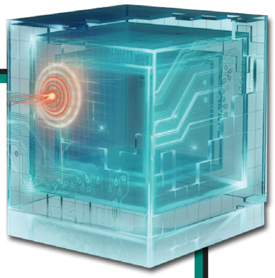
TASK | KSA

ID	Statement	Competency
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



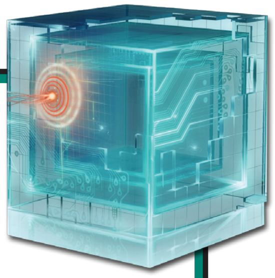
OPERATE AND MAINTAIN

CUSTOMER SERVICE AND TECHNICAL SUPPORT

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

TASK KSA

ID	Statement
428	Assist in the execution of disaster recovery and continuity of operations plans
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
695	Manage accounts, network rights, and access to systems and equipment
698	Manage inventory of information technology (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 and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

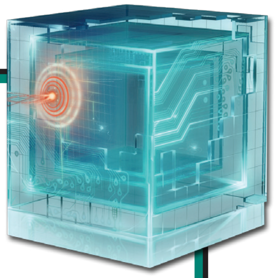
TASK KSA

ID	Statement	Competency
7	Knowledge of “knowledge base” capabilities for 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 and continuity of operations plans	Incident Management
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
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
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
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage)	Computers and Electronics

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

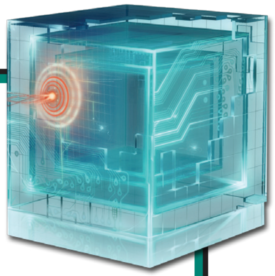
CUSTOMER SERVICE AND TECHNICAL SUPPORT

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

TASK | KSA

ID	Statement	Competency
281	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs])	Hardware
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



OPERATE AND MAINTAIN

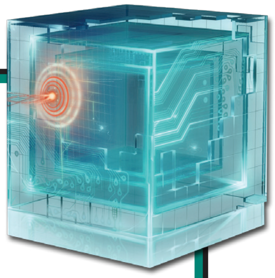
NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

TASK KSA

ID	Statement
462	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling)
522	Develop and implement network backup and recovery procedures
555	Diagnose network connectivity problems
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., Internetwork Operating System [IOS], firmware)
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

Data Administration | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis
Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

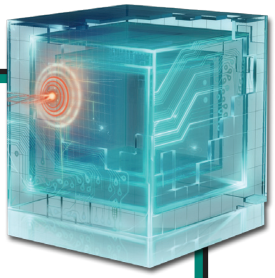
NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

TASK | KSA

ID	Statement	Competency
12	Knowledge of communication methods, principles, and concepts (e.g., cryptography, dual hubs, time multiplexers) 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
41	Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways	Infrastructure Design
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management	Infrastructure Design
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
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
133	Knowledge of telecommunications concepts	Telecommunications

NEXT PAGE | PREVIOUS PAGE



OPERATE AND MAINTAIN

NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

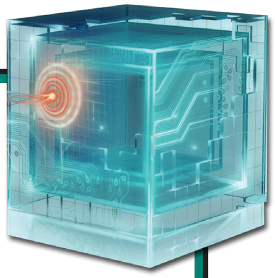
TASK | KSA

ID	Statement	Competency
148	Knowledge of Virtual Private Network (VPN) security	Encryption
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 network security practices	Information Systems/Network Security
207	"Skill in installing, configuring, and troubleshooting Local Area Network (LAN) and	
231	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)	Network Management
234	Skill in using sub-netting tools	Infrastructure Design
261	Knowledge of basic concepts, terminology, and operations of a wide range of communications media (e.g., computer and telephone networks, satellite, fiber, wireless)	Telecommunications
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup)	Infrastructure Design
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN])	Telecommunications
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)	Operating Systems
891	Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers)	Configuration Management
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

NETWORK SERVICES

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., 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.

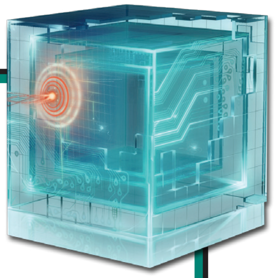
TASK | KSA

ID	Statement	Competency
900	Knowledge of web filtering technologies	Web Technology
901	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, Voice over Internet Protocol [VoIP], Instant Messenger [IM], web forums, direct video broadcasts)	Network Management
902	"Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fidelity [Wi-Fi],	
903	Knowledge of Wireless Fidelity (Wi-Fi)	Network Management
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management
989	Knowledge of Voice over Internet Protocol (VoIP)	Telecommunications
990	Knowledge of the common attack vectors on the network layer	Computer Network Defense
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



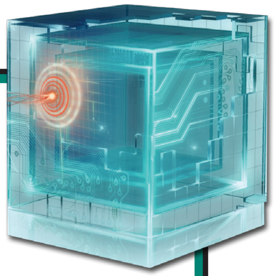
OPERATE AND MAINTAIN

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.

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 organizational standards, business rules, and needs
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 according to organizational policies
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
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.

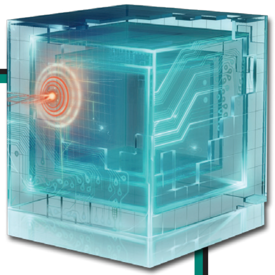
TASK | KSA

ID	Statement	Competency
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management	Infrastructure Design
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	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 information technology (IT) architecture	Information Technology Architecture
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly	Systems Life Cycle
148	Knowledge of Virtual Private Network (VPN) security	Encryption

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

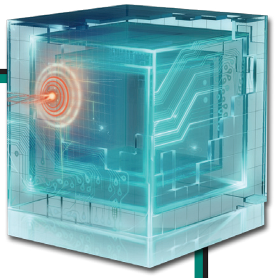
TASK | KSA

ID	Statement	Competency
167	Skill in conducting server planning, management, and maintenance	Network Management
170	Skill in configuring and optimizing software	Software Engineering
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
219	Skill in system administration for Unix/Linux operating systems	Operating Systems
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)	Operating Systems
287	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT])	Operating Systems
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)	Computer Languages
344	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems
386	Skill in using virtual machines	Operating Systems

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

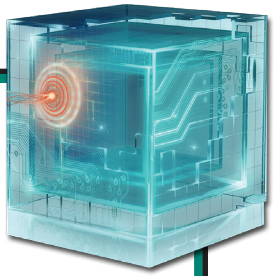
TASK | KSA

ID	Statement	Competency
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)	Configuration Management
986	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)	Identity Management
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

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

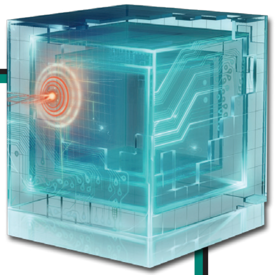
TASK | KSA

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 organization's 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 systems security 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 information assurance-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 plans
652	Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines
653	Implement security designs and approaches to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed
660	Implement specific information assurance (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

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

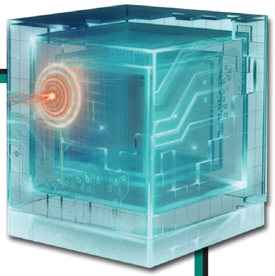
SYSTEMS SECURITY ANALYSIS

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

TASK | KSA

ID	Statement
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 senior leader 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 information assurance (IA) testing of developed applications and/or systems
767	Perform security reviews and identify security gaps in security architecture, resulting in recommendations for inclusion into the risk mitigation strategy
782	Plan and recommend modifications or adjustments based on exercise results or system environment
795	Properly document all systems security implementation, operations, and maintenance activities and update as necessary
806	Provide information assurance (IA) guidance to leadership
809	Provide input to the Risk Management Framework (RMF) 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
938	Ensure Recovery and Continuity plans are executable in the system operational environment

NEXT PAGE | PREVIOUS PAGE



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

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

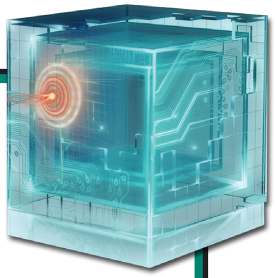
TASK | KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
18	Knowledge of circuit analysis	Computers and Electronics
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	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
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
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
65	Knowledge of information theory	Mathematical Reasoning
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SYSTEMS SECURITY ANALYSIS

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

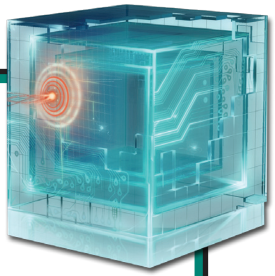
TASK | KSA

ID	Statement	Competency
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, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	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
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
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

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

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

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

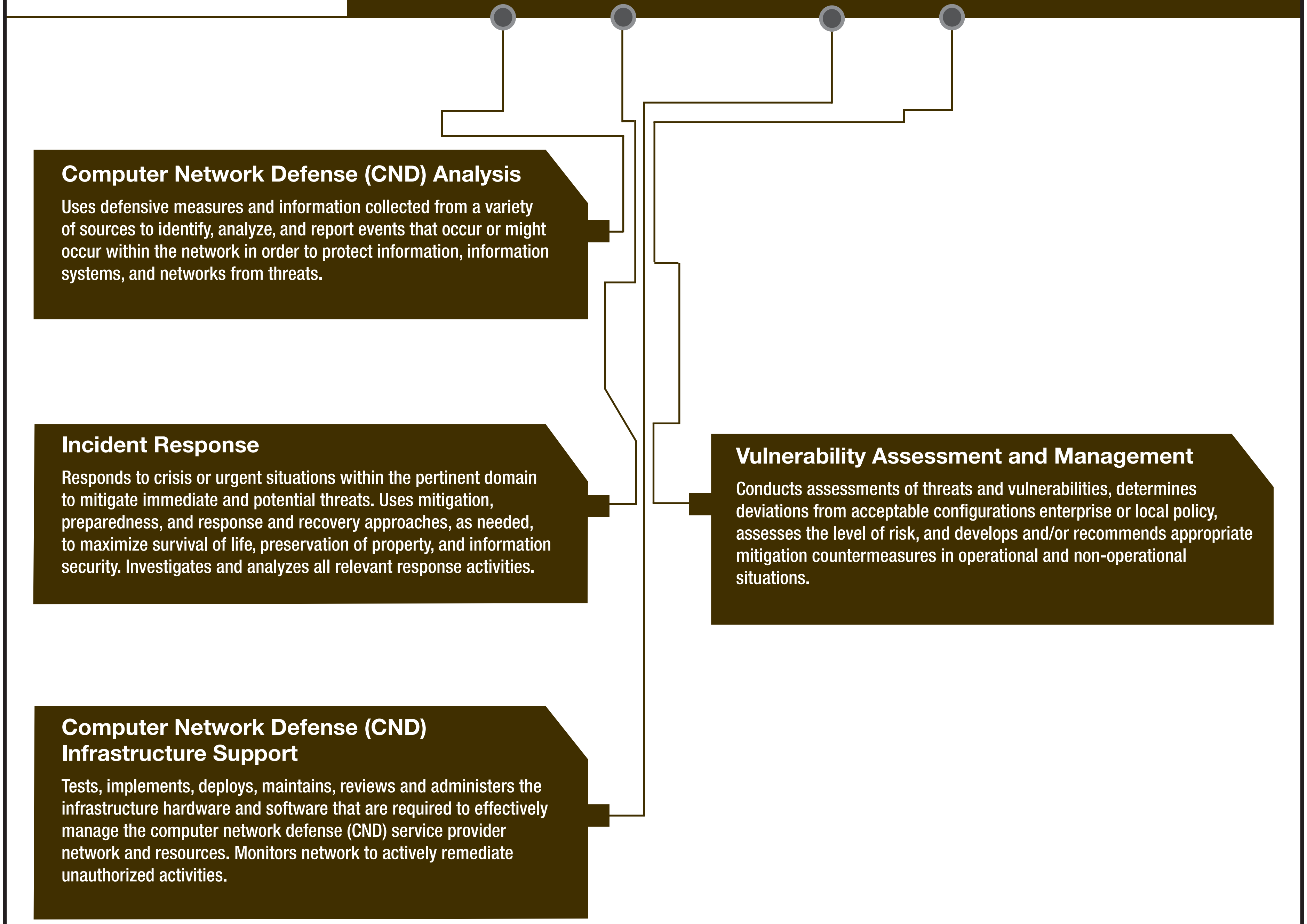
TASK | KSA

ID	Statement	Competency
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
179	Skill in designing security controls based on information assurance (IA) principles and tenets	Information Assurance
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
191	Skill in developing and applying security system access controls	Identity Management
199	Skill in evaluating the adequacy of security designs	Vulnerabilities Assessment
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

THE NATIONAL CYBERSECURITY
WORKFORCE
FRAMEWORK

PROTECT AND DEFEND

Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.



Computer Network Defense (CND) Analysis

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.

Incident Response

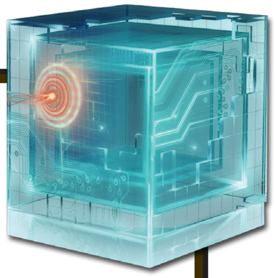
Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes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

Computer Network Defense (CND) Infrastructure Support

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

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.



PROTECT AND DEFEND

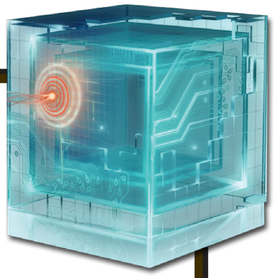
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

TASK | KSA

ID	Statement
427	Develop content for computer network defense (CND) tools
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
472	Coordinate with enterprise-wide computer network defense (CND) staff to validate network alerts
716	Monitor external data sources (e.g., computer network defense [CND] vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the enterprise
723	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment
745	Perform computer network defense (CND) trend analysis and reporting
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 (CND) practices
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
956	Provide timely detection, identification, and alerts of possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents and events from benign activities
958	Use computer network defense (CND) tools for continual monitoring and analysis of system activity to identify malicious activity
959	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, and effects on system and information
961	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)

NEXT PAGE | PREVIOUS PAGE



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

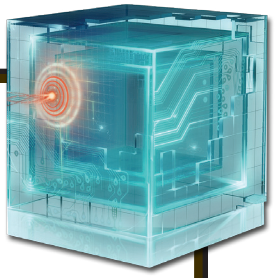
TASK KSA

ID	Statement
1010	Determine appropriate course of action in response to identified and analyzed anomalous network activity
1102	Conduct tests of information assurance (IA) safeguards in accordance with established test plans and procedures
1103	Determine tactics, techniques, and procedures (TTPs) for intrusion sets
1104	Examine network topologies to understand data flows through the network
1105	Recommend computing environment vulnerability corrections
1107	Identify and analyze anomalies in network traffic using metadata
1108	Conduct research, analysis, and correlation across a wide variety of all source data sets (e.g., indications and warnings)
1109	Validate Intrusion Detection System (IDS) alerts against network traffic using packet analysis tools
1110	Triage malware
1111	Identify applications and operating systems of a network device based on network traffic
1112	Reconstruct a malicious attack or activity based on network traffic
1113	Identify network mapping and operating system fingerprinting activities

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



PROTECT AND DEFEND

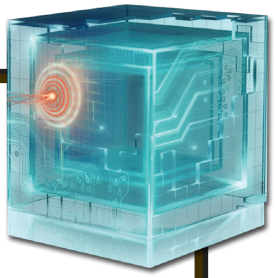
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

TASK | KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
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
59	Knowledge of Intrusion Detection System (IDS) tools and applications	Computer Network Defense
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and 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
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness

NEXT PAGE | PREVIOUS PAGE



PROTECT AND DEFEND

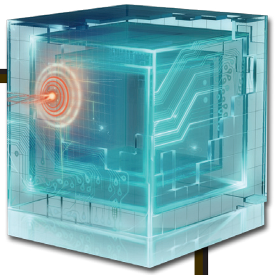
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

TASK | KSA

ID	Statement	Competency
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
102	Knowledge of programming language structures and logic	Computer Languages
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
110	Knowledge of security management	Information Assurance
115	Knowledge of content development	Computer Network Defense
138	Knowledge of the computer network defense (CND) service provider reporting structure and processes within one's own organization	Information Systems/Network Security
148	Knowledge of Virtual Private Network (VPN) security	Encryption
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
165	Skill in conducting open source research for troubleshooting novel client-level problems	Knowledge Management
175	Skill in developing and deploying signatures	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

TASK | KSA

ID	Statement	Competency
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
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	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
270	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities)	Computer Network Defense
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup)	Infrastructure Design
277	Knowledge of defense-in-depth principles and network security architecture	Computer Network Defense
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN])	Telecommunications
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)	Operating Systems
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)	Computer Languages
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)	Operating Systems
353	Skill in collecting data from a variety of computer network defense resources	Computer Network Defense

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

PROTECT AND DEFEND

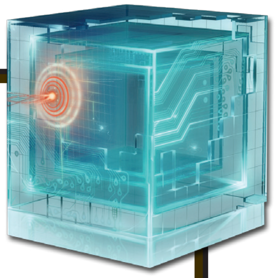
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

TASK KSA

ID	Statement	Competency
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
912	Knowledge of collection management processes, capabilities, and limitations	Configuration Management
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
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management
990	Knowledge of the common attack vectors on the network layer	Computer Network Defense
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1007	Skill in data reduction	Data Management
1008	Knowledge of how to troubleshoot basic systems and identify operating systems-related issues	Operating Systems
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) ANALYSIS

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.

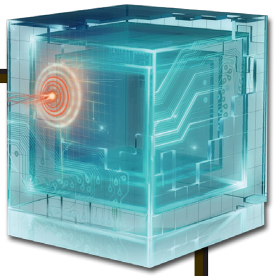
TASK | KSA

ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1114	Knowledge of encryption methodologies	Cryptography
1115	Skill in reading Hexadecimal data	Computer Languages
1116	Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode)	Computer Languages
1117	Skill in utilizing virtual networks for testing	Operating Systems
1118	Skill in reading and interpreting signatures (e.g., Snort)	Information Systems/Network Security
1119	Knowledge of signature implementation impact	Information Systems/Network Security
1120	Ability to interpret and incorporate data from multiple tool sources	Data Management
1121	Knowledge of Windows/Unix ports and services	Operating Systems

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

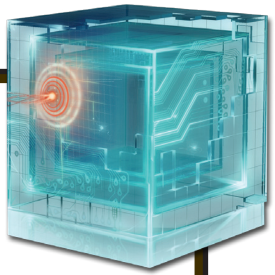
TASK | KSA

ID	Statement
470	Coordinate with and provide expert technical support to enterprise-wide computer network defense (CND) technicians to resolve CND incidents
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
716	Monitor external data sources (e.g., computer network defense [CND] vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND 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 [IDS] logs) to identify possible threats to network security
741	Perform command and control functions in response to incidents
743	Perform computer network defense (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time computer network defense (CND) 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
861	Track and document computer network defense (CND) incidents from initial detection through final resolution
882	Write and publish computer network defense (CND) guidance and reports on incident findings to appropriate constituencies
961	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

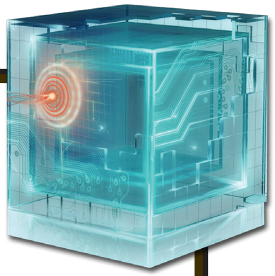
TASK KSA

ID	Statement
1030	Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise
1031	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis
Incident Response
Computer Network Defense (CND) Infrastructure Support
Vulnerability Assessment and Management

Home
Using This Document
Sample Job Titles
Securely Provision
Operate and Maintain
Protect and Defend
Investigate
Collect and Operate
Analyze
Oversight and Development



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.

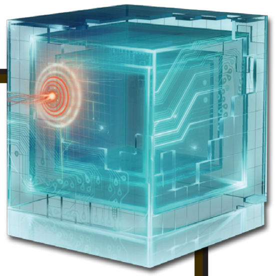
TASK | KSA

ID	Statement	Competency
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
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
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
153	Skill in handling malware	Computer Network Defense
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



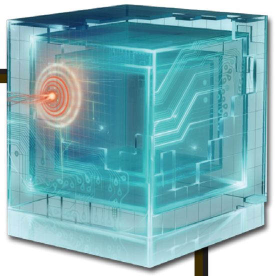
PROTECT AND DEFEND

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.

TASK | KSA

ID	Statement	Competency
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	Computer Network Defense
897	Skill in performing damage assessments	Information Assurance
923	Knowledge of security event correlation tools	Information Systems/Network Security
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1029	Knowledge of malware analysis concepts and methodology	Computer Network Defense
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security



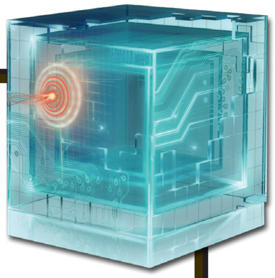
PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) INFRASTRUCTURE SUPPORT

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

TASK KSA

ID	Statement
393	Administer computer network defense (CND) test bed(s), and test and evaluate new CND applications, rules/signatures, access controls, and configurations of CND service provider managed platforms
471	Coordinate with Computer Network Defense (CND) Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized computer network defense (CND) applications
481	Create, edit, and manage changes to network access control lists on specialized computer network defense (CND) systems (e.g., firewalls and intrusion prevention systems)
643	Identify potential conflicts with implementation of any computer network defense (CND) tools within the CND service provider area of responsibility (e.g., tool/signature testing and optimization)
654	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for specialized computer network defense (CND) systems within the enterprise, and document and maintain records for them
769	Perform system administration on specialized computer network defense (CND) applications and systems (e.g., anti-virus, audit/remediation) or Virtual Private Network [VPN] devices, to include installation, configuration, maintenance, and backup/restoration
960	Assist in identifying, prioritizing, and coordinating the protection of critical computer network defense (CND) infrastructure and key resources



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) INFRASTRUCTURE SUPPORT

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

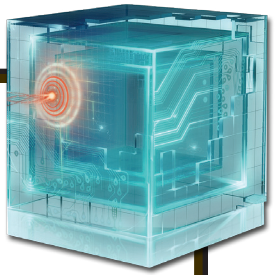
TASK | KSA

ID	Statement	Competency
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 Intrusion Detection System (IDS) tools and applications	Computer Network Defense
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
146	Knowledge of the types of Intrusion Detection System (IDS) hardware and software	Computer Network Defense
148	Knowledge of Virtual Private Network (VPN) security	Encryption

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



PROTECT AND DEFEND

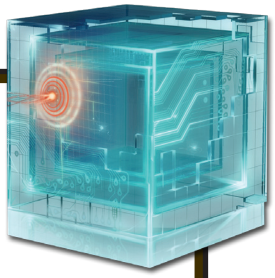
COMPUTER NETWORK DEFENSE (CND) INFRASTRUCTURE SUPPORT

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

TASK | KSA

ID	Statement	Competency
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
227	Skill in tuning sensors	Computer Network Defense
229	Skill in using incident handling methodologies	Incident Management
237	Skill in using Virtual Private Network (VPN) devices and encryption	Encryption
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense
900	Knowledge of web filtering technologies	Web Technology
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
989	Knowledge of Voice over Internet Protocol (VoIP)	Telecommunications
1011	Knowledge of processes for reporting network security related incidents	Security
1012	Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels	Internal Controls
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications

NEXT PAGE | PREVIOUS PAGE



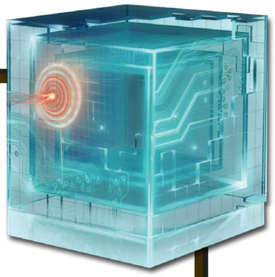
VULNERABILITY ASSESSMENT AND MANAGEMENT

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

TASK KSA

ID	Statement
411	Analyze organization's computer network defense (CND) policies and configurations and evaluate compliance with regulations and organizational directives
448	Conduct and/or support authorized penetration testing on enterprise network assets
685	Maintain deployable computer network defense (CND) audit toolkit (e.g., specialized computer network defense [CND] software/ hardware) to support computer network defense (CND) audit missions
692	Maintain knowledge of applicable computer network defense (CND) policies, regulations, and compliance documents specifically related to computer network defense (CND) auditing
784	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions
939	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance Countermeasure Reviews [TSCM], TEMPEST[1] countermeasure reviews)
940	Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure)
941	Assist with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)

[1] TEMPEST is a codename and not an acronym



PROTECT AND DEFEND

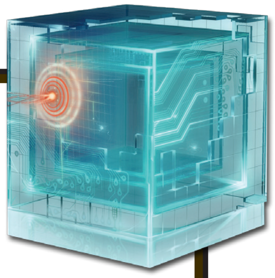
VULNERABILITY ASSESSMENT AND MANAGEMENT

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

TASK / KSA

ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing 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
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
102	Knowledge of programming language structures and logic	Computer Languages
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE



PROTECT AND DEFEND

VULNERABILITY ASSESSMENT AND MANAGEMENT

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

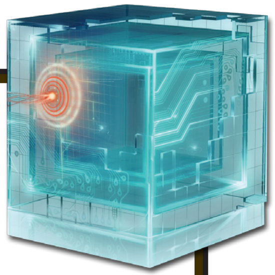
TASK | KSA

ID	Statement	Competency
115	Knowledge of content development	Computer Network Defense
123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment
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 using appropriate tools (e.g., Wireshark, tcpdump)	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
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
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense

NEXT PAGE | PREVIOUS PAGE

Computer Network Defense (CND) Analysis | Incident Response | Computer Network Defense (CND) Infrastructure Support | Vulnerability Assessment and Management

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



PROTECT AND DEFEND

VULNERABILITY ASSESSMENT AND MANAGEMENT

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

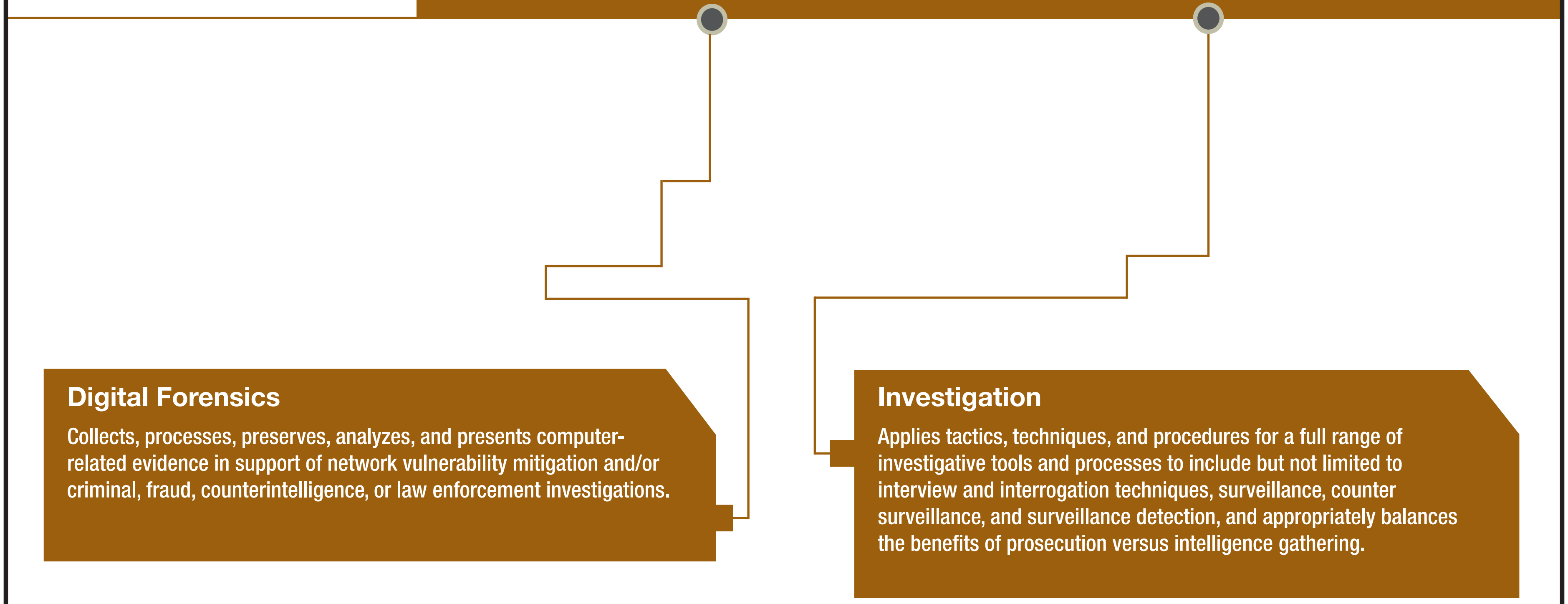
TASK KSA

ID	Statement	Competency
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE

INVESTIGATE

Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.



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.

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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

INVESTIGATE

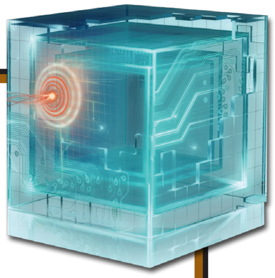
DIGITAL FORENSICS

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

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 (CND) 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 (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, compact discs (CDs), personal digital assistants (PDAs), mobile phones, global positioning satellite devices (GPSs), and all tape formats
482	Decrypt seized data using technical means
541	Provide technical summary of findings in accordance with established reporting procedures
564	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports)
573	Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence
613	Examine recovered data for information of relevance to the issue at hand
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
743	Perform computer network defense (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making 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

NEXT PAGE | PREVIOUS PAGE



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.

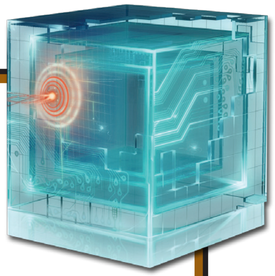
TASK KSA

ID	Statement
753	Perform hash comparison against established database
758	Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)
759	Perform timeline analysis
768	Perform static media analysis
771	Perform tier 1, 2, and 3 malware 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
868	Use data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost) to extract data for further analysis
870	Use network monitoring tools to capture and analyze network traffic associated with malicious activity
871	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence
882	Write and publish computer network defense (CND) guidance and reports on incident findings to appropriate constituencies
944	Conduct cursory binary analysis
1081	Perform virus scanning on digital media
1082	Perform file system forensic analysis

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



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.

TASK KSA

ID	Statement
1083	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive)
1084	Perform static malware analysis
1085	Utilize deployable forensics toolkit to support operations as necessary

Sub-Specialty Area: Digital Forensics (Law Enforcement/Counterintelligence)

The following tasks, combined with all of the parent tasks/KSAs comprise the entirety of the tasks/KSAs associated with this sub-specialty area.

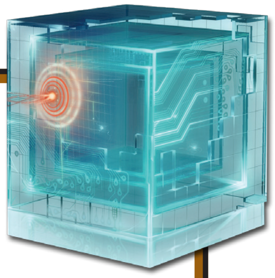
Digital Forensics (LE/CI) – Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

ID	Statement
429	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
620	Employ IT systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
622	Formulate a strategy to ensure chain of custody is maintained in such a way that the evidence is not altered (ex: phones/PDAs need a power source, hard drives need protection from shock and strong magnetic fields)
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

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



INVESTIGATE

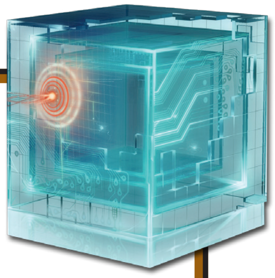
DIGITAL FORENSICS

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

TASK KSA

ID	Statement	Competency
24	Knowledge of basic concepts and practices of processing digital forensic data	Data Management
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	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
90	Knowledge of operating systems	Operating Systems
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
113	Knowledge of server and client operating systems	Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques	Computer Forensics
139	Knowledge of the common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications	Infrastructure Design
193	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans	Information Assurance
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE



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.

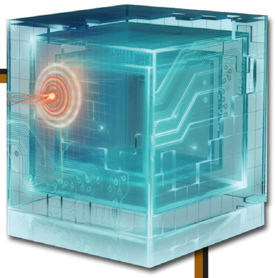
TASK KSA

ID	Statement	Competency
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage)	Computers and Electronics
287	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT])	Operating Systems
290	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)	Forensics
294	Knowledge of hacking methodologies in Windows or Unix/Linux environment	Surveillance
302	Knowledge of investigative implications of hardware, operating systems, and network technologies	Computer Forensics
310	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence)	Criminal Law
316	Knowledge of processes for collecting, 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 webmail 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

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



INVESTIGATE

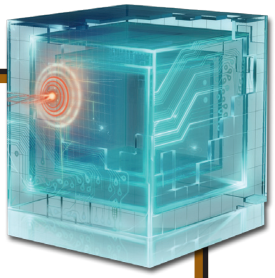
DIGITAL FORENSICS

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

TASK | KSA

ID	Statement	Competency
360	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics)	Computer Forensics
364	Skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files)	Operating Systems
369	Skill in collecting, 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, Forensic Tool Kit [FTK])	Computer Forensics
386	Skill in using virtual machines	Operating Systems
389	Skill in physically disassembling personal computers (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	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems)	Computer Forensics
908	Ability to decrypt digital data collections	Computer Forensics
923	Knowledge of security event correlation tools	Information Systems/Network Security
982	Knowledge of electronic evidence law	Criminal Law
983	Knowledge of legal rules of evidence and court procedure	Criminal Law

NEXT PAGE | PREVIOUS PAGE



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.

TASK KSA

ID	Statement	Competency
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1086	Knowledge of data carving tools and techniques (e.g., Foremost)	Computer Forensics
1087	Skill in deep analysis of captured malicious code (e.g., malware forensics)	Computer Network Defense
1088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump)	Computer Languages
1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment
1091	Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5])	Data Management
1092	Knowledge of anti-forensics tactics, techniques, and procedures (TTPS)	Computer Forensics
1093	Knowledge of common forensic tool configuration and support applications (e.g., VMWare, Wireshark)	Computer Forensics
1094	Knowledge of debugging procedures and tools	Software Development
1095	Knowledge of how different file types can be used for anomalous behavior	Vulnerabilities Assessment

NEXT PAGE | PREVIOUS PAGE

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.

TASK KSA

ID	Statement	Competency
1096	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro)	Computer Network Defense
1097	Knowledge of virtual machine aware malware, debugger aware malware, and packing	Computer Network Defense
1098	Skill in analyzing anomalous code as malicious or benign	Computer Network Defense
1099	Skill in analyzing volatile data	Computer Forensics
1100	Skill in identifying obfuscation techniques	Computer Network Defense
1101	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures	Computer Network Defense

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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

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 of victims and witnesses and conduct interviews or interrogations of 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)
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 information of relevance to the issue at hand
620	Employ information technology (IT) 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
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration

NEXT PAGE | PREVIOUS PAGE

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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

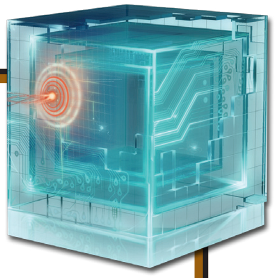
TASK | KSA

ID	Statement
637	Identify elements of proof of the crime
642	Identify outside attackers accessing the system from the 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	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

NEXT PAGE | PREVIOUS PAGE

Digital Forensics | Investigation

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



INVESTIGATE

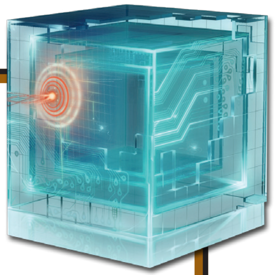
INVESTIGATION

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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

TASK | KSA

ID	Statement	Competency
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics
281	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs])	Hardware
290	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)	Forensics
310	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence)	Criminal Law
316	Knowledge of processes for collecting, 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 collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Forensics
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

NEXT PAGE | PREVIOUS PAGE



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, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

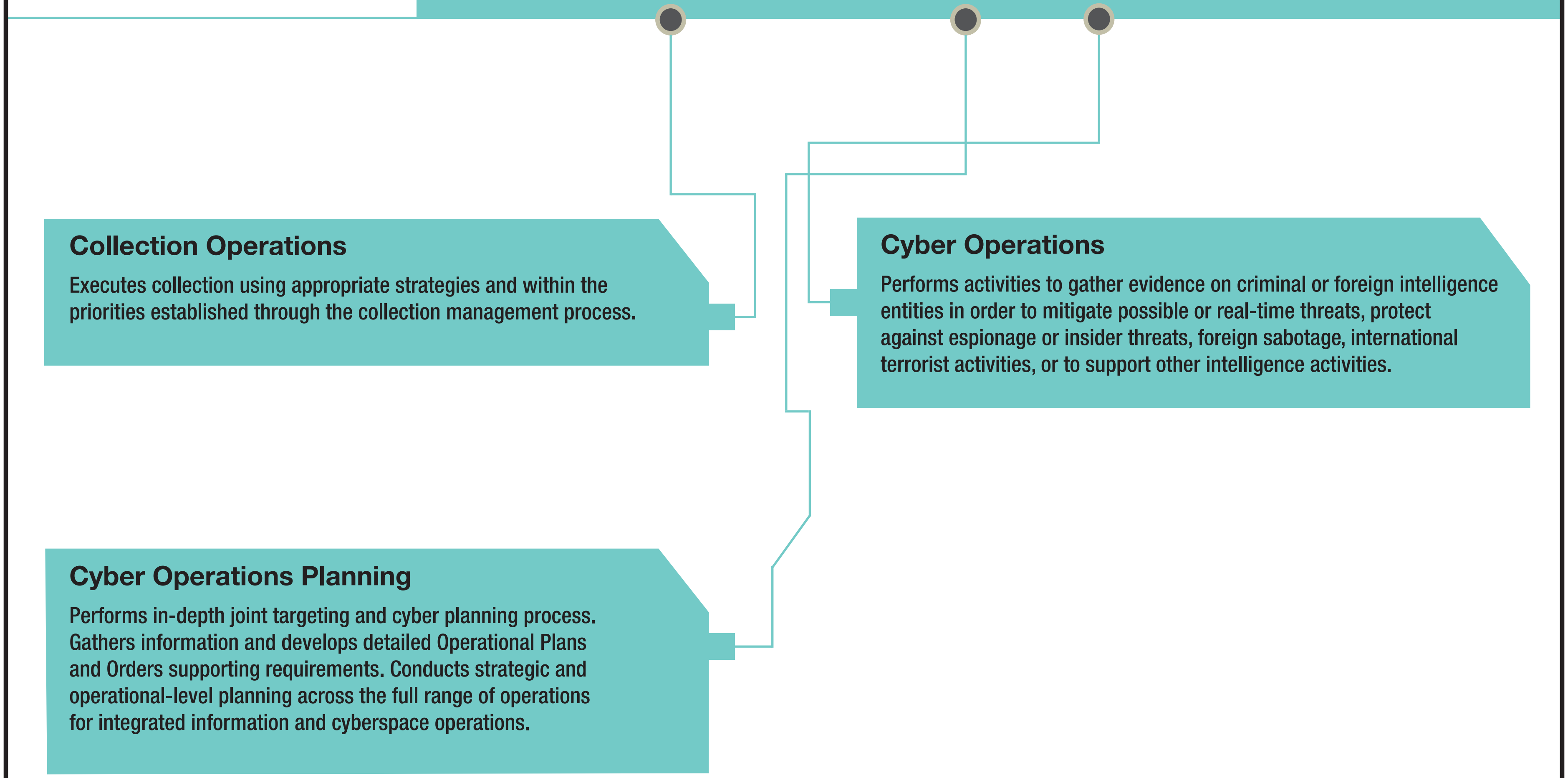
TASK | KSA

ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement

NEXT PAGE | PREVIOUS PAGE

COLLECT AND OPERATE

Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.



Collection Operations

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

Cyber Operations

Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Cyber Operations Planning

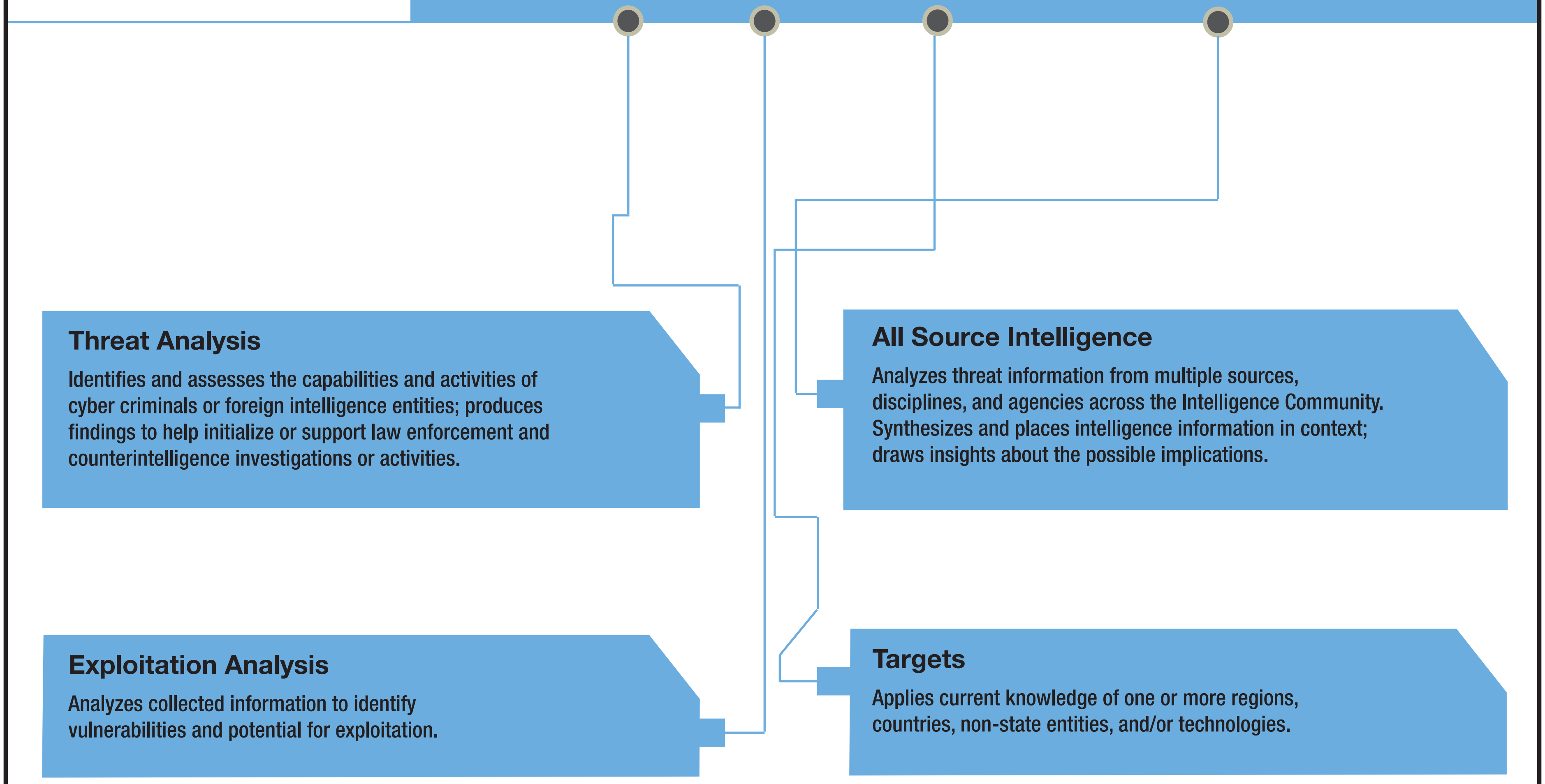
Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Due to the unique and highly specialized nature of this work, task and KSA-level content is not provided in this document for the 3 specialty areas in this category.

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

ANALYZE

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



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.

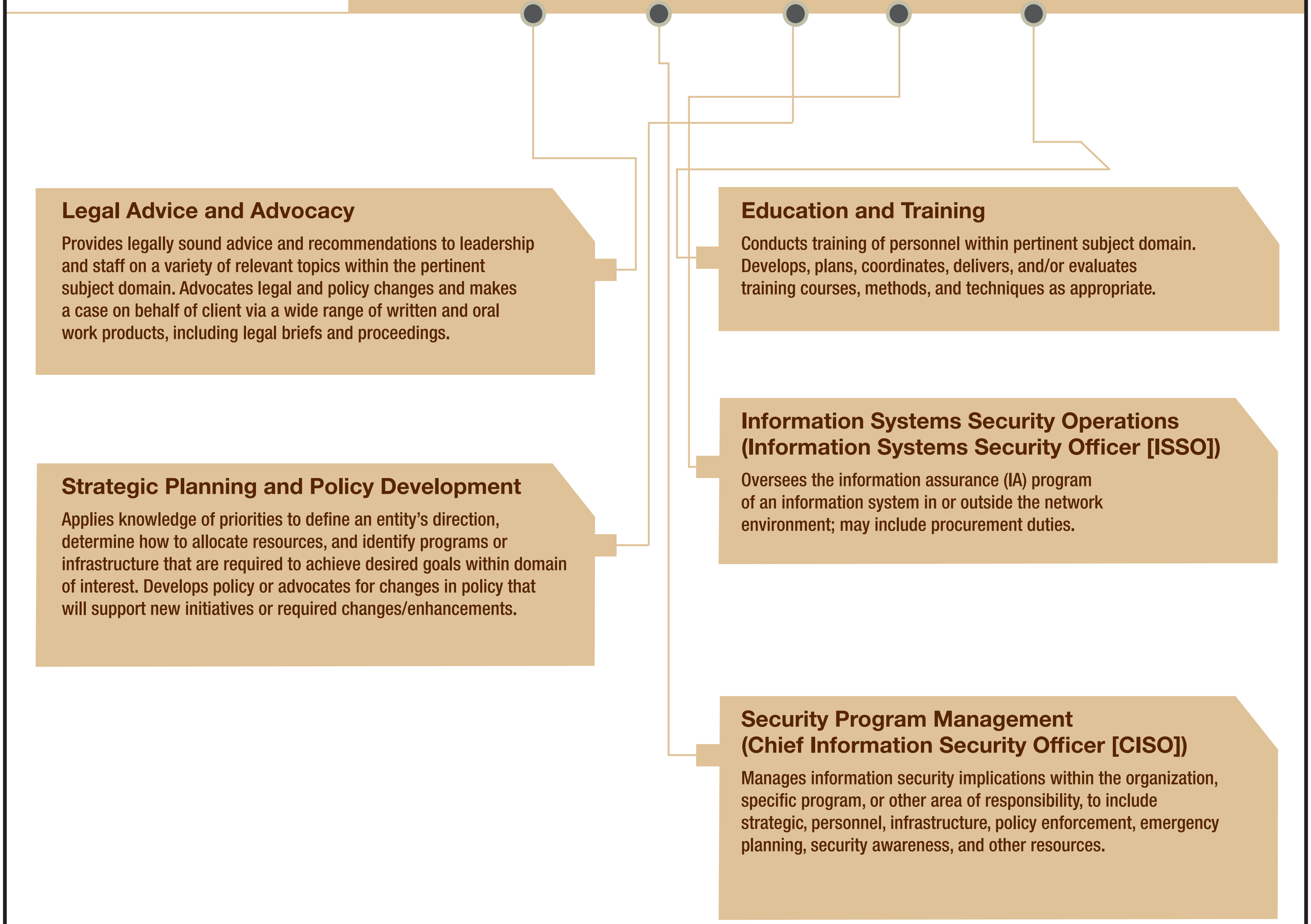
Targets

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

Due to the unique and highly specialized nature of this work, task and KSA-level content is not provided in this document for the four specialty areas in this category.

OVERSIGHT AND DEVELOPMENT

Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct 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.

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.

Education and Training

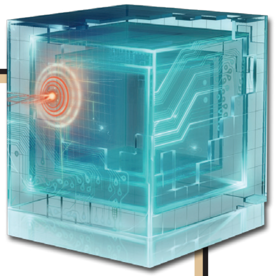
Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

Information Systems Security Operations (Information Systems Security Officer [ISSO])

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

Security Program Management (Chief Information Security Officer [CISO])

Manages 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.

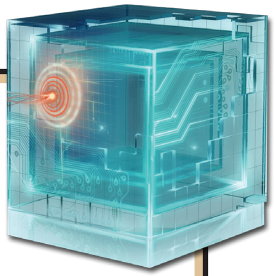


LEGAL ADVICE AND ADVOCACY

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.

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 information communication technology (ICT) 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	Evaluate the impact (e.g., 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



OVERSIGHT AND DEVELOPMENT / 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.

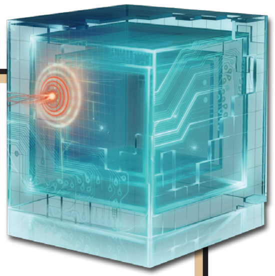
TASK | KSA

ID	Statement	Competency
27	Knowledge of cryptology	Cryptography
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
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 (e.g., requirements and priorities), dissemination practices, and legal authorities and restrictions	Organizational Awareness
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
954	Knowledge of Export Control regulations and responsible agencies for the purposes of reducing supply chain risk	Contracting/Procurement
981	Knowledge of International Traffic in Arms Regulations (ITARs) and relevance to cybersecurity	Criminal Law

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT / 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.

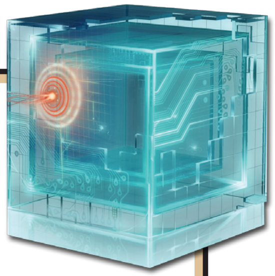
TASK KSA

ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1070	Ability to determine impact of technology trend data on laws, regulations, and/or policies	Legal, Government and Jurisprudence

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

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.

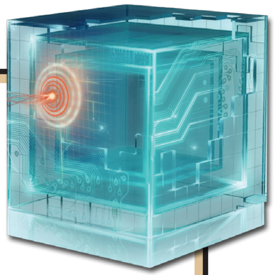
TASK KSA

ID	Statement
410	Analyze organizational information security policy
424	Assess policy needs and collaborate with stakeholders to develop policies to govern information technology (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 information technology (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 (IA) 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 information technology (IT) management, staff, and users
838	Review existing and proposed policies with stakeholders
840	Review or conduct audits of information technology (IT) programs and projects

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

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.

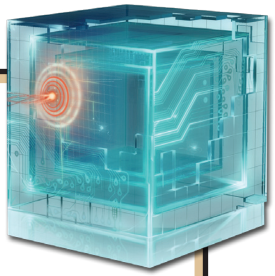
TASK KSA

ID	Statement
847	Serve on agency and interagency policy boards
854	Support the Chief Information Officer (CIO) in the formulation of information technology (IT)-related policies
884	Write information assurance (IA) policy and instructions
919	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals
946	Ensure established cybersecurity strategy is intrinsically linked to organizational mission objectives
955	Draft and publish a supply chain security/risk management policy
1023	Identify and track the status of protected information assets
1024	Apply assessment data of identified threats in decision-making
1025	Triage protected assets
1026	Oversee development and implementation of high-level control architectures
1027	Translate applicable laws, statutes, and regulatory documents and integrate into policy
1041	Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



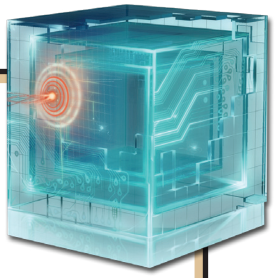
STRATEGIC PLANNING AND POLICY DEVELOPMENT

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.

TASK | KSA

ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
244	Ability to determine the validity of technology trend data	Technology Awareness
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
320	Knowledge of external organizations and academic institutions dealing with cybersecurity issues	External Awareness
336	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII])	Telecommunications
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
954	Knowledge of Export Control regulations and responsible agencies for the purposes of reducing supply chain risk	Contracting/Procurement

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

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.

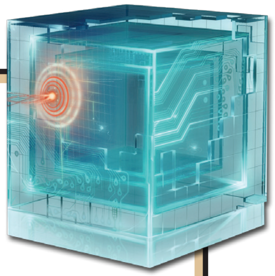
TASK | KSA

ID	Statement	Competency
1021	Knowledge of risk threat assessment	Risk Management
1022	Knowledge of the nature and function of the relevant information structure	Enterprise Architecture
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

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

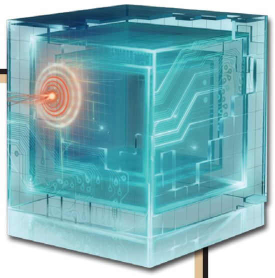
TASK | KSA

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
606	Evaluate the effectiveness and comprehensiveness of existing training programs
624	Guide employees through relevant development and training choices
778	Plan classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment
779	Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
841	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions)
842	Revise curriculum end course content based on feedback from previous training sessions

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

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

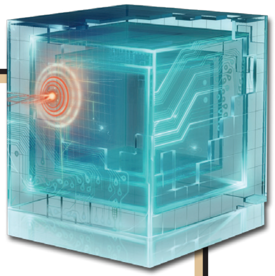
TASK KSA

ID	Statement
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
953	Coordinate with human resources to ensure job announcements are written to reflect required training, education, and/or experience

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT EDUCATION AND TRAINING

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

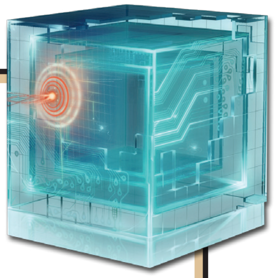
TASK KSA

ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
90	Knowledge of operating systems	Operating Systems
246	Knowledge and experience in the Instructional System Design (ISD) methodology	Multimedia Technologies
252	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools, and laws/regulations	Computer Network Defense
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage)	Computers and Electronics
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
314	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others
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

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



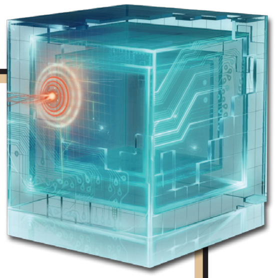
EDUCATION AND TRAINING

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

TASK KSA

ID	Statement	Competency
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
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
952	Knowledge of emerging security issues, risks, and vulnerabilities	Technology Awareness
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

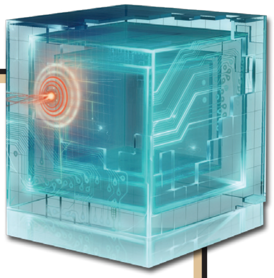
INFORMATION SYSTEMS SECURITY OPERATIONS (INFORMATION SYSTEMS SECURITY OFFICER [ISSO])

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

TASK | KSA

ID	Statement
397	Advise appropriate senior leadership or authorizing official of changes affecting the organization's information assurance (IA) posture
440	Collect and maintain data needed to meet system information assurance (IA) reporting
584	Ensure that information assurance (IA) inspections, tests, and reviews are coordinated for the network environment
585	Ensure that information assurance (IA) requirements are integrated into the continuity planning for that system and/or organization(s)
590	Ensure that protection and detection capabilities are acquired or developed using the information system security engineering approach and are consistent with organization-level information assurance (IA) architecture
598	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed
600	Evaluate cost-benefit, economic, and risk analysis in decision-making process
731	Participate in information security risk assessments during the Security Assessment and Authorization (SA&A) process
733	Participate in the development or modification of the computer environment information assurance (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 information assurance (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 information assurance (IA) requirements
852	Supervise or manage protective or corrective measures when an information assurance (IA) incident or vulnerability is discovered

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

INFORMATION SYSTEMS SECURITY OPERATIONS (INFORMATION SYSTEMS SECURITY OFFICER [ISSO])

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

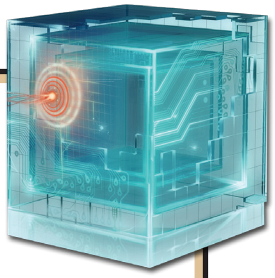
TASK | KSA

ID	Statement
869	Use federal and organization-specific published documents to manage operations of their computing environment system(s)
962	Identify security requirements specific to an information technology (IT) system in all phases of the system lifecycle
963	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
964	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals
1016	Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs)
1017	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices
1041	Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



INFORMATION SYSTEMS SECURITY OPERATIONS (INFORMATION SYSTEMS SECURITY OFFICER [ISSO])

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

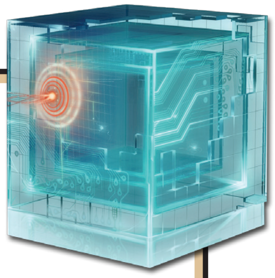
TASK | KSA

ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
37	Knowledge of disaster recovery and continuity of operations plans	Incident Management
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
77	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
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

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

INFORMATION SYSTEMS SECURITY OPERATIONS (INFORMATION SYSTEMS SECURITY OFFICER [ISSO])

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

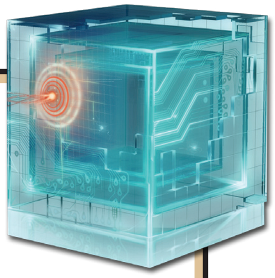
TASK | KSA

ID	Statement	Competency
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., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
143	Knowledge of the organization’s enterprise information technology (IT) goals and objectives	Enterprise Architecture
173	Skill in creating policies that reflect system security objectives	Information Systems Security Certification
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
325	Knowledge of secure acquisitions (e.g., relevant Contracting Officer’s Technical Representative [COTR] duties, secure procurement, supply chain risk management)	Contracting/Procurement
965	Knowledge of organization's risk tolerance and/or risk management approach	Risk Management
966	Knowledge of enterprise incident response program, roles, and responsibilities	Incident Management
967	Knowledge of current and emerging threats/threat vectors	Information Systems/Network Security
1004	Knowledge of critical information technology (IT) procurement requirements	Contracting/Procurement
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



OVERSIGHT AND DEVELOPMENT

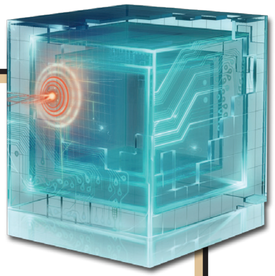
INFORMATION SYSTEMS SECURITY OPERATIONS (INFORMATION SYSTEMS SECURITY OFFICER [ISSO])

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

TASK KSA

ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

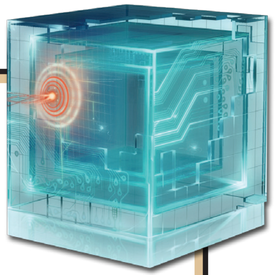
SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

TASK | KSA

ID	Statement
391	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (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 senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture
396	Advise senior management (e.g., Chief Information Officer [CIO]) on cost-benefit analysis of information security programs, policies, processes, systems, and elements
445	Communicate the value of information technology (IT) security throughout all levels of the organization's stakeholders
473	Collaborate with organizational managers to support organizational objectives
475	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance
578	Ensure security improvement actions are evaluated, validated, and implemented as required
596	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy
600	Evaluate cost-benefit, economic, and risk analysis in decision-making process
628	Identify alternative information security strategies to address organizational security objective
640	Identify information technology (IT) security program implications of new technologies or technology upgrades
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 (CND) information
676	Interpret and/or approve security requirements relative to the capabilities of new information technologies

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

SECURITY PROGRAM MANAGEMENT (CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

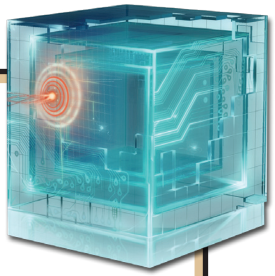
TASK | KSA

ID	Statement
677	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s information assurance (IA) program
679	Lead and align information technology (IT) security priorities with the security strategy
680	Lead and oversee information security budget, staffing, and contracting
705	Manage the monitoring of information security data sources to maintain organizational situational awareness
706	Manage the publishing of computer network defense (CND) guidance (e.g., Time Compliance Network Orders [TCNOs], concept of operations, net analyst reports) for the organization
707	Manage threat or target analysis of computer network defense (CND) information and production of threat information within the enterprise
711	Monitor and evaluate the effectiveness of the enterprise's information assurance (IA) security safeguards to ensure they provide the intended level of protection
730	Oversee the information security training and awareness program
801	Provide enterprise information assurance (IA) and supply chain risk guidance for development of the disaster recovery and continuity of operations plans
810	Provide leadership and direction to information technology (IT) personnel by ensuring that information assurance (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
848	Recommend policy and coordinate review and approval

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



SECURITY PROGRAM MANAGEMENT (CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

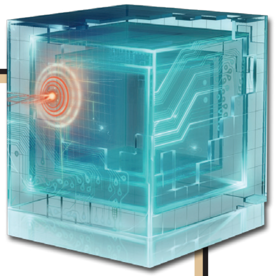
TASK KSA

ID	Statement
862	Track audit findings and recommendations to ensure appropriate mitigation actions are taken
919	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals
947	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies
948	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk
949	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements
1018	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals
1032	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance
1035	Forecast ongoing service demands and ensure security assumptions are reviewed as necessary
1041	Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development



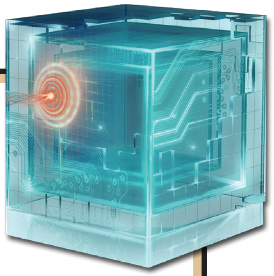
SECURITY PROGRAM MANAGEMENT (CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

TASK KSA

ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	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 and 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 information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	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
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

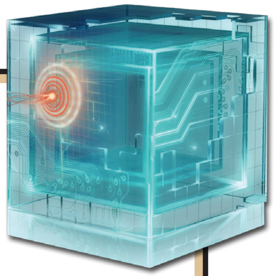
SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

TASK | KSA

ID	Statement	Competency
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
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
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
132	Knowledge of technology integration processes	Systems Integration
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE



OVERSIGHT AND DEVELOPMENT

SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])

Manages 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.

TASK | KSA

ID	Statement	Competency
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
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

NEXT PAGE | PREVIOUS PAGE

Legal Advice and Advocacy | Strategic Planning and Policy Development | Education and Training | Information Systems Security Operations (Information Systems Security Officer [ISSO]) | Security Program Management (Chief Information Security Officer [CISO])

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)
http://csrc.nist.gov/nice