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

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

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

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

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

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

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

Please provide your ideas, suggestions, and specific feedback on the content of this document by following instructions at http://csrc.nist.gov/nice/framework/
DEFINING THE CYBERSECURITY POPULATION

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

The Defining Structure

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

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

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

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

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

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

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

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

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

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

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

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

**Call to Action**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer).
OVERSEE, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization’s IA requirements. Ensures compliance from internal and external perspectives.

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

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

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

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

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

Information Assurance Compliance

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

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

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>408</td>
<td></td>
<td>Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application</td>
</tr>
<tr>
<td>414</td>
<td></td>
<td>Analyze user needs and software requirements to determine feasibility of design within time and cost constraints</td>
</tr>
<tr>
<td>417</td>
<td></td>
<td>Apply coding and testing standards, apply security testing tools (including “fuzzing” static-analysis code scanning tools), and conduct code reviews</td>
</tr>
<tr>
<td>418</td>
<td></td>
<td>Apply secure code documentation</td>
</tr>
<tr>
<td>432</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>446</td>
<td></td>
<td>Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program</td>
</tr>
<tr>
<td>459</td>
<td></td>
<td>Conduct trial runs of programs and software applications to be sure they will produce the desired information and that the instructions are correct</td>
</tr>
<tr>
<td>461</td>
<td></td>
<td>Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements and interfaces</td>
</tr>
<tr>
<td>465</td>
<td></td>
<td>Consult with customers about software system design and maintenance</td>
</tr>
<tr>
<td>467</td>
<td></td>
<td>Consult with engineering staff to evaluate interface between hardware and software</td>
</tr>
<tr>
<td>477</td>
<td></td>
<td>Correct errors by making appropriate changes and rechecking the program to ensure that the desired results are produced</td>
</tr>
<tr>
<td>TASK ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design</td>
<td></td>
</tr>
<tr>
<td>515</td>
<td>Develop and direct software system testing and validation procedures, programming, and documentation</td>
<td></td>
</tr>
<tr>
<td>543</td>
<td>Develop secure code and error messages</td>
<td></td>
</tr>
<tr>
<td>558</td>
<td>Direct software programming and development of documentation</td>
<td></td>
</tr>
<tr>
<td>602</td>
<td>Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration</td>
<td></td>
</tr>
<tr>
<td>634</td>
<td>Identify basic common coding flaws at a high level</td>
<td></td>
</tr>
<tr>
<td>644</td>
<td>Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development</td>
<td></td>
</tr>
<tr>
<td>645</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>709</td>
<td>Modify existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance</td>
<td></td>
</tr>
<tr>
<td>756</td>
<td>Perform integrated QA testing for security functionality and resiliency attack</td>
<td></td>
</tr>
<tr>
<td>764</td>
<td>Perform secure programming and understand how to identify potential flaws in codes that will mitigate the possibility of vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>Perform threat and vulnerability analysis whenever an application or system undergoes a major change</td>
<td></td>
</tr>
<tr>
<td>785</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>826</td>
<td>Recognize security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing</td>
<td></td>
</tr>
<tr>
<td>TASK ID</td>
<td>TASK</td>
<td>Statement</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-----------</td>
</tr>
<tr>
<td>850</td>
<td>Securely Provision</td>
<td>Store, retrieve, and manipulate data for analysis of system capabilities and requirements</td>
</tr>
<tr>
<td>851</td>
<td>Software Engineering</td>
<td>Supervise and assign work to programmers, designers, technologists, technicians, and other engineering and scientific personnel</td>
</tr>
<tr>
<td>865</td>
<td>Information Assurance</td>
<td>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</td>
</tr>
</tbody>
</table>
Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

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

<table>
<thead>
<tr>
<th>Task</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>3</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems</td>
</tr>
<tr>
<td>6</td>
<td>Ability to use and understand mathematical concepts (e.g., discrete math)</td>
</tr>
<tr>
<td>20</td>
<td>Knowledge of complex data structures</td>
</tr>
<tr>
<td>23</td>
<td>Knowledge of computer programming principles such as object-oriented design</td>
</tr>
<tr>
<td>38</td>
<td>Knowledge of agency IA architecture</td>
</tr>
<tr>
<td>40</td>
<td>Knowledge of agency evaluation and validation requirements</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
</tr>
<tr>
<td>54</td>
<td>Knowledge of IA or IA-enabled software products</td>
</tr>
<tr>
<td>56</td>
<td>Knowledge of IA principles and methods that apply to software development</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
</tr>
<tr>
<td>70</td>
<td>Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption</td>
</tr>
<tr>
<td>72</td>
<td>Knowledge of local area and wide area networking principles and concepts including bandwidth management</td>
</tr>
<tr>
<td>74</td>
<td>Knowledge of low-level computer languages (e.g., assembly languages)</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
</tr>
<tr>
<td>91</td>
<td>Knowledge of networking architecture</td>
</tr>
<tr>
<td>100</td>
<td>Knowledge of Privacy Impact Assessments</td>
</tr>
<tr>
<td>109</td>
<td>Knowledge of secure configuration management techniques</td>
</tr>
<tr>
<td>116</td>
<td>Knowledge of software debugging principles</td>
</tr>
<tr>
<td>117</td>
<td>Knowledge of software design tools, methods, and techniques</td>
</tr>
<tr>
<td>118</td>
<td>Knowledge of software development models (waterfall model, spiral model, etc.)</td>
</tr>
<tr>
<td>123</td>
<td>Knowledge of system and application security threats and vulnerabilities including buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, and malicious code</td>
</tr>
<tr>
<td>149</td>
<td>Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language</td>
</tr>
<tr>
<td>168</td>
<td>Skill in conducting software debugging</td>
</tr>
<tr>
<td>172</td>
<td>Skill in creating and utilizing mathematical or statistical models</td>
</tr>
<tr>
<td>174</td>
<td>Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams</td>
</tr>
<tr>
<td>177</td>
<td>Skill in designing countermeasures to identified security risks</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>185</td>
<td>Skill in developing applications that can log errors, exceptions, and application faults and logging</td>
</tr>
<tr>
<td>191</td>
<td>Skill in developing and applying security system access controls</td>
</tr>
<tr>
<td>197</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks</td>
</tr>
<tr>
<td>238</td>
<td>Skill in writing code in a modern programming language (e.g., Java, C++)</td>
</tr>
<tr>
<td>904</td>
<td>Knowledge of interpreted and compiled computer languages</td>
</tr>
<tr>
<td>905</td>
<td>Knowledge of secure coding techniques</td>
</tr>
<tr>
<td>922</td>
<td>Skill in using network analysis tools to identify vulnerabilities</td>
</tr>
</tbody>
</table>
**SECURELY PROVISION**

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>413</td>
<td></td>
<td>Analyze user needs and requirements to plan system architecture</td>
</tr>
<tr>
<td>437</td>
<td></td>
<td>Collaborate with system developers to select appropriate design solutions or ensure the compatibility of system components</td>
</tr>
<tr>
<td>483</td>
<td></td>
<td>Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event</td>
</tr>
<tr>
<td>484</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>502</td>
<td></td>
<td>Design system architecture or system components required to meet user needs</td>
</tr>
<tr>
<td>511</td>
<td></td>
<td>Develop a system security context and a preliminary system security concept of operations, and define baseline system security requirements in accordance with applicable IA requirements</td>
</tr>
<tr>
<td>561</td>
<td></td>
<td>Document and address agency information security, IA architecture and systems security engineering requirements throughout the acquisition lifecycle</td>
</tr>
<tr>
<td>563</td>
<td></td>
<td>Document design specifications, installation instructions, and other system-related information</td>
</tr>
<tr>
<td>569</td>
<td></td>
<td>Ensure all definition and architecture activities (system lifecycle support plans, concept of operations, operational procedures and maintenance training materials, etc.) are properly documented and updated as necessary</td>
</tr>
<tr>
<td>579</td>
<td></td>
<td>Ensure that acquired or developed system(s) and architecture(s) are consistent with agency IA architecture</td>
</tr>
<tr>
<td>601</td>
<td></td>
<td>Evaluate current or emerging technologies to consider factors such as cost, security, compatibility, or usability</td>
</tr>
<tr>
<td>603</td>
<td></td>
<td>Evaluate interface between hardware and software and operational and performance requirements of overall system</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>605</td>
<td>Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents</td>
<td></td>
</tr>
<tr>
<td>646</td>
<td>Identify the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately</td>
<td></td>
</tr>
<tr>
<td>765</td>
<td>Perform security reviews, identify gaps in security architecture, and develop a security risk management plan</td>
<td></td>
</tr>
<tr>
<td>797</td>
<td>Provide advice on project costs, design concepts, or design changes</td>
<td></td>
</tr>
<tr>
<td>807</td>
<td>Provide input on security requirements to be included in statements of work and other appropriate procurement documents</td>
<td></td>
</tr>
<tr>
<td>809</td>
<td>Provide input to the IA Certification and Accreditation (C&amp;A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)</td>
<td></td>
</tr>
<tr>
<td>849</td>
<td>Specify power supply requirements and configuration based on system performance expectations and design specifications</td>
<td></td>
</tr>
<tr>
<td>864</td>
<td>Translate proposed technical solutions into technical specifications</td>
<td></td>
</tr>
<tr>
<td>883</td>
<td>Write detailed functional specifications that document the architecture development process</td>
<td></td>
</tr>
</tbody>
</table>
Develops the systems concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>18</td>
<td>Knowledge of circuit analysis</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>21</td>
<td>Knowledge of computer algorithms</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>22</td>
<td>Knowledge of computer networking fundamentals</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>25</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
<td>Cryptography</td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
</tr>
<tr>
<td>34</td>
<td>Knowledge of database systems</td>
<td>Database Management Systems</td>
</tr>
<tr>
<td>38</td>
<td>Knowledge of agency IA architecture</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>39</td>
<td>Knowledge of agency confidentiality, integrity, and availability requirements</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>40</td>
<td>Knowledge of agency evaluation and validation requirements</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>42</td>
<td>Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware</td>
<td>Hardware Engineering</td>
</tr>
<tr>
<td>43</td>
<td>Knowledge of embedded systems</td>
<td>Embedded Computers</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>46</td>
<td>Knowledge of fault tolerance</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>51</td>
<td>Knowledge of how system components are installed, integrated, and optimized</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>52</td>
<td>Knowledge of human-computer interaction principles</td>
<td>Human Factors</td>
</tr>
<tr>
<td>53</td>
<td>Knowledge of IA Certification and Accreditation process</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>54</td>
<td>Knowledge of IA or IA-enabled software products</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>65</td>
<td>Knowledge of information theory</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>75</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>78</td>
<td>Knowledge of microprocessors</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>79</td>
<td>Knowledge of network access and authorization (e.g., public key infrastructure)</td>
<td>Identity Management</td>
</tr>
<tr>
<td>82</td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>84</td>
<td>Knowledge of network management principles, models, and tools</td>
<td>Network Management</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>90</td>
<td>Knowledge of operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>94</td>
<td>Knowledge of parallel and distributed computing concepts</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>108</td>
<td>Knowledge of risk management processes, including steps and methods for assessing risk</td>
<td>Risk Management</td>
</tr>
<tr>
<td>109</td>
<td>Knowledge of secure configuration management techniques</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>110</td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>111</td>
<td>Knowledge of security system design tools, methods, and techniques</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>119</td>
<td>Knowledge of software engineering</td>
<td>Software Engineering</td>
</tr>
<tr>
<td>130</td>
<td>Knowledge of systems testing and evaluation methods</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>133</td>
<td>Knowledge of telecommunications concepts</td>
<td>Telecommunications</td>
</tr>
<tr>
<td>144</td>
<td>Knowledge of the systems engineering process</td>
<td>Systems Life Cycle</td>
</tr>
<tr>
<td>147</td>
<td>Knowledge of various types of computer architectures</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>180</td>
<td>Skill in designing the integration of hardware and software solutions</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>183</td>
<td>Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>197</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>238</td>
<td>Skill in writing code in a modern programming language (e.g., Java, C++)</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>904</td>
<td>Knowledge of interpreted and compiled computer languages</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>922</td>
<td>Skill in using network analysis tools to identify vulnerabilities</td>
<td>Vulnerabilities Assessment</td>
</tr>
</tbody>
</table>
Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

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

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

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

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

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

**SYSTEMS REQUIREMENTS PLANNING**

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

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>458</td>
<td>Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications</td>
</tr>
<tr>
<td>466</td>
<td>Consult with customers to evaluate functional requirements</td>
</tr>
<tr>
<td>476</td>
<td>Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions</td>
</tr>
<tr>
<td>487</td>
<td>Define project scope and objectives based on customer requirements</td>
</tr>
<tr>
<td>497</td>
<td>Design and document test procedures and quality standards</td>
</tr>
<tr>
<td>517</td>
<td>Develop and document requirements, capabilities, and constraints for design procedures and processes</td>
</tr>
<tr>
<td>528</td>
<td>Develop cost estimates for a newly acquired or modified system</td>
</tr>
<tr>
<td>560</td>
<td>Document a system context and preliminary system concept of operations (CONOPS)</td>
</tr>
<tr>
<td>630</td>
<td>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)</td>
</tr>
<tr>
<td>669</td>
<td>Integrate and align information security and/or information assurance policies to ensure system analysis meets security requirements</td>
</tr>
<tr>
<td>700</td>
<td>Manage IT projects to ensure that developed solutions meet customer requirements</td>
</tr>
<tr>
<td>726</td>
<td>Oversee and make recommendations regarding configuration management</td>
</tr>
<tr>
<td>760</td>
<td>Perform needs analysis to determine opportunities for new and improved business process solutions</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>780</td>
<td>Plan system implementation to ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware)</td>
</tr>
<tr>
<td>789</td>
<td>Prepare use cases to justify the need for specific IT solutions</td>
</tr>
<tr>
<td>863</td>
<td>Translate functional requirements into design solutions</td>
</tr>
</tbody>
</table>
### Securely Provision

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>ID</th>
<th>Statement</th>
<th>KSA</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Knowledge of applicable business processes and operations of customer organizations</td>
<td>Requirements Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Knowledge of capabilities and requirements analysis</td>
<td>Requirements Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Knowledge of computer networking fundamentals</td>
<td>Infrastructure Design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
<td>Cryptography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Knowledge of fault tolerance</td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Knowledge of how system components are installed, integrated, and optimized</td>
<td>Systems Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Knowledge of IA Certification and Accreditation process</td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Knowledge of IA principles</td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Knowledge of industry-standard and organizationally accepted analysis principles and methods</td>
<td>Logical Systems Design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Knowledge of information theory</td>
<td>Mathematical Reasoning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Knowledge of IT architectural concepts and frameworks</td>
<td>Information Technology Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics</td>
<td>Mathematical Reasoning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>Knowledge of microprocessors</td>
<td>Computers and Electronics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TASK</td>
<td>KSA</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>-----------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td></td>
<td>Knowledge of network access and authorization (e.g., public key infrastructure)</td>
<td>Identity Management</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td></td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td></td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td></td>
<td>Knowledge of network management principles, models, and tools</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td></td>
<td>Knowledge of new and emerging IT and information security technologies</td>
<td>Technology Awareness</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td></td>
<td>Knowledge of operating systems</td>
<td>Operating Systems</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td></td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td></td>
<td>Knowledge of parallel and distributed computing concepts</td>
<td>Information Technology Architecture</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td></td>
<td>Knowledge of process engineering concepts</td>
<td>Logical Systems Design</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td></td>
<td>Knowledge of secure configuration management techniques</td>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td></td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
<td></td>
</tr>
<tr>
<td>124</td>
<td></td>
<td>Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools</td>
<td>Logical Systems Design</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td></td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design</td>
<td>Requirements Analysis</td>
<td></td>
</tr>
<tr>
<td>129</td>
<td></td>
<td>Knowledge of systems lifecycle management principles</td>
<td>Systems Life Cycle</td>
<td></td>
</tr>
<tr>
<td>130</td>
<td></td>
<td>Knowledge of systems testing and evaluation methods</td>
<td>Systems Testing and Evaluation</td>
<td></td>
</tr>
<tr>
<td>133</td>
<td></td>
<td>Knowledge of telecommunications concepts</td>
<td>Telecommunications</td>
<td></td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td>Knowledge of the systems engineering process</td>
<td>Systems Life Cycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>155</td>
<td>Skill in applying and incorporating IT technologies into proposed solutions</td>
<td>Technology Awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>156</td>
<td>Skill in applying confidentiality, integrity, and availability principles</td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>158</td>
<td>Skill in applying organization-specific systems analysis principles and techniques</td>
<td>Systems Testing and Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>Skill in conducting capabilities and requirements analysis</td>
<td>Requirements Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>166</td>
<td>Skill in conducting queries and developing algorithms to analyze data structures</td>
<td>Database Management Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>220</td>
<td>Skill in systems integration testing</td>
<td>Systems Testing and Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>224</td>
<td>Skill in the use of design modeling (such as unified modeling language)</td>
<td>Modeling and Simulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>Ability to interpret and translate customer requirements into operational cyber actions</td>
<td>Requirements Analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Test and Evaluation

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

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

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

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

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Statement</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Knowledge of agency IA architecture</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>40</td>
<td>Knowledge of agency evaluation and validation requirements</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>54</td>
<td>Knowledge of IA or IA-enabled software products</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>83</td>
<td>Knowledge of network hardware devices and functions</td>
<td>Hardware</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>127</td>
<td>Knowledge of systems administration concepts</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>144</td>
<td>Knowledge of the systems engineering process</td>
<td>Systems Life Cycle</td>
</tr>
<tr>
<td>169</td>
<td>Skill in conducting test events</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>176</td>
<td>Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data)</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>182</td>
<td>Skill in determining an appropriate level of test rigor for a given system</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>190</td>
<td>Skill in developing operations-based testing scenarios</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>238</td>
<td>Skill in writing code in a modern programming language (e.g., Java, C++)</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>ID</td>
<td>Task</td>
<td>Statement</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>239</td>
<td>Skill in writing test plans</td>
<td>Skill in writing test plans</td>
</tr>
<tr>
<td>904</td>
<td>Knowledge of interpreted and compiled computer languages</td>
<td>Knowledge of interpreted and compiled computer languages</td>
</tr>
</tbody>
</table>
Works on the development phases of the systems development lifecycle.
(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer)

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>399</td>
<td></td>
<td>Allocate information protection needs to systems</td>
</tr>
<tr>
<td>416</td>
<td></td>
<td>Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support</td>
</tr>
<tr>
<td>419</td>
<td></td>
<td>Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications</td>
</tr>
<tr>
<td>425</td>
<td></td>
<td>Assess the effectiveness of information protection measures utilized by system(s)</td>
</tr>
<tr>
<td>426</td>
<td></td>
<td>Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile</td>
</tr>
<tr>
<td>431</td>
<td></td>
<td>Build, test, and modify product prototypes using working models or theoretical models</td>
</tr>
<tr>
<td>457</td>
<td></td>
<td>Conduct Privacy Impact Analysis of the application’s security design for the appropriate security controls which protect the confidentiality and integrity of personally identifiable information (PII)</td>
</tr>
<tr>
<td>493</td>
<td></td>
<td>Design and develop Cross-Domain Solutions (CDS) including IA considerations for CDS</td>
</tr>
<tr>
<td>494</td>
<td></td>
<td>Design and develop IA or IA-enabled products</td>
</tr>
<tr>
<td>495</td>
<td></td>
<td>Design and develop secure interface specifications between interconnected systems</td>
</tr>
<tr>
<td>496</td>
<td></td>
<td>Design and develop system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation</td>
</tr>
<tr>
<td>500</td>
<td></td>
<td>Design hardware, operating systems, and software applications to adequately addresses IA security requirements</td>
</tr>
<tr>
<td>501</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>503</td>
<td></td>
<td>Design to minimum security requirements to ensure requirements are met for all systems and/or applications</td>
</tr>
<tr>
<td>ID</td>
<td>Task Description</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>516</td>
<td>Develop and direct system testing and validation procedures and documentation</td>
<td></td>
</tr>
<tr>
<td>527</td>
<td>Develop architectures or system components consistent with technical specifications</td>
<td></td>
</tr>
<tr>
<td>530</td>
<td>Develop detailed security design documentation for component and interface specifications to support system design and development</td>
<td></td>
</tr>
<tr>
<td>531</td>
<td>Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure complete testing prior to systems entering a production environment</td>
<td></td>
</tr>
<tr>
<td>532</td>
<td>Develop IA designs for agency IS to include automated IS applications, networks, and special purpose environments with platform IT interconnectivity (e.g., weapons systems, sensors, medical technologies, or distribution systems)</td>
<td></td>
</tr>
<tr>
<td>533</td>
<td>Develop IA designs for agency IS with high integrity and availability requirements</td>
<td></td>
</tr>
<tr>
<td>534</td>
<td>Develop IA designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET)</td>
<td></td>
</tr>
<tr>
<td>535</td>
<td>Develop IA designs for systems processing Sensitive Compartmented Information (SCI)</td>
<td></td>
</tr>
<tr>
<td>542</td>
<td>Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed</td>
<td></td>
</tr>
<tr>
<td>544</td>
<td>Develop security designs for new or existing system(s)</td>
<td></td>
</tr>
<tr>
<td>547</td>
<td>Develop specific IA countermeasures and risk mitigation strategies for systems and/or applications</td>
<td></td>
</tr>
<tr>
<td>549</td>
<td>Develop systems that provide adequate access controls</td>
<td></td>
</tr>
<tr>
<td>553</td>
<td>Develop/update security policies/requirements that meet the security objectives (confidentiality, integrity, and availability) of the system</td>
<td></td>
</tr>
<tr>
<td>562</td>
<td>Document application security design features, providing a functional description of their security implementation</td>
<td></td>
</tr>
<tr>
<td>568</td>
<td>Employ secure configuration management processes</td>
<td></td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>575</td>
<td>Ensure IA design and development activities are properly documented and updated as necessary.</td>
<td></td>
</tr>
<tr>
<td>626</td>
<td>Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.</td>
<td></td>
</tr>
<tr>
<td>632</td>
<td>Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.</td>
<td></td>
</tr>
<tr>
<td>648</td>
<td>Identify, assess, and recommend IA or IA-enabled products for use within a system and ensure recommended products are in compliance with agency evaluation and validation requirements.</td>
<td></td>
</tr>
<tr>
<td>659</td>
<td>Implement security designs for new or existing system(s).</td>
<td></td>
</tr>
<tr>
<td>662</td>
<td>Incorporate IA vulnerability solutions into system designs (e.g., Information Assurance Vulnerability Alerts).</td>
<td></td>
</tr>
<tr>
<td>672</td>
<td>Integrate IA policies into system development.</td>
<td></td>
</tr>
<tr>
<td>737</td>
<td>Perform an IS risk assessment and design security countermeasures to mitigate identified risks.</td>
<td></td>
</tr>
<tr>
<td>766</td>
<td>Perform security reviews and identify security gaps in security architecture.</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>Perform threat and vulnerability analysis whenever an application or system undergoes a major change.</td>
<td></td>
</tr>
<tr>
<td>803</td>
<td>Provide guidelines for implementing developed systems to customers or installation teams.</td>
<td></td>
</tr>
<tr>
<td>808</td>
<td>Provide input to implementation plans and standard operating procedures.</td>
<td></td>
</tr>
<tr>
<td>809</td>
<td>Provide input to the IA Certification and Accreditation (C&amp;A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials).</td>
<td></td>
</tr>
<tr>
<td>850</td>
<td>Store, retrieve, and manipulate data for analysis of system capabilities and requirements.</td>
<td></td>
</tr>
<tr>
<td>856</td>
<td>Provide support to security/certification test and evaluation activities.</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>860</td>
<td>Trace all system security requirements to design components</td>
<td></td>
</tr>
<tr>
<td>874</td>
<td>Utilize models and simulations to analyze or predict system performance under different operating conditions</td>
<td></td>
</tr>
<tr>
<td>877</td>
<td>Verify stability, interoperability, portability, or scalability of system architecture</td>
<td></td>
</tr>
</tbody>
</table>
Works on the development phases of the systems development lifecycle.  
*(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer)*

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>18</td>
<td>Knowledge of circuit analysis</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>21</td>
<td>Knowledge of computer algorithms</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>25</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
<td>Cryptography</td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
</tr>
<tr>
<td>34</td>
<td>Knowledge of database systems</td>
<td>Database Management Systems</td>
</tr>
<tr>
<td>38</td>
<td>Knowledge of agency IA architecture</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>40</td>
<td>Knowledge of agency evaluation and validation requirements</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>42</td>
<td>Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware</td>
<td>Hardware Engineering</td>
</tr>
<tr>
<td>43</td>
<td>Knowledge of embedded systems</td>
<td>Embedded Computers</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>46</td>
<td>Knowledge of fault tolerance</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>51</td>
<td>Knowledge of how system components are installed, integrated, and optimized</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>52</td>
<td>Knowledge of human-computer interaction principles</td>
<td>Human Factors</td>
</tr>
<tr>
<td>54</td>
<td>Knowledge of IA or IA-enabled software products</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>ID</td>
<td>Task Description</td>
<td>Competency</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>64</td>
<td>Knowledge of Information Security Systems Engineering principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>65</td>
<td>Knowledge of information theory</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>70</td>
<td>Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>72</td>
<td>Knowledge of local area and wide area networking principles and concepts including bandwidth management</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>75</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>78</td>
<td>Knowledge of microprocessors</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>79</td>
<td>Knowledge of network access and authorization (e.g., public key infrastructure)</td>
<td>Identity Management</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>82</td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>84</td>
<td>Knowledge of network management principles, models, and tools</td>
<td>Network Management</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>90</td>
<td>Knowledge of operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>94</td>
<td>Knowledge of parallel and distributed computing concepts</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>100</td>
<td>Knowledge of Privacy Impact Assessments</td>
<td>Personnel Safety and Security</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>109</td>
<td>Knowledge of secure configuration management techniques</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>110</td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>119</td>
<td>Knowledge of software engineering</td>
<td>Software Engineering</td>
</tr>
<tr>
<td>124</td>
<td>Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools</td>
<td>Logical Systems Design</td>
</tr>
<tr>
<td>130</td>
<td>Knowledge of systems testing and evaluation methods</td>
<td>Systems Testing and Evaluation</td>
</tr>
<tr>
<td>133</td>
<td>Knowledge of telecommunications concepts</td>
<td>Telecommunications</td>
</tr>
<tr>
<td>144</td>
<td>Knowledge of the systems engineering process</td>
<td>Systems Life Cycle</td>
</tr>
<tr>
<td>147</td>
<td>Knowledge of various types of computer architectures</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>173</td>
<td>Skill in creating policies that reflect system security objectives</td>
<td>Information Systems Security Certification</td>
</tr>
<tr>
<td>177</td>
<td>Skill in designing countermeasures to identified security risks</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>179</td>
<td>Skill in designing security controls based on Information Assurance principles and tenets</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>180</td>
<td>Skill in designing the integration of hardware and software solutions</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>181</td>
<td>Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>191</td>
<td>Skill in developing and applying security system access controls</td>
<td>Identity Management</td>
</tr>
<tr>
<td>197</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>199</td>
<td>Skill in evaluating the adequacy of security designs</td>
<td>Vulnerabilities Assessment</td>
</tr>
</tbody>
</table>
### SECURELY PROVISION

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>238</td>
<td>Skill in writing code in a modern programming language (e.g., Java, C++)</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>904</td>
<td>Knowledge of interpreted and compiled computer languages</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>922</td>
<td>Skill in using network analysis tools to identify vulnerabilities</td>
<td>Vulnerabilities Assessment</td>
</tr>
</tbody>
</table>
Operate and Maintain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*SAMPLE JOB TITLES: Content Staging Specialist, Data Architect, Data Manager, Data Warehouse Specialist, Database Administrator, Database Developer, Information Dissemination Manager, Systems Operations Personnel*

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

### DATA ADMINISTRATION

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

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task &amp; KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>28</td>
<td>Knowledge of data administration and data standardization policies and standards</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
</tr>
<tr>
<td>31</td>
<td>Knowledge of data mining and data warehousing principles</td>
</tr>
<tr>
<td>32</td>
<td>Knowledge of database management systems, query languages, table relationships, and views</td>
</tr>
<tr>
<td>35</td>
<td>Knowledge of digital rights management</td>
</tr>
<tr>
<td>41</td>
<td>Knowledge of agency LAN/WAN pathways</td>
</tr>
<tr>
<td>44</td>
<td>Knowledge of enterprise messaging systems and associated software</td>
</tr>
<tr>
<td>79</td>
<td>Knowledge of network access and authorization (e.g., public key infrastructure)</td>
</tr>
<tr>
<td>90</td>
<td>Knowledge of operating systems</td>
</tr>
<tr>
<td>98</td>
<td>Knowledge of policy-based and risk adaptive access controls</td>
</tr>
<tr>
<td>104</td>
<td>Knowledge of query languages such as SQL (structured query language)</td>
</tr>
<tr>
<td>120</td>
<td>Knowledge of sources, characteristics, and uses of the organization’s data assets</td>
</tr>
<tr>
<td>133</td>
<td>Knowledge of telecommunications concepts</td>
</tr>
<tr>
<td>137</td>
<td>Knowledge of the characteristics of physical and virtual data storage media</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>152</td>
<td>Skill in allocating storage capacity in the design of data management systems</td>
</tr>
<tr>
<td>178</td>
<td>Skill in designing databases</td>
</tr>
<tr>
<td>186</td>
<td>Skill in developing data dictionaries</td>
</tr>
<tr>
<td>187</td>
<td>Skill in developing data models</td>
</tr>
<tr>
<td>188</td>
<td>Skill in developing data repositories</td>
</tr>
<tr>
<td>201</td>
<td>Skill in generating queries and reports</td>
</tr>
<tr>
<td>208</td>
<td>Skill in maintaining databases</td>
</tr>
<tr>
<td>213</td>
<td>Skill in optimizing database performance</td>
</tr>
<tr>
<td>910</td>
<td>Knowledge of database theory</td>
</tr>
</tbody>
</table>
**Operate and Maintain**

**Information Systems Security Management**

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>ID</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>397</td>
<td>Advise the DAA of changes affecting the enterprise’s IA posture</td>
</tr>
<tr>
<td></td>
<td>405</td>
<td>Analyze identified security strategies and select the best approach or practice for the enterprise</td>
</tr>
<tr>
<td></td>
<td>415</td>
<td>Analyze, develop, approve, and issue enterprise IA policies</td>
</tr>
<tr>
<td></td>
<td>440</td>
<td>Collect and maintain data needed to meet system IA reporting</td>
</tr>
<tr>
<td></td>
<td>523</td>
<td>Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow IT and IA policies and procedures</td>
</tr>
<tr>
<td></td>
<td>536</td>
<td>Develop IT security requirements specific to an IT acquisition for inclusion in procurement documents</td>
</tr>
<tr>
<td></td>
<td>540</td>
<td>Develop procedures to ensure system users are aware of their IA responsibilities before granting access to agency's information systems</td>
</tr>
<tr>
<td></td>
<td>545</td>
<td>Develop security requirements for hardware, software, and services acquisitions</td>
</tr>
<tr>
<td></td>
<td>581</td>
<td>Ensure that compliance monitoring occurs, and review results of across the network environment</td>
</tr>
<tr>
<td></td>
<td>583</td>
<td>Ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate IT security configuration guidelines, policies, and procedures</td>
</tr>
<tr>
<td></td>
<td>584</td>
<td>Ensure that IA inspections, tests, and reviews are coordinated for the network environment</td>
</tr>
<tr>
<td></td>
<td>585</td>
<td>Ensure that IA requirements are integrated into the Continuity of Operations Plan (COOP) for that system or agency</td>
</tr>
<tr>
<td></td>
<td>586</td>
<td>Ensure that IA security requirements are appropriately identified in computer environment operation procedures</td>
</tr>
<tr>
<td></td>
<td>589</td>
<td>Ensure that IT information security recovery processes are monitored and that IA features and procedures are properly restored</td>
</tr>
<tr>
<td>Task</td>
<td>KSA</td>
<td>Statement</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>-----------</td>
</tr>
<tr>
<td>590</td>
<td></td>
<td>Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with agency-level IA architecture</td>
</tr>
<tr>
<td>591</td>
<td></td>
<td>Ensure that security related provisions of the system acquisition documents meet all identified security needs</td>
</tr>
<tr>
<td>592</td>
<td></td>
<td>Ensure that system security configuration guidelines are followed</td>
</tr>
<tr>
<td>598</td>
<td></td>
<td>Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed</td>
</tr>
<tr>
<td>610</td>
<td></td>
<td>Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents</td>
</tr>
<tr>
<td>625</td>
<td></td>
<td>Help prepare IA certification and accreditation documentation</td>
</tr>
<tr>
<td>719</td>
<td></td>
<td>Monitor system performance and review for compliance with IA security and privacy requirements within the computer environment</td>
</tr>
<tr>
<td>731</td>
<td></td>
<td>Participate in an information security risk assessment during the Certification and Accreditation process</td>
</tr>
<tr>
<td>733</td>
<td></td>
<td>Participate in the development or modification of the computer environment IA security program plans and requirements</td>
</tr>
<tr>
<td>790</td>
<td></td>
<td>Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations</td>
</tr>
<tr>
<td>816</td>
<td></td>
<td>Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents</td>
</tr>
<tr>
<td>824</td>
<td></td>
<td>Recognize a possible security violation and take appropriate action to report the incident, as required</td>
</tr>
<tr>
<td>828</td>
<td></td>
<td>Recommend resource allocations required to securely operate and maintain an organization’s IA requirements</td>
</tr>
<tr>
<td>852</td>
<td></td>
<td>Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered</td>
</tr>
<tr>
<td>853</td>
<td></td>
<td>Support and administer data retention and recovery within the computing environment</td>
</tr>
<tr>
<td>869</td>
<td></td>
<td>Use federal and organization-specific published documents to manage operations of their computing environment system(s)</td>
</tr>
</tbody>
</table>
### Operate and Maintain

**Information Systems Security Management**

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>9</td>
<td>Knowledge of applicable business processes and operations of customer organizations</td>
<td>Requirements Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>37</td>
<td>Knowledge of disaster recovery continuity of operations plans</td>
<td>Incident Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>55</td>
<td>Knowledge of IA principles</td>
<td>Information Assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>58</td>
<td>Knowledge of identified vulnerabilities, alerts, and bulletins (IAVA, IAVB)</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>62</td>
<td>Knowledge of industry-standard and organizationally accepted analysis principles and methods</td>
<td>Logical Systems Design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>69</td>
<td>Knowledge of IT security certification and accreditation requirements</td>
<td>Information Systems Security Certification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>71</td>
<td>Knowledge of IT security principles and regulations</td>
<td>Information Systems Security Certification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>76</td>
<td>Knowledge of measures or indicators of system performance and availability</td>
<td>Information Technology Performance Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>77</td>
<td>Knowledge of methods for evaluating, implementing, and disseminating IT security tools and procedures</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>86</td>
<td>Knowledge of network systems management methods including end-to-end systems performance monitoring</td>
<td>Network Management</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Knowledge of new and emerging IT and information security technologies</td>
<td>Technology Awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Knowledge of pertinent government laws and information technology regulations</td>
<td>Legal, Government and Jurisprudence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods</td>
<td>Systems Life Cycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>Knowledge of server and client operating systems</td>
<td>Operating Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>Knowledge of structured analysis principles and methods</td>
<td>Logical Systems Design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design</td>
<td>Requirements Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>Knowledge of systems diagnostic tools and fault identification techniques</td>
<td>Systems Testing and Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>129</td>
<td>Knowledge of systems lifecycle management principles</td>
<td>Systems Life Cycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>Knowledge of the organization’s enterprise IT goals and objectives</td>
<td>Enterprise Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>183</td>
<td>Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes</td>
<td>Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>203</td>
<td>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</td>
<td>Information Technology Performance Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>325</td>
<td>Knowledge of secure acquisitions (COTR, procurement, supply chain management).</td>
<td>Contracting/Procurement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**OPERATE AND MAINTAIN**

**KNOWLEDGE MANAGEMENT**

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

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

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>5</td>
<td>Ability to match the appropriate knowledge repository technology for a given application or environment</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
</tr>
<tr>
<td>56</td>
<td>Knowledge of IA principles and methods that apply to software development</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
</tr>
<tr>
<td>91</td>
<td>Knowledge of networking architecture</td>
</tr>
<tr>
<td>134</td>
<td>Knowledge of the capabilities and functionality associated with various content creation technologies (wikis, social networking, blogs, etc.)</td>
</tr>
<tr>
<td>135</td>
<td>Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines, etc.)</td>
</tr>
<tr>
<td>136</td>
<td>Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint, etc.)</td>
</tr>
<tr>
<td>163</td>
<td>Skill in conducting information searches</td>
</tr>
<tr>
<td>164</td>
<td>Skill in conducting knowledge mapping (map of knowledge repositories)</td>
</tr>
<tr>
<td>189</td>
<td>Skill in developing expert directories that allow end-users to easily reach Subject Matter Experts</td>
</tr>
<tr>
<td>223</td>
<td>Skill in the measuring and reporting of intellectual capital</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>230</td>
<td>Skill in using knowledge management technologies</td>
</tr>
<tr>
<td>907</td>
<td>Skill in data mining techniques</td>
</tr>
<tr>
<td>910</td>
<td>Knowledge of database theory</td>
</tr>
</tbody>
</table>
## OPERATE AND MAINTAIN

### CUSTOMER SERVICE AND TECHNICAL SUPPORT

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>7</td>
<td>Knowledge of “knowledge base” capabilities in identifying the solutions to less common and more complex system problems</td>
</tr>
<tr>
<td>33</td>
<td>Knowledge of database procedures used for documenting and querying reported incidents</td>
</tr>
<tr>
<td>37</td>
<td>Knowledge of disaster recovery continuity of operations plans</td>
</tr>
<tr>
<td>76</td>
<td>Knowledge of measures or indicators of system performance and availability</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
</tr>
<tr>
<td>127</td>
<td>Knowledge of systems administration concepts</td>
</tr>
<tr>
<td>142</td>
<td>Knowledge of the operations and processes for diagnosing common or recurring system problems</td>
</tr>
<tr>
<td>145</td>
<td>Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly</td>
</tr>
<tr>
<td>165</td>
<td>Skill in conducting open source research for troubleshooting novel client-level problems</td>
</tr>
<tr>
<td>204</td>
<td>Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation</td>
</tr>
<tr>
<td>221</td>
<td>Skill in testing and configuring network workstations and peripherals</td>
</tr>
<tr>
<td>Task ID</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>222</td>
<td>Skill in the basic operation of computers</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**OPERATE AND MAINTAIN**

**NETWORK SERVICES**

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

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

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

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>KSA</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td></td>
<td>Knowledge of basic communication methods, principles, and concepts (e.g., crypto, dual hubs, time multiplexers, etc.) that support the network infrastructure</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware</td>
<td>Hardware</td>
</tr>
<tr>
<td>55</td>
<td></td>
<td>Knowledge of IA principles</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>70</td>
<td></td>
<td>Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>72</td>
<td></td>
<td>Knowledge of local area and wide area networking principles and concepts including bandwidth management</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>76</td>
<td></td>
<td>Knowledge of measures or indicators of system performance and availability</td>
<td>Information Technology Performance Assessment</td>
</tr>
<tr>
<td>80</td>
<td></td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td></td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>86</td>
<td></td>
<td>Knowledge of network systems management methods including end-to-end systems performance monitoring</td>
<td>Network Management</td>
</tr>
<tr>
<td>106</td>
<td></td>
<td>Knowledge of remote access technology concepts</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>112</td>
<td></td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods</td>
<td>Systems Life Cycle</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>Knowledge of systems administration concepts</td>
<td>Operating Systems</td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>Knowledge of telecommunications concepts</td>
<td>Telecommunications</td>
<td></td>
</tr>
<tr>
<td>154</td>
<td>Skill in analyzing network traffic capacity and performance characteristics</td>
<td>Capacity Management</td>
<td></td>
</tr>
<tr>
<td>193</td>
<td>Skill in developing, testing, and implementing network infrastructure contingency and recovery plans</td>
<td>Information Assurance</td>
<td></td>
</tr>
<tr>
<td>198</td>
<td>Skill in establishing a routing schema</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>205</td>
<td>Skill in implementing, maintaining, and improving established security practices</td>
<td>Information Systems/Network Security</td>
<td></td>
</tr>
<tr>
<td>207</td>
<td>Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>231</td>
<td>Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>891</td>
<td>Skill in configuring and utilizing hardware-based computer protection tools (e.g., hardware firewalls, servers, routers)</td>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>892</td>
<td>Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)</td>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>893</td>
<td>Skill in securing network communications</td>
<td>Information Assurance</td>
<td></td>
</tr>
<tr>
<td>896</td>
<td>Skill in protecting a network against malware</td>
<td>Information Assurance</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>Knowledge of web filtering technologies</td>
<td>Web Technology</td>
<td></td>
</tr>
<tr>
<td>901</td>
<td>Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts)</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>902</td>
<td>Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>903</td>
<td>Knowledge of wireless fidelity (WIFI)</td>
<td>Network Management</td>
<td></td>
</tr>
</tbody>
</table>
## SYSTEM ADMINISTRATION

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>434</td>
<td>Check server availability, functionality, integrity, and efficiency</td>
</tr>
<tr>
<td>452</td>
<td>Conduct functional and connectivity testing to ensure continuing operability</td>
</tr>
<tr>
<td>456</td>
<td>Conduct periodic server maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing</td>
</tr>
<tr>
<td>499</td>
<td>Design group policies and access control lists to ensure compatibility with agency standards</td>
</tr>
<tr>
<td>518</td>
<td>Develop and document systems administration standard operating procedures</td>
</tr>
<tr>
<td>521</td>
<td>Develop and implement local network usage policies and procedures</td>
</tr>
<tr>
<td>668</td>
<td>Install server fixes, updates, and enhancements</td>
</tr>
<tr>
<td>683</td>
<td>Maintain baseline system security per DISA Security Technical Implementation Guides (STIGs)</td>
</tr>
<tr>
<td>695</td>
<td>Manage accounts, network rights, and access to systems and equipment</td>
</tr>
<tr>
<td>701</td>
<td>Manage server resources including performance, capacity, availability, serviceability, and recoverability</td>
</tr>
<tr>
<td>713</td>
<td>Monitor and maintain server configuration</td>
</tr>
<tr>
<td>728</td>
<td>Oversee installation, implementation, configuration, and support of network components</td>
</tr>
<tr>
<td>763</td>
<td>Perform repairs on faulty server hardware</td>
</tr>
<tr>
<td>776</td>
<td>Plan and coordinate the installation of new or modified hardware, operating systems, and other baseline software</td>
</tr>
<tr>
<td>781</td>
<td>Plan, execute, and verify data redundancy and system recovery procedures</td>
</tr>
<tr>
<td>TASK ID</td>
<td>Statement</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>811</td>
<td>Provide ongoing optimization and problem solving support</td>
</tr>
<tr>
<td>835</td>
<td>Resolve hardware/software interface and interoperability problems</td>
</tr>
</tbody>
</table>
## Task: Operate and Maintain

**System Administration**

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>89</td>
<td>Knowledge of new technological developments in server administration</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>96</td>
<td>Knowledge of performance tuning tools and techniques</td>
<td>Information Technology Performance Assessment</td>
</tr>
<tr>
<td>99</td>
<td>Knowledge of principles and methods for integrating server components</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>112</td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods</td>
<td>Systems Life Cycle</td>
</tr>
<tr>
<td>113</td>
<td>Knowledge of server and client operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>114</td>
<td>Knowledge of server diagnostic tools and fault identification techniques</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>127</td>
<td>Knowledge of systems administration concepts</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>141</td>
<td>Knowledge of the enterprise IT architecture</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>167</td>
<td>Skill in conducting server planning, management, and maintenance</td>
<td>Network Management</td>
</tr>
<tr>
<td>170</td>
<td>Skill in configuring and optimizing software</td>
<td>Software Engineering</td>
</tr>
<tr>
<td>TASK</td>
<td>KSA</td>
<td>Statement</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>171</td>
<td></td>
<td>Skill in correcting physical and technical problems which impact server performance</td>
</tr>
<tr>
<td>194</td>
<td></td>
<td>Skill in diagnosing connectivity problems</td>
</tr>
<tr>
<td>195</td>
<td></td>
<td>Skill in diagnosing failed servers</td>
</tr>
<tr>
<td>202</td>
<td></td>
<td>Skill in identifying and anticipating server performance, availability, capacity, or configuration problems</td>
</tr>
<tr>
<td>206</td>
<td></td>
<td>Skill in installing computer and server upgrades</td>
</tr>
<tr>
<td>209</td>
<td></td>
<td>Skill in maintaining directory services</td>
</tr>
<tr>
<td>211</td>
<td></td>
<td>Skill in monitoring and optimizing server performance</td>
</tr>
<tr>
<td>216</td>
<td></td>
<td>Skill in recovering failed servers</td>
</tr>
<tr>
<td>891</td>
<td></td>
<td>Skill in configuring and utilizing hardware-based computer protection tools (e.g., hardware firewalls, servers, routers)</td>
</tr>
<tr>
<td>892</td>
<td></td>
<td>Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)</td>
</tr>
</tbody>
</table>
## Operate and Maintain

### Systems Security Analysis

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>419</td>
<td></td>
<td>Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications</td>
</tr>
<tr>
<td>420</td>
<td></td>
<td>Apply security policies to meet security objectives of the system</td>
</tr>
<tr>
<td>421</td>
<td></td>
<td>Apply service-oriented security architecture principles to meet agency confidentiality, integrity, and availability requirements</td>
</tr>
<tr>
<td>525</td>
<td></td>
<td>Develop and test system fail-over or system operations transfer to an alternate site based on system availability requirements</td>
</tr>
<tr>
<td>559</td>
<td></td>
<td>Discover organizational trends with regard to the security posture of systems</td>
</tr>
<tr>
<td>571</td>
<td></td>
<td>Ensure all operations and maintenance activities are properly documented and updated as necessary</td>
</tr>
<tr>
<td>572</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>576</td>
<td></td>
<td>Ensure IA-enabled products or other compensating security control technologies reduce identified risk to an acceptable level</td>
</tr>
<tr>
<td>593</td>
<td></td>
<td>Establish adequate access controls based on principles of least privilege and need-to-know</td>
</tr>
<tr>
<td>616</td>
<td></td>
<td>Exercise the system Disaster Recovery and Continuity Of Operations</td>
</tr>
<tr>
<td>651</td>
<td></td>
<td>Implement and manage an Information Assurance Program</td>
</tr>
<tr>
<td>652</td>
<td></td>
<td>Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines</td>
</tr>
<tr>
<td>653</td>
<td></td>
<td>Implement approaches to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>Implement security controls that ensure users can only perform actions for which they have authorization, based on principles of least privilege and separation of duty</td>
<td></td>
</tr>
<tr>
<td>658</td>
<td>Implement security designs and properly mitigate identified threats</td>
<td></td>
</tr>
<tr>
<td>660</td>
<td>Implement specific IA countermeasures for systems and/or applications</td>
<td></td>
</tr>
<tr>
<td>661</td>
<td>Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation</td>
<td></td>
</tr>
<tr>
<td>670</td>
<td>Integrate and/or implement Cross-Domain Solutions (CDS) in a secure environment</td>
<td></td>
</tr>
<tr>
<td>671</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>708</td>
<td>Mitigate/correct security deficiencies identified during security/certification testing or identify risk acceptance for the appropriate DAA or authorized representative</td>
<td></td>
</tr>
<tr>
<td>717</td>
<td>Monitor information protection assurance mechanisms related to system implementation and testing practices</td>
<td></td>
</tr>
<tr>
<td>729</td>
<td>Oversee minimum security requirements are in place for all applications</td>
<td></td>
</tr>
<tr>
<td>754</td>
<td>Perform IA testing of developed applications and/or systems</td>
<td></td>
</tr>
<tr>
<td>767</td>
<td>Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy</td>
<td></td>
</tr>
<tr>
<td>782</td>
<td>Plan, and recommend modifications or adjustments based on exercise results or system environment; ensure Recovery and Continuity plans are executable in the system operational environment</td>
<td></td>
</tr>
<tr>
<td>795</td>
<td>Properly document all implementation, operations, and maintenance activities and update as necessary</td>
<td></td>
</tr>
<tr>
<td>806</td>
<td>Provide information assurance guidance to leadership</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>809</td>
<td>Provide input to the IA Certification and Accreditation (C&amp;A) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)</td>
<td></td>
</tr>
<tr>
<td>876</td>
<td>Verify and update security documentation reflecting the application/system security design features</td>
<td></td>
</tr>
<tr>
<td>880</td>
<td>Work with others to resolve computer security incidents and vulnerability compliance</td>
<td></td>
</tr>
</tbody>
</table>
## OPERATE AND MAINTAIN

### SYSTEMS SECURITY ANALYSIS

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>18</td>
<td>Knowledge of circuit analysis</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>21</td>
<td>Knowledge of computer algorithms</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>25</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
<td>Cryptography</td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
</tr>
<tr>
<td>34</td>
<td>Knowledge of database systems</td>
<td>Database Management Systems</td>
</tr>
<tr>
<td>42</td>
<td>Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware</td>
<td>Hardware Engineering</td>
</tr>
<tr>
<td>43</td>
<td>Knowledge of embedded systems</td>
<td>Embedded Computers</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>46</td>
<td>Knowledge of fault tolerance</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>51</td>
<td>Knowledge of how system components are installed, integrated, and optimized</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>52</td>
<td>Knowledge of human-computer interaction principles</td>
<td>Human Factors</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>65</td>
<td>Knowledge of information theory</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>70</td>
<td>Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>75</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics</td>
<td>Mathematical Reasoning</td>
</tr>
<tr>
<td>78</td>
<td>Knowledge of microprocessors</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>79</td>
<td>Knowledge of network access and authorization (e.g., public key infrastructure)</td>
<td>Identity Management</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>82</td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>84</td>
<td>Knowledge of network management principles, models, and tools</td>
<td>Network Management</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>90</td>
<td>Knowledge of operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>94</td>
<td>Knowledge of parallel and distributed computing concepts</td>
<td>Information Technology Architecture</td>
</tr>
<tr>
<td>108</td>
<td>Knowledge of risk management processes, including steps and methods for assessing risk</td>
<td>Risk Management</td>
</tr>
<tr>
<td>109</td>
<td>Knowledge of secure configuration management techniques</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>110</td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>111</td>
<td>Knowledge of security system design tools, methods, and techniques</td>
<td>Information Systems/Network Security</td>
</tr>
</tbody>
</table>

**SYSTEMS SECURITY ANALYSIS**

**TASK**

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
</table>

**OPERATE AND MAINTAIN**

**KSA**

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
</table>

**NEXT PAGE | PREVIOUS PAGE**
### Systems Security Analysis

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

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

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

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

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

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

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

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

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

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

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

## COMPUTER NETWORK DEFENSE

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


<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>427</td>
<td></td>
<td>427</td>
<td>Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise</td>
</tr>
<tr>
<td>433</td>
<td></td>
<td>433</td>
<td>Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources</td>
</tr>
<tr>
<td>472</td>
<td></td>
<td>472</td>
<td>Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts</td>
</tr>
<tr>
<td>716</td>
<td></td>
<td>716</td>
<td>Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise</td>
</tr>
<tr>
<td>723</td>
<td></td>
<td>723</td>
<td>Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event’s history, status, and potential impact for further action</td>
</tr>
<tr>
<td>750</td>
<td></td>
<td>750</td>
<td>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</td>
</tr>
<tr>
<td>800</td>
<td></td>
<td>800</td>
<td>Provide daily summary reports of network events and activity relevant to Computer Network Defense practices</td>
</tr>
<tr>
<td>823</td>
<td></td>
<td>823</td>
<td>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts</td>
</tr>
</tbody>
</table>
# Protect and Defend

## Computer Network Defense

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


<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Knowledge of access authentication methods</td>
<td>Identity Management</td>
</tr>
<tr>
<td>13</td>
<td>Knowledge of basic system, network, and operating system hardening techniques</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>19</td>
<td>Knowledge of Computer Network Defense tools, including open source tools, and their capabilities</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>26</td>
<td>Knowledge of cross-domain guards</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>49</td>
<td>Knowledge of host/network access controls (e.g., access control list)</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>61</td>
<td>Knowledge of incident response and handling methodologies</td>
<td>Incident Management</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>66</td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>ID</td>
<td>KSA</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>87</td>
<td>Knowledge of network traffic analysis methods</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>88</td>
<td>Knowledge of new and emerging IT and information security technologies</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>95</td>
<td>Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>110</td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>115</td>
<td>Knowledge of signature development</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>138</td>
<td>Knowledge of the Computer Network Defense Service Provider reporting structure and processes within one’s own agency or organization</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>148</td>
<td>Knowledge of VPN security</td>
<td>Encryption</td>
</tr>
<tr>
<td>150</td>
<td>Knowledge of what constitutes a “threat” to a network</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>175</td>
<td>Skill in developing and deploying signatures</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>181</td>
<td>Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>212</td>
<td>Skill in network mapping and recreating network topologies</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>ID</td>
<td>TASK</td>
<td>KSA</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>214</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>229</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>233</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>234</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>271</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>278</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>286</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>342</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>347</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>895</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>915</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
<tr>
<td>922</td>
<td>Computer Network Defense</td>
<td></td>
</tr>
</tbody>
</table>
## INCIDENT RESPONSE

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>438</td>
<td></td>
<td>Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise</td>
</tr>
<tr>
<td>470</td>
<td></td>
<td>Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents</td>
</tr>
<tr>
<td>474</td>
<td></td>
<td>Coordinate with intelligence analysts to correlate threat assessment data</td>
</tr>
<tr>
<td>478</td>
<td></td>
<td>Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation</td>
</tr>
<tr>
<td>686</td>
<td></td>
<td>Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission</td>
</tr>
<tr>
<td>716</td>
<td></td>
<td>Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise</td>
</tr>
<tr>
<td>738</td>
<td></td>
<td>Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security</td>
</tr>
<tr>
<td>741</td>
<td></td>
<td>Perform command and control functions in response to incidents</td>
</tr>
<tr>
<td>743</td>
<td></td>
<td>Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation</td>
</tr>
<tr>
<td>745</td>
<td></td>
<td>Perform Computer Network Defense trend analysis and reporting</td>
</tr>
<tr>
<td>755</td>
<td></td>
<td>Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems</td>
</tr>
<tr>
<td>TASK ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>762</td>
<td>Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)</td>
<td></td>
</tr>
<tr>
<td>823</td>
<td>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts</td>
<td></td>
</tr>
<tr>
<td>846</td>
<td>Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.</td>
<td></td>
</tr>
<tr>
<td>861</td>
<td>Track and document Computer Network Defense incidents from initial detection through final resolution</td>
<td></td>
</tr>
<tr>
<td>882</td>
<td>Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies</td>
<td></td>
</tr>
</tbody>
</table>
Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ID</strong></td>
<td><strong>Statement</strong></td>
</tr>
<tr>
<td>13</td>
<td>Knowledge of basic system, network, and operating system hardening techniques</td>
</tr>
<tr>
<td>24</td>
<td>Knowledge of concepts and practices of processing digital information</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
</tr>
<tr>
<td>49</td>
<td>Knowledge of host/network access controls (e.g., access control list)</td>
</tr>
<tr>
<td>50</td>
<td>Knowledge of how network services and protocols interact to provide network communications</td>
</tr>
<tr>
<td>60</td>
<td>Knowledge of incident categories, incident responses, and timelines for responses</td>
</tr>
<tr>
<td>61</td>
<td>Knowledge of incident response and handling methodologies</td>
</tr>
<tr>
<td>66</td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
</tr>
<tr>
<td>87</td>
<td>Knowledge of network traffic analysis methods</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
</tr>
<tr>
<td>93</td>
<td>Knowledge of packet-level analysis</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
</tr>
<tr>
<td>150</td>
<td>Knowledge of what constitutes a “threat” to a network</td>
</tr>
<tr>
<td>153</td>
<td>Skill in analyzing malware</td>
</tr>
<tr>
<td>217</td>
<td>Skill in seizing and preserving digital evidence</td>
</tr>
<tr>
<td>229</td>
<td>Skill in using incident handling methodologies</td>
</tr>
<tr>
<td>893</td>
<td>Skill in securing network communications</td>
</tr>
<tr>
<td>895</td>
<td>Skill in recognizing and categorizing types of vulnerabilities and associated attacks</td>
</tr>
<tr>
<td>896</td>
<td>Skill in protecting a network against malware</td>
</tr>
<tr>
<td>897</td>
<td>Skill in performing damage assessments</td>
</tr>
<tr>
<td>923</td>
<td>Knowledge of security event correlation tools</td>
</tr>
</tbody>
</table>
## COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT

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


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

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


<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Knowledge of basic system, network, and operating system hardening techniques</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>49</td>
<td>Knowledge of host/network access controls (e.g., access control list)</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>59</td>
<td>Knowledge of IDS tools and applications</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>61</td>
<td>Knowledge of incident response and handling methodologies</td>
<td>Incident Management</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>87</td>
<td>Knowledge of network traffic analysis methods</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>93</td>
<td>Knowledge of packet-level analysis</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>146</td>
<td>Knowledge of the types of IDS hardware and software</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>150</td>
<td>Knowledge of what constitutes a “threat” to a network</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>157</td>
<td>Skill in applying host/network access controls (e.g., access control list)</td>
<td>Identity Management</td>
</tr>
<tr>
<td>175</td>
<td>Skill in developing and deploying signatures</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>181</td>
<td>Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>219</td>
<td>Skill in system administration for Unix/Linux operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>227</td>
<td>Skill in tuning sensors</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>229</td>
<td>Skill in using incident handling methodologies</td>
<td>Incident Management</td>
</tr>
<tr>
<td>237</td>
<td>Skill in using VPN devices and encryption</td>
<td>Encryption</td>
</tr>
<tr>
<td>893</td>
<td>Skill in securing network communications</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>896</td>
<td>Skill in protecting a network against malware</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>900</td>
<td>Knowledge of web filtering technologies</td>
<td>Web Technology</td>
</tr>
</tbody>
</table>
**PROTECT AND DEFEND**

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>391</td>
<td></td>
<td>Acquire and manage the necessary resources, including financial resources, to support IT security goals and objectives and reduce overall organizational risk</td>
</tr>
<tr>
<td>392</td>
<td></td>
<td>Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program</td>
</tr>
<tr>
<td>395</td>
<td></td>
<td>Advise CIO on risk levels and security posture</td>
</tr>
<tr>
<td>396</td>
<td></td>
<td>Advise the CIO on cost/benefit analysis of information security programs, policies, processes, and systems</td>
</tr>
<tr>
<td>445</td>
<td></td>
<td>Communicate the value of IT security within the organization</td>
</tr>
<tr>
<td>468</td>
<td></td>
<td>Continuously validate the organization against additional mandates, as developed, to ensure full compliance</td>
</tr>
<tr>
<td>473</td>
<td></td>
<td>&quot;Coordinate with information security, physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization&quot;</td>
</tr>
<tr>
<td>475</td>
<td></td>
<td>Coordinate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance</td>
</tr>
<tr>
<td>574</td>
<td></td>
<td>Evaluate, monitor, and ensure compliance with data security policies and relevant legal and regulatory requirements</td>
</tr>
<tr>
<td>578</td>
<td></td>
<td>Ensure security improvement actions are implemented as required.</td>
</tr>
<tr>
<td>582</td>
<td></td>
<td>Ensure that data classification and data management policies and guidance are issue-updated</td>
</tr>
<tr>
<td>596</td>
<td></td>
<td>&quot;Establish overall enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization’s overall security strategy&quot;</td>
</tr>
<tr>
<td>600</td>
<td></td>
<td>Evaluate cost benefit, economic, and risk analysis in decision making process</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>604</td>
<td>Evaluate proposals to determine if proposed security solutions effectively address enterprise requirements, as detailed in solicitation documents</td>
<td></td>
</tr>
<tr>
<td>608</td>
<td>Evaluate the effectiveness of procurement function in addressing information security requirements through procurement activities, and recommend improvements</td>
<td></td>
</tr>
<tr>
<td>610</td>
<td>Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents</td>
<td></td>
</tr>
<tr>
<td>628</td>
<td>Identify alternative functional IA security strategies to address organizational IT security concerns</td>
<td></td>
</tr>
<tr>
<td>631</td>
<td>Identify and prioritize critical business functions in collaboration with organizational stakeholders</td>
<td></td>
</tr>
<tr>
<td>640</td>
<td>Identify IT security program implications of new technologies or technology upgrades</td>
<td></td>
</tr>
<tr>
<td>650</td>
<td>Implement and enforce Computer Network Defense policies and procedures reflecting applicable laws, policies, procedures, and regulations (such as U.S. Codes 10 and 50)</td>
<td></td>
</tr>
<tr>
<td>674</td>
<td>Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information</td>
<td></td>
</tr>
<tr>
<td>676</td>
<td>Interpret and/or approve security requirements relative to the capabilities of new information technologies</td>
<td></td>
</tr>
<tr>
<td>677</td>
<td>Interpret patterns of non compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s IA program</td>
<td></td>
</tr>
<tr>
<td>679</td>
<td>Lead and align IT security priorities with the organization’s mission and vision</td>
<td></td>
</tr>
<tr>
<td>680</td>
<td>Lead and oversee information security budget, staffing, and contracting</td>
<td></td>
</tr>
<tr>
<td>705</td>
<td>Manage the monitoring of external Computer Network Defense data sources to maintain enterprise situational awareness</td>
<td></td>
</tr>
<tr>
<td>706</td>
<td>Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs, etc.) for the enterprise constituency</td>
<td></td>
</tr>
<tr>
<td>TASK ID</td>
<td>KSA</td>
<td>Statement</td>
</tr>
<tr>
<td>---------</td>
<td>-----</td>
<td>-----------</td>
</tr>
<tr>
<td>707</td>
<td></td>
<td>Manage threat or target analysis of Computer Network Defense information and production of threat information within the enterprise</td>
</tr>
<tr>
<td>711</td>
<td></td>
<td>Monitor and evaluate the effectiveness of the enterprise’s IA security safeguards to ensure they provide the intended level of protection</td>
</tr>
<tr>
<td>730</td>
<td></td>
<td>Oversee the information security training and awareness program</td>
</tr>
<tr>
<td>801</td>
<td></td>
<td>Provide enterprise IA guidance for development of the Continuity of Operations Plans</td>
</tr>
<tr>
<td>810</td>
<td></td>
<td>Provide leadership and direction to IT personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities</td>
</tr>
<tr>
<td>818</td>
<td></td>
<td>Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters</td>
</tr>
<tr>
<td>844</td>
<td></td>
<td>Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enterprise</td>
</tr>
<tr>
<td>848</td>
<td></td>
<td>Specify policy and coordinate review and approval</td>
</tr>
<tr>
<td>862</td>
<td></td>
<td>Track compliance of audit findings (Computer Network Defense findings), incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken</td>
</tr>
</tbody>
</table>
## PROTECT AND DEFEND

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
<td>Knowledge of applicable business processes and operations of customer organizations</td>
<td>Requirements Analysis</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
<td>Cryptography</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>Knowledge of disaster recovery continuity of operations plans</td>
<td>Incident Management</td>
</tr>
<tr>
<td>49</td>
<td></td>
<td>Knowledge of host/network access controls (e.g., access control list)</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>55</td>
<td></td>
<td>Knowledge of IA principles</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>61</td>
<td></td>
<td>Knowledge of incident response and handling methodologies</td>
<td>Incident Management</td>
</tr>
<tr>
<td>62</td>
<td></td>
<td>Knowledge of industry-standard and organizationally accepted analysis principles and methods</td>
<td>Logical Systems Design</td>
</tr>
<tr>
<td>66</td>
<td></td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>80</td>
<td></td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td></td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>84</td>
<td></td>
<td>Knowledge of network management principles, models, and tools</td>
<td>Network Management</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Knowledge of network systems management methods including end-to-end systems performance monitoring</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>Knowledge of network traffic analysis methods</td>
<td>Vulnerabilities Assessment</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Knowledge of new and emerging IT and information security technologies</td>
<td>Technology Awareness</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)</td>
<td>Vulnerabilities Assessment</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>Knowledge of resource management principles and techniques</td>
<td>Project Management</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>Knowledge of security management</td>
<td>Information Assurance</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods</td>
<td>Systems Life Cycle</td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>Knowledge of server and client operating systems</td>
<td>Operating Systems</td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
<td>Operating Systems</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., ISO) relating to system design</td>
<td>Requirements Analysis</td>
<td></td>
</tr>
<tr>
<td>129</td>
<td>Knowledge of systems lifecycle management principles</td>
<td>Systems Life Cycle</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>Knowledge of technology integration processes</td>
<td>Systems Integration</td>
<td></td>
</tr>
<tr>
<td>150</td>
<td>Knowledge of what constitutes a “threat” to a network</td>
<td>Information Systems/Network Security</td>
<td></td>
</tr>
<tr>
<td>299</td>
<td>Knowledge of information security program management and project management principles and techniques</td>
<td>Project Management</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>Skill in deconflicting cyber operations and activities</td>
<td>Political Savvy</td>
<td></td>
</tr>
<tr>
<td>919</td>
<td>Ability to promote awareness of security issues among management and ensure sound security principles are reflected in organizations’ visions and goals</td>
<td>Political Savvy</td>
<td></td>
</tr>
</tbody>
</table>
**PROTECT AND DEFEND**

**VULNERABILITY ASSESSMENT AND MANAGEMENT**

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>411</td>
<td></td>
<td>Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives</td>
</tr>
<tr>
<td>448</td>
<td></td>
<td>Conduct authorized penetration testing of enterprise network assets</td>
</tr>
<tr>
<td>685</td>
<td></td>
<td>Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions</td>
</tr>
<tr>
<td>692</td>
<td></td>
<td>Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing</td>
</tr>
<tr>
<td>744</td>
<td></td>
<td>Perform Computer Network Defense risk assessments within the enterprise</td>
</tr>
<tr>
<td>746</td>
<td></td>
<td>Perform Computer Network Defense vulnerability assessments within the enterprise</td>
</tr>
<tr>
<td>784</td>
<td></td>
<td>Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>4</td>
<td>Ability to identify systemic security issues based on the analysis of vulnerability and configuration data</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>10</td>
<td>Knowledge of application vulnerabilities</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>13</td>
<td>Knowledge of basic system, network, and operating system hardening techniques</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>17</td>
<td>Knowledge of certified ethical hacking principles and techniques</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>63</td>
<td>Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>85</td>
<td>Knowledge of network security architecture, including the application of Defense-In-Depth principles</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>92</td>
<td>Knowledge of Open System Interconnection model</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>95</td>
<td>Knowledge of penetration testing tools and techniques (e.g., metasploit, neosploit, etc.)</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>102</td>
<td>Knowledge of programming language structures and logic</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>150</td>
<td>Knowledge of what constitutes a “threat” to a network</td>
<td>Information Systems/Network Security</td>
</tr>
<tr>
<td>157</td>
<td>Skill in applying host/network access controls (e.g., access control list)</td>
<td>Identity Management</td>
</tr>
<tr>
<td>181</td>
<td>Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>210</td>
<td>Skill in mimicking threat behaviors</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>214</td>
<td>Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>225</td>
<td>Skill in the use of penetration testing tools and techniques</td>
<td>Vulnerabilities Assessment</td>
</tr>
<tr>
<td>226</td>
<td>Skill in the use of social engineering techniques</td>
<td>Human Factors</td>
</tr>
<tr>
<td>238</td>
<td>Skill in writing code in a modern programming language (e.g., Java, C++)</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>897</td>
<td>Skill in performing damage assessments</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>904</td>
<td>Knowledge of interpreted and compiled computer languages</td>
<td>Computer Languages</td>
</tr>
<tr>
<td>922</td>
<td>Skill in using network analysis tools to identify vulnerabilities</td>
<td>Vulnerabilities Assessment</td>
</tr>
</tbody>
</table>
INVESTIGATE

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

Investigation
Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
(Example job titles: Computer Crime Investigator; Special Agent)

Digital Forensics
Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.
(Example job titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Forensic Analyst (Cryptologic); Forensic Technician; Network Forensic Examiner).
### INVESTIGATE  DIGITAL FORENSICS

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>438</td>
<td></td>
<td>Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise</td>
</tr>
<tr>
<td>447</td>
<td></td>
<td>Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion</td>
</tr>
<tr>
<td>463</td>
<td></td>
<td>Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis</td>
</tr>
<tr>
<td>480</td>
<td></td>
<td>Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats</td>
</tr>
<tr>
<td>482</td>
<td></td>
<td>Decrypt seized data using technical means</td>
</tr>
<tr>
<td>541</td>
<td></td>
<td>Develop reports which organize and document recovered evidence and forensic processes used</td>
</tr>
<tr>
<td>564</td>
<td></td>
<td>Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)</td>
</tr>
<tr>
<td>573</td>
<td></td>
<td>Ensure chain of custody is followed for all digital media acquired (e.g., indications, analysis, and warning standard operating procedures)</td>
</tr>
<tr>
<td>613</td>
<td></td>
<td>Examine recovered data for items of relevance to the issue at hand</td>
</tr>
<tr>
<td>636</td>
<td></td>
<td>Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration</td>
</tr>
<tr>
<td>686</td>
<td></td>
<td>Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>743</td>
<td>Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation</td>
<td></td>
</tr>
<tr>
<td>749</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>752</td>
<td>Perform file signature analysis</td>
<td></td>
</tr>
<tr>
<td>753</td>
<td>Perform hash comparison against established database</td>
<td></td>
</tr>
<tr>
<td>758</td>
<td>Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)</td>
<td></td>
</tr>
<tr>
<td>759</td>
<td>Perform MAC timeline analysis on a file system</td>
<td></td>
</tr>
<tr>
<td>768</td>
<td>Perform static media analysis</td>
<td></td>
</tr>
<tr>
<td>771</td>
<td>Perform tier 1, 2, and 3 malware analysis</td>
<td></td>
</tr>
<tr>
<td>774</td>
<td>Perform Windows registry analysis</td>
<td></td>
</tr>
<tr>
<td>786</td>
<td>Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures)</td>
<td></td>
</tr>
<tr>
<td>817</td>
<td>Provide technical assistance on digital evidence matters to appropriate personnel</td>
<td></td>
</tr>
<tr>
<td>825</td>
<td>Recognize and accurately report forensic artifacts indicative of a particular operating system</td>
<td></td>
</tr>
<tr>
<td>839</td>
<td>Review forensic images and other data sources for recovery of potentially relevant information</td>
<td></td>
</tr>
<tr>
<td>867</td>
<td>Update hash comparison databases from various libraries (e.g., National Software Reference Library, National Security Agency/Central Security Service Information Systems Incident Response Team)</td>
<td></td>
</tr>
<tr>
<td>868</td>
<td>Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis</td>
<td></td>
</tr>
</tbody>
</table>
### Investigate

#### Digital Forensics

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>870</td>
<td>Use network monitoring tools to capture real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis</td>
</tr>
<tr>
<td>871</td>
<td>Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence</td>
</tr>
<tr>
<td>882</td>
<td>Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies</td>
</tr>
</tbody>
</table>

**Tasks below are critical for law enforcement and counterintelligence cybersecurity specialty only**

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>429</td>
<td>Assist in the gathering and preservation of evidence used in the prosecution of computer crimes</td>
</tr>
<tr>
<td>620</td>
<td>Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property</td>
</tr>
<tr>
<td>622</td>
<td>Formulate a strategy to insure chain of custody is maintained in such a way that the evidence is not altered (e.g., phones/PDAs need a power source, hard drives need protection from shock)</td>
</tr>
<tr>
<td>799</td>
<td>Provide consultation to investigators and prosecuting attorneys regarding the findings of computer examinations</td>
</tr>
<tr>
<td>819</td>
<td>Provide testimony related to computer examinations</td>
</tr>
<tr>
<td>846</td>
<td>Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.</td>
</tr>
<tr>
<td>872</td>
<td>Use an array of specialized computer investigative techniques and programs to resolve the investigation</td>
</tr>
</tbody>
</table>
**INVESTIGATE**

**DIGITAL FORENSICS**

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

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ID</strong></td>
<td><strong>Statement</strong></td>
</tr>
<tr>
<td>24</td>
<td>Knowledge of concepts and practices of processing digital information</td>
</tr>
<tr>
<td>25</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)</td>
</tr>
<tr>
<td>29</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools</td>
</tr>
<tr>
<td>61</td>
<td>Knowledge of incident response and handling methodologies</td>
</tr>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
</tr>
<tr>
<td>113</td>
<td>Knowledge of server and client operating systems</td>
</tr>
<tr>
<td>114</td>
<td>Knowledge of server diagnostic tools and fault identification techniques</td>
</tr>
<tr>
<td>122</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems</td>
</tr>
<tr>
<td>153</td>
<td>Skill in analyzing malware</td>
</tr>
<tr>
<td>264</td>
<td>Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)</td>
</tr>
</tbody>
</table>
## INVESTIGATE

### DIGITAL FORENSICS

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

#### Digital Forensics

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>389</td>
<td>Skill in disassembling PCs</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>888</td>
<td>Knowledge of types of digital forensics data and how to recognize them</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>889</td>
<td>Knowledge of deployable forensics</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>890</td>
<td>Knowledge of forensics in multiple operating system environments</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>908</td>
<td>Ability to decrypt digital data collections</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>923</td>
<td>Knowledge of security event correlation tools</td>
<td>Information Systems/Network Security</td>
</tr>
</tbody>
</table>

**KSAs below are critical for law enforcement and counterintelligence cybersecurity professionals only**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>217</td>
<td>Skill in seizing and preserving digital evidence</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>310</td>
<td>Knowledge of legal governance related to admissibility (Federal Rules of Evidence)</td>
<td>Criminal Law</td>
</tr>
<tr>
<td>360</td>
<td>Skill in finding and extracting information of evidentiary value</td>
<td>Computer Forensics</td>
</tr>
</tbody>
</table>
# INVESTIGATE

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

*Sample Job Titles: Computer Crime Investigator, Special Agent*

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>402</td>
<td></td>
<td>Analyze computer-generated threats</td>
</tr>
<tr>
<td>429</td>
<td></td>
<td>Assist in the gathering and preservation of evidence used in the prosecution of computer crimes</td>
</tr>
<tr>
<td>447</td>
<td></td>
<td>Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion</td>
</tr>
<tr>
<td>454</td>
<td></td>
<td>Conduct interviews and interrogations of victims, witnesses, and suspects</td>
</tr>
<tr>
<td>507</td>
<td></td>
<td>Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion</td>
</tr>
<tr>
<td>512</td>
<td></td>
<td>Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet</td>
</tr>
<tr>
<td>564</td>
<td></td>
<td>Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)</td>
</tr>
<tr>
<td>597</td>
<td></td>
<td>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)</td>
</tr>
<tr>
<td>613</td>
<td></td>
<td>Examine recovered data for items of relevance to the issue at hand</td>
</tr>
<tr>
<td>620</td>
<td></td>
<td>Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property</td>
</tr>
<tr>
<td>623</td>
<td></td>
<td>Fuse computer network attack analyses with criminal and counterintelligence investigations and operations</td>
</tr>
<tr>
<td>633</td>
<td></td>
<td>Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action</td>
</tr>
<tr>
<td>635</td>
<td></td>
<td>Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>636</td>
<td>Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration</td>
<td></td>
</tr>
<tr>
<td>637</td>
<td>Identify elements of the crime</td>
<td></td>
</tr>
<tr>
<td>642</td>
<td>Identify outside attackers accessing the system from Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges</td>
<td></td>
</tr>
<tr>
<td>649</td>
<td>Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations</td>
<td></td>
</tr>
<tr>
<td>663</td>
<td>Independently conduct large-scale investigations of criminal activities involving complicated computer programs and networks</td>
<td></td>
</tr>
<tr>
<td>788</td>
<td>Prepare reports to document analysis</td>
<td></td>
</tr>
<tr>
<td>792</td>
<td>Process crime scenes</td>
<td></td>
</tr>
<tr>
<td>843</td>
<td>Secure the electronic device or information source</td>
<td></td>
</tr>
<tr>
<td>871</td>
<td>Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence</td>
<td></td>
</tr>
</tbody>
</table>
Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

*Sample Job Titles: Computer Crime Investigator, Special Agent*

<table>
<thead>
<tr>
<th>Task</th>
<th>KSA</th>
<th>Knowledge of pertinent government laws and information technology regulations</th>
<th>Legal, Government and Jurisprudence</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>97</td>
<td></td>
<td>Skill in seizing and preserving digital evidence</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>105</td>
<td></td>
<td>Knowledge of electronic devices such as computer systems and their components, access control devices, digital cameras, handheld devices, electronic organizers, hard drives, memory cards, modems, network components, connectors, pagers, printers, removable storage devices scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems, and other miscellaneous electronic items</td>
<td>Hardware</td>
</tr>
<tr>
<td>217</td>
<td></td>
<td>Knowledge of Forensic Chain of Evidence</td>
<td>Forensics</td>
</tr>
<tr>
<td>281</td>
<td></td>
<td>Knowledge of laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)</td>
<td>Forensics</td>
</tr>
<tr>
<td>290</td>
<td></td>
<td>Knowledge of legal governance related to admissibility (Federal Rules of Evidence)</td>
<td>Criminal Law</td>
</tr>
<tr>
<td>305</td>
<td></td>
<td>Knowledge of processes for packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data</td>
<td>Criminal Law</td>
</tr>
<tr>
<td>310</td>
<td></td>
<td>Knowledge of types and collection of persistent data</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>340</td>
<td></td>
<td>Skill in processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data</td>
<td>Forensics</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>383</td>
<td>Skill in using scientific rules and methods to solve problems</td>
<td>Reasoning</td>
<td></td>
</tr>
<tr>
<td>917</td>
<td>Knowledge of social dynamics of computer attackers in a global context</td>
<td>External Awareness</td>
<td></td>
</tr>
</tbody>
</table>
Operate and Collect

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

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

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

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

No Tasks or KSAs are available for these specialty areas
ANALYZE

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

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

Exploitation Analysis
Analyzes collected information to identify vulnerabilities and potential for exploitation.

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.

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

No Tasks or KSAs are available for these specialty areas
SUPPORT

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

Legal Advice and Advocacy

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

(Example job titles: Legal Advisor/SJA)

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.

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

Education and Training

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

(Example job titles: Cyber Trainer; Information Security Trainer; Security Training Coordinator)
**LEGAL ADVICE AND ADVOCACY**

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

*Sample Job Titles: Legal Advisor/SJA*

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

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

*Sample Job Titles: Legal Advisor/SJA*

<table>
<thead>
<tr>
<th>TASK</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
</tr>
<tr>
<td>88</td>
<td>Knowledge of new and emerging IT and information security technologies</td>
</tr>
<tr>
<td>97</td>
<td>Knowledge of pertinent government laws and information technology regulations</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
</tr>
<tr>
<td>244</td>
<td>Ability to determine the validity of technology trend data</td>
</tr>
<tr>
<td>250</td>
<td>Knowledge of administrative/criminal legal cyber guidelines</td>
</tr>
<tr>
<td>253</td>
<td>Knowledge of applicable statutes in Title 10 of the U.S. Code</td>
</tr>
<tr>
<td>255</td>
<td>Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)</td>
</tr>
<tr>
<td>257</td>
<td>Knowledge of applicable statutes in Title 32 of the U.S. Code</td>
</tr>
<tr>
<td>259</td>
<td>Knowledge of applicable statutes in Title 50 of the U.S. Code (War and National Defense)</td>
</tr>
<tr>
<td>279</td>
<td>Knowledge of Electronic Communications Privacy Act (ECPA)</td>
</tr>
<tr>
<td>282</td>
<td>Knowledge of emerging computer-based technology that have potential for exploitation by adversaries</td>
</tr>
<tr>
<td>Task ID</td>
<td>Statement</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>288</td>
<td>Knowledge of Foreign Intelligence Surveillance Act and Protect America Act laws and regulations associated with electronic surveillance</td>
</tr>
<tr>
<td>297</td>
<td>Knowledge of industry indicators useful for identifying technology trends</td>
</tr>
<tr>
<td>300</td>
<td>Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions</td>
</tr>
<tr>
<td>318</td>
<td>Knowledge of Presidential Directives and executive branch guidelines that apply to cyber activities</td>
</tr>
<tr>
<td>323</td>
<td>Knowledge of search and seizure laws</td>
</tr>
<tr>
<td>333</td>
<td>Knowledge of the implications of the Bill of Rights (Amendments 1-10 of the U.S. Constitution) for cybersecurity</td>
</tr>
<tr>
<td>338</td>
<td>Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence</td>
</tr>
<tr>
<td>339</td>
<td>Knowledge of the structure and intent of military operation plans, concept operation plans, orders, and standing rules of engagement</td>
</tr>
<tr>
<td>377</td>
<td>Skill in tracking and analyzing technical and legal trends that will impact cyber activities</td>
</tr>
</tbody>
</table>
**STRATEGIC PLANNING AND POLICY DEVELOPMENT**

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

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>KSA</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>410</td>
<td></td>
<td>Analyze organizational information security policy</td>
</tr>
<tr>
<td>424</td>
<td></td>
<td>Assess policy needs and collaborate with stakeholders to develop policies to govern IT activities</td>
</tr>
<tr>
<td>485</td>
<td></td>
<td>Define current and future business environments</td>
</tr>
<tr>
<td>492</td>
<td></td>
<td>Design a cybersecurity strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan</td>
</tr>
<tr>
<td>524</td>
<td></td>
<td>Develop and maintain strategic plans</td>
</tr>
<tr>
<td>539</td>
<td></td>
<td>Develop policy, programs, and guidelines for implementation</td>
</tr>
<tr>
<td>565</td>
<td></td>
<td>Draft and publish security policy</td>
</tr>
<tr>
<td>594</td>
<td></td>
<td>Establish and maintain communication channels with stakeholders</td>
</tr>
<tr>
<td>629</td>
<td></td>
<td>Identify and address IT workforce planning and management issues, such as recruitment, retention, and training</td>
</tr>
<tr>
<td>641</td>
<td></td>
<td>Identify organizational policy stakeholders</td>
</tr>
<tr>
<td>720</td>
<td></td>
<td>Monitor the rigorous application of information security/information assurance policies, principles, and practices in the delivery of planning and management services</td>
</tr>
<tr>
<td>724</td>
<td></td>
<td>Obtain consensus on proposed policy change from stakeholders</td>
</tr>
<tr>
<td>812</td>
<td></td>
<td>Provide policy guidance to IT management, staff, and users</td>
</tr>
<tr>
<td>838</td>
<td></td>
<td>Review existing and proposed policies with stakeholders</td>
</tr>
<tr>
<td>840</td>
<td></td>
<td>Review or conduct audits of IT programs and projects</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>847</td>
<td>Serve on agency and interagency policy boards</td>
<td></td>
</tr>
<tr>
<td>854</td>
<td>Support the CIO in the formulation of IT-related policies</td>
<td></td>
</tr>
<tr>
<td>884</td>
<td>Write Information Assurance (IA) policy and instructions.</td>
<td></td>
</tr>
</tbody>
</table>
### Strategic Planning and Policy Development

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Knowledge of cryptology</td>
<td>Cryptography</td>
</tr>
<tr>
<td>45</td>
<td>Knowledge of existing IA security principles, policies, and procedures</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>88</td>
<td>Knowledge of new and emerging IT and information security technologies</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>105</td>
<td>Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>244</td>
<td>Ability to determine the validity of technology trend data</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>250</td>
<td>Knowledge of administrative/criminal legal cyber guidelines</td>
<td>Criminal Law</td>
</tr>
<tr>
<td>253</td>
<td>Knowledge of applicable statutes in Title 10 of the U.S. Code</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>255</td>
<td>Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>257</td>
<td>Knowledge of applicable statutes in Title 32 of the U.S. Code</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>259</td>
<td>Knowledge of applicable statutes in Title 50 of the U.S. Code (War and National Defense)</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>279</td>
<td>Knowledge of Electronic Communications Privacy Act (ECPA)</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>282</td>
<td>Knowledge of emerging computer-based technology that have potential for exploitation by adversaries</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>288</td>
<td>Knowledge of Foreign Intelligence Surveillance Act and Protect America Act laws and regulations associated with electronic surveillance</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>297</td>
<td>Knowledge of industry indicators useful for identifying technology trends</td>
<td>Technology Awareness</td>
</tr>
<tr>
<td>300</td>
<td>Knowledge of intelligence reporting principles, policies, procedures, and vehicles,</td>
<td>Organizational Awareness</td>
</tr>
<tr>
<td></td>
<td>including report formats, reportability criteria (requirements and priorities),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dissemination practices, and legal authorities and restrictions</td>
<td></td>
</tr>
<tr>
<td>318</td>
<td>Knowledge of Presidential Directives and executive branch guidelines that apply to</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td></td>
<td>cyber activities</td>
<td></td>
</tr>
<tr>
<td>320</td>
<td>Knowledge of private-sector organizations and academic institutions dealing with cyber-</td>
<td>External Awareness</td>
</tr>
<tr>
<td></td>
<td>security issues</td>
<td></td>
</tr>
<tr>
<td>323</td>
<td>Knowledge of search and seizure laws</td>
<td>Criminal Investigation</td>
</tr>
<tr>
<td>333</td>
<td>Knowledge of the implications of the Bill of Rights (Amendments 1-10 of the U.S.</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td></td>
<td>Constitution) for cybersecurity</td>
<td></td>
</tr>
<tr>
<td>336</td>
<td>Knowledge of the nature and function of the National Information Infrastructure</td>
<td>Telecommunications</td>
</tr>
<tr>
<td>338</td>
<td>Knowledge of the principal methods, procedures, and techniques of gathering information</td>
<td>Reasoning</td>
</tr>
<tr>
<td></td>
<td>and producing, reporting, and sharing intelligence</td>
<td></td>
</tr>
<tr>
<td>377</td>
<td>Skill in tracking and analyzing technical and legal trends that will impact cyber activities</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>887</td>
<td>Knowledge of human system integration principles including accessibility factors and</td>
<td>Human Factors</td>
</tr>
<tr>
<td></td>
<td>standards</td>
<td></td>
</tr>
<tr>
<td>918</td>
<td>Ability to prepare and deliver education and awareness briefings to ensure that systems,</td>
<td>Teaching Others</td>
</tr>
<tr>
<td></td>
<td>network, and data users are aware of and adhere to systems security policies and procedures</td>
<td></td>
</tr>
<tr>
<td>919</td>
<td>Ability to promote awareness of security issues among management and ensure sound security</td>
<td>Political Savvy</td>
</tr>
<tr>
<td></td>
<td>principles are reflected in organizations’ visions and goals</td>
<td></td>
</tr>
</tbody>
</table>
Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

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

<table>
<thead>
<tr>
<th>TASK ID</th>
<th>TASK DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>453</td>
<td>Conduct interactive training exercises to create an effective learning environment</td>
</tr>
<tr>
<td>479</td>
<td>Correlate mission requirements to training</td>
</tr>
<tr>
<td>490</td>
<td>Deliver training courses tailored to the audience and physical environment</td>
</tr>
<tr>
<td>491</td>
<td>Demonstrate concepts, procedures, software, equipment, and technology applications to coworkers, subordinates, or others</td>
</tr>
<tr>
<td>504</td>
<td>Design training curriculum and course content</td>
</tr>
<tr>
<td>510</td>
<td>Determine training requirements (e.g., subject matter, format, location)</td>
</tr>
<tr>
<td>538</td>
<td>Develop new or identify existing awareness and training materials that are appropriate for intended audiences</td>
</tr>
<tr>
<td>551</td>
<td>Develop the goals and objectives for cybersecurity training, education, or awareness</td>
</tr>
<tr>
<td>567</td>
<td>Educate customers in established procedures and processes to ensure professional media standards are met</td>
</tr>
<tr>
<td>587</td>
<td>Ensure that information security personnel are receiving the appropriate level and type of training</td>
</tr>
<tr>
<td>588</td>
<td>Ensure that information security personnel can identify the limits of their capabilities (legally, technically, and skill) and the organization that may assist</td>
</tr>
<tr>
<td>606</td>
<td>Evaluate the effectiveness and comprehensiveness of existing training programs</td>
</tr>
<tr>
<td>624</td>
<td>Guide new and junior coworkers through career development and training choices</td>
</tr>
<tr>
<td>778</td>
<td>Plan classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>779</td>
<td>Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)</td>
</tr>
<tr>
<td>833</td>
<td>Report tactical or strategic information derived from forensic processes through appropriate law enforcement/counter-intelligence channels.</td>
</tr>
<tr>
<td>841</td>
<td>Review training documentation (e.g., Course Content Documents [COD], Lesson Plans, Student Texts, examinations, Schedules of Instruction [SOI], course descriptions)</td>
</tr>
<tr>
<td>842</td>
<td>Revise curriculum and course content based on feedback from previous training sessions</td>
</tr>
<tr>
<td>845</td>
<td>Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media, cartography)</td>
</tr>
<tr>
<td>855</td>
<td>Support the design and execution of exercise scenarios</td>
</tr>
<tr>
<td>885</td>
<td>Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce</td>
</tr>
</tbody>
</table>
Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Statement</th>
<th>Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>81</td>
<td>Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services</td>
<td>Infrastructure Design</td>
</tr>
<tr>
<td>90</td>
<td>Knowledge of operating systems</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>246</td>
<td>Knowledge and experience in the Instructional System Design methodology</td>
<td>Multimedia Technologies</td>
</tr>
<tr>
<td>252</td>
<td>Knowledge of and experience in Insider Threat investigations, reporting, investigative tools, and laws/regulations</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>253</td>
<td>Knowledge of applicable statutes in Title 10 of the U.S. Code</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>255</td>
<td>Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure)</td>
<td>Legal, Government and Jurisprudence</td>
</tr>
<tr>
<td>264</td>
<td>Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)</td>
<td>Computers and Electronics</td>
</tr>
<tr>
<td>305</td>
<td>Knowledge of laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)</td>
<td>Forensics</td>
</tr>
<tr>
<td>314</td>
<td>Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain</td>
<td>Teaching Others</td>
</tr>
<tr>
<td>ID</td>
<td>Statement</td>
<td>Competency</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>332</td>
<td>Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience</td>
<td>Teaching Others</td>
</tr>
<tr>
<td>344</td>
<td>Knowledge of virtualization technologies and virtual machine development and maintenance</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>359</td>
<td>Skill in developing and executing technical training programs and curricula</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>363</td>
<td>Skill in identifying gaps in technical capabilities</td>
<td>Teaching Others</td>
</tr>
<tr>
<td>376</td>
<td>Skill in talking to others to convey information effectively</td>
<td>Oral Communication</td>
</tr>
<tr>
<td>918</td>
<td>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</td>
<td>Teaching Others</td>
</tr>
</tbody>
</table>