Software Assurance Professional Competency Model

October 2012

General Cybersecurity Role Overview

Software Assurance Professional Overview	
OPM Series	2210, INFOSEC Parenthetical
GS-Level	GS - 12 through GS - 15
DHS Agency/Component	National Protection and Programs Directorate (NPPD)/Cybersecurity and Communications (CS&C) Software Assurance
Related Roles	• Software Assurance Engineer • Cyber Software Assurance Developer/Integrator • Information Security Systems & Software Development Professional (ISSSDP) • Security Test Engineer
Typical Degrees/Formal Education	• Master of Science (M.S.), Computer Science • Master of Information Systems (MIS) • Master of Software Assurance (MSwA) • Master of Science (M.S.), Software Engineering • Certificate of Software Assurance (associated with M.S.)
Preferred Professional Certifications	• Certified Secure Software Lifecycle Professional (CSSLP) • Secure Development (GIAC) **NOTE:** These certifications are not required within the role; however acquiring these certifications may be beneficial to successful job performance.
Description	As a multi-disciplinary cyber security function, Software Assurance (SwA) advances and enables security and resilience of software throughout the lifecycle. Addresses means to reduce exploitable software weaknesses and improve capabilities that routinely develop, acquire, and deploy resilient software products. Provides infrastructure for SwA Community of Practice (COP) and enables interagency public-private collaboration on SwA to increase use and awareness of SwA resources. Advances the use of software-relevant rating schemes. Collaborates in the development and publishing of software security content and SwA curriculum courseware and material focused on integrating software security content into relevant education and training programs. Enables software security automation and measurement capabilities through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, structured threat information, cyber observables, and common attacks which target software; enhances software transparency and security diagnostic & measurement capabilities. Example activities of the Software Assurance Professional include one or more of the following: • Enhancing development and acquisition processes and capability benchmarking to address software security needs • Transitioning software assurance processes and practices into standards and maturity models suitable for voluntary adoption • Managing software assurance projects by effectively balancing scope, costs, and boundaries with customer needs • Collaborating in the development and publishing of software security content and software assurance (SwA) curriculum courseware and material • Developing methods to monitor and measure new compliance standards • Documenting design specifications, installation instructions, and other software-related information • Identifying security and resilience expectations based on target requirements • Coordinating with other agencies to develop integration plans for new SwA training courses • Assessing policy needs by considering the needs of the organization and collaborating with stakeholders and executive leadership • Providing an infrastructure for the SwA Community of Practice (COP)

Software Assurance Professional Overview	
	• Organizing topics and key points according to guidance for risks relevant to software-reliant capabilities • Conducting assessments of software system threats and vulnerabilities • Conducting comparative analysis of customer needs and available research and industry trends/technologies
Special Note	• SwA is a multi-disciplinary cyber security function requiring a team with several specialty areas (competencies). This CS&C Software Assurance Professional cybersecurity competency model is intended to provide a means for supporting NICE's nationally coordinated effort to focus on cybersecurity awareness, training, and professional development. This model contains role-specific cybersecurity competencies that can be used to establish a baseline for the DHS Cybersecurity Workforce Initiative (CWI) and inform workforce development and talent management activities for cybersecurity roles across DHS. This model was not developed with the intention of supporting formal hiring/selection or performance management (i.e., performance appraisals). Role dependent, it is not expected that any single individual would possess all the competencies. • The Typical Degrees / Formal Education listed above are examples of degrees/formal education individuals in this role typically hold. Formal training, plus requisite years of experience (e.g., similar industry or military experience) can potentially be substituted

Software Assurance Professional Competency Model (Summary)

Specialty Area (Competency)	Definition
Software Assurance and Security Engineering	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
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.
Vulnerability Assessment and Management	Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
Cyber Threat Analysis	Using cyber means, identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produce findings to help initialize or support law enforcement and counterintelligence investigations or activities.
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.
Systems Security 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.
Strategic Planning and Policy Development	Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identifies 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.
Technology Research and Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.
Education and Training	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.
Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Key to Reading the Competency Model

<table>
<tr><td>Specialty Area Title</td><td colspan="2">Specialty Area Definition: This definition is like a mission statement for the specialty area. It is a broad statement that sets the scope for the specialty.</td></tr>
<tr><td colspan="3">Example Tasks Identified as Part of Competency:
• These tasks are included to give context around the competency. This is not meant to be an exhaustive list, but rather a few examples that came up during the conversation with the subject matter experts.</td></tr>
<tr><td colspan="3">BEHAVIORAL INDICATORS
<i>(Describes how the competency manifests itself in observable on-the-job behavior)</i></td></tr>
<tr><td>1
Basic</td><td colspan="2">• This is the <b>basic</b> level of proficiency. At this level, the individual understands the subject matter and is seen as someone who can perform basic or developmental level work in activities requiring this specialty. The individual is capable of demonstrating this specialty after being given specific instructions and guidance and can engage in general conversation about this specialty. The individual implements with frequent help - often depending on others to perform specialty.</td></tr>
<tr><td>2
Intermediate</td><td colspan="2">• This is the <b>intermediate</b> level of proficiency. At this level, the individual can apply the subject matter and is considered someone who has the capability to fully perform work that requires application of this specialty. The individual is capable of demonstrating this specialty in straightforward and routine situations and can contribute knowledge or new ideas in applying this specialty. The individual implements with little help and works independently most of the time.</td></tr>
<tr><td>3
Advanced</td><td colspan="2">• This is the <b>advanced</b> level of proficiency. At this level, the individual can analyze the subject matter and is seen as someone who can immediately contribute to the success of work requiring this specialty. The individual is confident in serving as an advisor and is sought out to provide insight into the application of this specialty. The individual works independently and coaches and leads others.</td></tr>
<tr><td>4
Expert</td><td colspan="2">• This is the <b>expert</b> level of proficiency. At this level the individual can synthesize/evaluate the subject matter and is looked to as an expert in this specialty. Others view this individual as a role model capable of leading or teaching others in this area and they consult with him/her for assistance or guidance with work requiring this specialty. The individual obtains best-in-class results, setting the standard for performance.</td></tr>
<tr><td colspan="3">CRITICALITY</td></tr>
<tr><td>Importance</td><td>Required at Entry</td><td>Criticality</td></tr>
<tr><td>Establishes the significance of the competency to successful performance in the occupation
1 = Not at all Important
5 = Extremely Important</td><td>Identifies the competencies required on day 1 of the job versus those that can be learned over time
1 = Not Required
3 = Definitely Required</td><td>An evaluation of Importance and Required at Entry ratings to determine which competencies could be used to make personnel decisions</td></tr>
<tr><td colspan="3">PROFICIENCY TARGETS</td></tr>
<tr><td>Entry/Apprentice (GS-#-#)</td><td>Journey (GS-#-#)</td><td>Senior/Master (GS-#-#)</td></tr>
<tr><td colspan="3"><i>Identifies the proficiency at which a person in a specific career level should be performing. Aligns with the Behavioral Indicator descriptions above (Career levels will differ by occupation)</i></td></tr>
</table>

Software Assurance Professional Competency Model

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

Example Tasks Identified as Part of Competency:

- Collaborates in the development and publishing of software security content and software assurance (SwA) curriculum courseware and material
- Enhances development and acquisition processes and capability benchmarking
- Contributes software engineering and assurance knowledge by supporting activities in the advancement of software-relevant rating schemes

BEHAVIORAL INDICATORS

1 Basic	• Demonstrates basic knowledge of software engineering and assurance frameworks to describe software security automation and measurement capabilities • Demonstrates basic knowledge of software assurance when working with a mentor to assist in the integration of products
2 Intermediate	• Contributes software engineering and assurance knowledge by supporting activities in the advancement of software-relevant rating schemes and when integrating products with information assurance/information security safeguards • Applies knowledge of information systems security, ethical hacking, multiple network analysis, configuration management, integration, and deployment issues when supporting the secure design, development, testing, integration, implementation, sustainment and/or documentation of software applications
3 Advanced	• Applies advanced knowledge in information security, ethical hacking, multiple network analysis, configuration management, integration, and deployment issues to collaborate in the development and publishing of software security content and software assurance (SwA) curriculum courseware and material focused on integrating security content into relevant education and training programs • Lends advanced knowledge of software assurance and enterprise architecture to coordinate and collaborate across the organization and serve as a trusted advisor, providing input into architectural design and development of enterprise-wide applications, systems and services
4 Expert	• Blends software assurance and leadership expertise to support a wide range of technical and programmatic activities for program offices, to include leading the review and assessment of software system architecture, system requirements, and their allocation to lower level specifications; and overseeing design, code and test activities, trade off studies, software verification and validation (V&V), and system testing and integration • Enhances development and acquisition processes and capability benchmarking to address software security needs, and transitions software assurance processes and practices into standards and maturity models suitable for voluntary adoption • Enables interagency public-private collaboration on software assurance to increase use and awareness of software assurance resources • Serves as senior advisor on architectural design and development of enterprise-wide application and integrates policies and procedures across government agencies • Lends software assurance program strategic sourcing expertise by serving as a senior advisor to procurement and contract management in support of systems and software acquisitions • Lends expert software engineering and assurance expertise to oversee and enable software security automation and measurement capabilities through development and oversight of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks, which target software; enhances software transparency and security diagnostic and measurement capabilities throughout the agency and across federal government

CRITICALITY

Importance	Required at Entry	Criticality
Extremely Important	Definitely Required	Extremely Important – Definitely Required at Entry

PROFICIENCY TARGETS

<table>
<tr><th>Software Assurance and Security Engineering</th><th colspan="2">Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.</th></tr>
<tr><td>Project Lead
(GS 12/13)</td><td>Senior
(GS 14)</td><td>Director
(GS 15)</td></tr>
<tr><td>3 - Advanced</td><td>4 - Expert</td><td>4 - Expert</td></tr>
</table>

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. Ensure compliance from internal and external perspectives.

Example Tasks Identified as Part of Competency:

- Develops methods to monitor and measure new compliance standards
- Creates protocols, procedures, and guidelines to mitigate security risks
- Performs validation steps, comparing actual results with expected results and identifying impact and risk
- Provides input to software Certification and Accreditation (C&A) process, activities, and related documentation (e.g., system life-cycle support plans, concepts of operations, operational procedures and maintenance of training materials)

BEHAVIORAL INDICATORS

1 Basic	• Demonstrates basic knowledge of static and dynamic analysis to assist in the identification of vulnerabilities in applications, across databases, networks, network-based environments, and operating systems • Identifies risks and tests management, operational, technical and security controls of a system against general guidelines (i.e., NIST 500 and 800 series) when providing input to simple vulnerability assessment activities • Lends basic knowledge of software security certification and accreditation requirements to monitor software security requirements and identify suspected anomalies; seeks appropriate technical experts to validate findings
2 Intermediate	• Applies knowledge of static and dynamic analysis to identify vulnerabilities in applications, across databases, networks, network-based environments, and operating systems, and makes recommendations for remediation when appropriate • Applies knowledge of software security certification and accreditation requirements to monitor and evaluate a system's compliance with software security requirements; and perform validation steps, comparing actual results with expected results and identifying impact and risk
3 Advanced	• Lends advanced knowledge in software assurance to provide input into leadership decisions to advance static and dynamic analysis reporting for applications, across databases, networks, network-based environments, and operating systems, and direct remediation as appropriate; creates protocols, procedures, and guidelines to mitigate security risks • Lends advanced knowledge of software architecture (e.g., topology, protocols) to develop methods to monitor and measure new compliance standards by assessing current protocols and procedures and determining the most efficient course of action
4 Expert	• Oversees and evaluates policies, procedures, and mechanisms to ensure compliance with the information assurance framework by assessing them against new software security principles, regulations, and mandates; thereby promoting and enabling security resilience of software throughout the lifecycle • Plans strategies and builds consensus (internal and external to the organization) for the integration and implementation of information assurance strategies by identifying key stakeholders and gaining their input • Lends expert software engineering and assurance frameworks to oversee and enable software security automation and measurement capabilities through development and oversight of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks, which target software • Enhances software transparency and security diagnostic and measurement capabilities and oversees the development of protocols, procedures, and guidelines that mitigate security risks

CRITICALITY

Importance	Required at Entry	Criticality
Very Important	Definitely Required	Very Important – Definitely Required at Entry

PROFICIENCY TARGETS

Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
3 - Advanced	4 - Expert	4 - Expert

Vulnerability Assessment and Management	Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
Example Tasks Identified as Part of Competency: • Conducts assessments of software system threats and vulnerabilities • Presents and prepares publications on security assessment functions to contribute to Vulnerability Assessment Management activities within the organization • Reviews threat and vulnerability assessment findings to quantify and prioritize vulnerabilities in a system	
BEHAVIORAL INDICATORS	
1 Basic	• Applies basic data gathering approaches and knowledge of computer systems and related information security software and hardware components, network systems and databases to collect and assemble documentation for a systems assessment • Demonstrates basic knowledge of static and dynamic analysis to assist in the identification of vulnerabilities in applications, across databases, networks, network-based environments, and operating systems
2 Intermediate	• Applies best practices and/or recognized methodology to perform an evaluation of software systems and operations; analyzes the results of evaluations against codes of practices and provides recommendations and next steps for action • Lends knowledge of software security aspects, such as coding, operating systems, programing languages and policies when conducting assessments of software system threats and vulnerabilities; aggregates and synthesizes findings to create metrics of vulnerabilities, findings and recommendations and develops reports for senior management review • Lends knowledge of vulnerabilities in software systems and attack patterns when performing vulnerability and risk assessments for the purposes of preparing assessment reports that identify technical and procedural findings • Applies knowledge of static and dynamic analysis to identify vulnerabilities in applications, across databases, networks, network-based environments, and operating systems, and makes recommendations for remediation when appropriate • Uses analytical skills and employs critical thinking to identify operational vulnerabilities and consequences to the stability of software assurance
3 Advanced	• Interprets and applies organizational security guidelines to act as team lead and oversee threat and vulnerability assessments for software systems, determine deviations from acceptable configurations and recommend appropriate mitigations and countermeasures • Applies advanced knowledge of information system security, ethical hacking, multiple network analysis, configuration management, and integration when assessing vulnerability assessment findings and devising mitigation and remediation strategies • Ensures activities accurately reflect the vulnerability assessment process by reviewing current information systems security safeguards and operations, and mapping operational processes to appropriate guidelines • Applies advanced knowledge of static and dynamic analysis to identify vulnerabilities in system designs, applications, and operating systems, and makes recommendations for remediation when appropriate • Reviews threat and vulnerability assessment findings to quantify and prioritize vulnerabilities in a system and take necessary actions to either mitigate or accept known risks (i.e., residual risk) based upon experience • Shares best practices for adhering to established guidelines when conducting assessments of threats and vulnerabilities by reviewing and validating testing reports for quality and providing a comprehensive depiction of security functions

Vulnerability Assessment and Management	Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
4 Expert	• Lends expert software engineering and assurance frameworks to oversee and enable software security automation and measurement capabilities through development and oversight of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks, which target software; enhances software transparency and security vulnerability, diagnostic and measurement capabilities throughout the agency and across federal government • Leverages expert knowledge in vulnerability scanning, network, and/or system and operating hardening techniques and hacking principles to conduct research on continuous improvement and present and prepare publications on security assessment functions to contribute to Vulnerability Assessment Management activities within the organization • Applies expertise in vulnerabilities assessment, computer network defense and software assurance to manage and coordinate assessment program activities, develop program plans, and budget resources and personnel • Ensures options for consideration reflect Homeland Security goals in cybersecurity practice and support infrastructure protection via cybersecurity capacity and capability building • Interfaces with various levels of evaluation stakeholders about the results of a vulnerability assessment (gaps in practice, process, and capability, etc.) and lends expert knowledge by providing recommendations and next steps after the evaluation • Performs risk management activities by using evaluation results to create or enhance the quality of deliverables and informational products aimed to mitigate gaps and vulnerabilities • Shares best practices for adhering to established guidelines when conducting assessments of threats and vulnerabilities by reviewing and validating reports for quality and comprehensive depiction of security assessment functions

CRITICALITY		
Importance	**Required at Entry**	**Criticality**
Very Important	Definitely Required	Very Important – Definitely Required at Entry
PROFICIENCY TARGETS		
Project Lead (GS 12/13)	**Senior (GS 14)**	**Director (GS 15)**
3 - Advanced	4 - Expert	4 - Expert

Cyber Threat Analysis	Using cyber means, identify and assess the capabilities and activities of cyber criminals or foreign intelligence entities; produce findings to help initialize or support law enforcement and counterintelligence investigations or activities.
Example Tasks Identified as Part of Competency: • Organizes topics and key points according to guidance for threats that target software-reliant capabilities • Collects intelligence and actively identifies cyber-threats and counterintelligence information • Reports risk exposures based on security automation that uses common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks, which target software	
BEHAVIORAL INDICATORS	
1 Basic	• Applies basic knowledge of front-end collection systems, including network traffic collection, filtering, and selection to collect intelligence and actively identify cyber-threats and counterintelligence information • Follows industry-standard and organizationally accepted analysis principles and methods to assist in determining risk exposures based on collected data
2 Intermediate	• Applies knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise to organize topics and key points according to guidance for threats that target software-reliant capabilities • Applies knowledge of static and dynamic analysis to identify malware, vulnerabilities and exploitable weaknesses in applications, databases, networks, network-based environments, and operating systems, and makes recommendations for remediation when appropriate
3 Advanced	• Lends advanced knowledge of common adversary tactics, techniques, and procedures in assigned Area of Responsibility (i.e., specific tactics, techniques, and procedures; emerging capabilities, etc.) to support the production of software systems identifying adversarial tools, techniques, methods of operation and assess whether it can be turned to advantage • Coordinates security automation and practices with cybersecurity incident management and response organizations efforts by keeping up-to-date on applicable efforts and identifying potential areas of conflict; mitigates any identified gaps or interference issues and delegates the responsibility to the appropriate personnel as needed • Lends advanced knowledge in software assurance to provide input into leadership decisions that address means to reduce exploitable software weaknesses and improve capabilities that routinely develop, acquire and deploy resilient software products • Analyzes static and dynamic analysis report findings for applications, databases, networks, network-based environments, and operating systems, and directs remediation as appropriate; creates protocols, procedures, and guidelines to mitigate cybersecurity risks
4 Expert	• Keeps current on evolving and emerging technologies that may involve multi-disciplined intelligence and/or evoke new risks and interfaces with other organizations to maintain situational awareness, stay ahead of future threats and leverage best practices • Lends expert software engineering and assurance frameworks to oversee and enable software security automation and measurement capabilities through development and provides oversight of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks, which target software

CRITICALITY		
Importance	Required at Entry	Criticality
Important	Preferred, but not required	Important – Preferred, but Not Required at Entry
PROFICIENCY TARGETS		
Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
2 - Intermediate	3 - Advanced	4 - Expert

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 Tasks Identified as Part of Competency: • Conducts comparative analysis of customer needs, recommended CONOPS, and available research and industry trends/technologies • Develops cost estimates for a newly acquired or modified system, and defines scope and objectives based on a customer's system requirements • Keeps abreast of changes in cybersecurity and industry best practices to develop innovative capital asset and infrastructure planning strategies at the national level	
BEHAVIORAL INDICATORS	
1 Basic	• Conducts research to review security and organizational policies across multiple organizations in an effort to identify system requirements and effectively communicate key findings to supervisors and managers • Draws from basic understanding of system requirements when documenting organization requirements during meetings and taking detailed notes, reviewing them for accuracy, and clarifying information as needed • Contributes basic knowledge of lifecycle management and Federal Acquisition Regulations (FAR) when participating in systems requirements planning meetings
2 Intermediate	• Consults with customers to capture data, and demonstrates the ability to ask insightful questions to derive functional requirements from their concerns; aligns functional requirements to standards and regulations to recommend customer-oriented solutions • Demonstrates ability to interpret customer requirements by translating customer needs into functional requirements, mapping those to organizational policies, procedures, and guidelines and developing initial Concept of Operations (CONOPs) • Assists in risk analysis, feasibility studies and/or trade-off analysis to help resolve issues and refine functional requirements and specifications • Gathers requirements when assisting in the preparation of technical, cyber-related contract documents such as Requests for Proposals (RFPs) and Statements of Work (SOWs) • Contributes knowledge of systems lifecycle phases, checkpoints, and deliverables when providing input to procurement SOWs
3 Advanced	• Benchmarks systems requirements (e.g., security, costs, technical, business data, and processes) to organizational policies by conducting a thorough evaluation of options and mapping proposed solutions directly to customer requirements and expressed needs • Conducts comparative analysis of customer needs, recommended CONOPS, and available research and industry trends/technologies; synthesizes this information and tailors it to customer audiences to effectively formulate and articulate final system operations to appropriate audiences; develops cost estimates to identify resources (e.g., personnel, types of equipment, and location) needed to facilitate solution implementation • Applies knowledge of capabilities and requirements analysis when conducting risk analyses, feasibility studies, and/or trade-off analyses to develop, document, and refine functional requirements and specifications for customers • Demonstrates the ability to justify the need for specific IT solutions by translating functional requirements into design solutions within use case reports • Serves as Contracting Officer's Technical Representative (COTR) for IT investments, following prescribed methods when reviewing budget status; provides input to capital assessment infrastructure planning • Combines knowledge of contracting principles and cybersecurity needs to develop and prepare multiple accessory documents (e.g., purchase, acquisition plans, cost estimates, Requests for Quotations (RFQs), Service Contracts, SOWs) • Analyzes and evaluates performance, resources, cost, and schedule in order to achieve business objectives; refines project objectives and makes timely adjustments to project plan, team, and schedule if necessary • Identifies, prioritizes, and monitors risks that may have adverse impact on project and develops risk mitigation strategies • Acquires appropriate resources and clarifies roles and responsibilities of project personnel

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.
4 Expert	• Designs and establishes metrics to manage cost, schedule, and performance throughout the project life cycle • Defines and determines project objectives, risks, tasks, deliverables, and parameters • Selects project personnel, develops personnel roster, and assures that all project personnel understand their roles, responsibilities, and desired project outcomes • Leads requirements planning sessions with customers by directly communicating with the customers, allocating staff resources, and executing the agenda; subsequently manages the overall project plan by effectively balancing scope, costs, and boundaries with customer needs; and continuously reviews project processes, ensuring customer requirements are met and resources are effectively utilized • Gathers supporting team members and delegates responsibilities for customer consultation meetings by reviewing customer requests and adequately aligning team member's skills to address specific customer needs • Evaluates potential technical solutions by reviewing analyses and determining top recommended solutions that best address customer resources and expressed needs; refines CONOPs by determining the implication of the requirements and their impacts to organizational security and interoperability • Develops cost estimates for a newly acquired or modified system, and defines scope and objectives based on a customer's system requirements; guides others in managing overall project plan by balancing scope, costs and boundaries • Keeps abreast of current and developing technologies and applies expert knowledge of agency's IA/information security architecture, policies and procedures to identify and articulate current and future agency systems needs and technical solutions that align with business needs • Lends awareness of DHS missions and financial data to manage capital assessment infrastructure planning for new cybersecurity technology, spanning initial concept, installation, and implementation • Lends consulting expertise to complex, cyber-contracting activities by participating in major contract negotiations, and coaches others on project package preparation and procurement/acquisition methodologies • Identifies and administers new task orders based on active monitoring of contractor progress on major installation projects against the submitted invoice • Keeps abreast of changes in cybersecurity and industry best practices to develop innovative capital asset and infrastructure planning strategies at the national level • Collaborates with national-level programs to develop SOWs and select appropriate firms for national Indefinite Delivery/Indefinite Quantity (IDIQ) contracts • Develops organizational cybersecurity infrastructure proposal describing benefits to each department to justify them to the head of the organization

CRITICALITY		
Importance	Required at Entry	Criticality
Very Important	Definitely Required	Very Important – Definitely Required at Entry
PROFICIENCY TARGETS		
Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
2 - Intermediate	3 - Advanced	4 - Expert

Systems Security 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 Tasks Identified as Part of Competency:

- Documents design specifications, installation instructions, and other software-related information
- Provides input to cybersecurity protection needs (e.g. security controls, architecture and design) and advises others on enterprise wide security requirements
- Analyzes user needs and requirements for software-reliant capabilities

BEHAVIORAL INDICATORS	
1 Basic	• Describes major components of an enterprise architecture to end-users and customers and uses basic data gathering skills to document design specifications, and user needs; reports findings that support design activities for secure software systems within the software development lifecycle • With guidance and supervision, participates in software security review processes within an enterprise architecture by applying basic knowledge of systems testing and evaluation methods and documenting gaps found in the security architecture • Applies basic knowledge of enterprise architecture and risk management processes, including steps and methods for assessing risk when researching applicable current or emerging technologies and reporting findings related to software security, compatibility, and/or usability
2 Intermediate	• Analyzes user needs and requirements, considers software development and security requirements based on the deployment environment, and interprets and uses enterprise architectural guidelines to make design recommendations for secure software systems • Documents design specifications, installation instructions, and other software-related information to integrate and migrate existing and planned platforms in support of an organization's enterprise architecture, and identifies software system issues and considerations for applicability and risk • Lends skill in discerning protection needs (e.g., security controls) and demonstrates ability to recognize architecture and design considerations when performing software reviews, identifying gaps in software security and providing recommendations into risk management plans
3 Advanced	• Applies advanced knowledge of information security aspects, such as coding, operating systems, programming languages, databases, and federal/agency policies when analyzing user needs and requirements; implements software development and security requirements based on the deployment environment, and interprets architectural guidelines to design secure software systems within the software development lifecycle • Analyzes user needs and requirements, and interprets and uses enterprise architectural guidelines to ensure that acquired or developed software applications and system(s) are consistent with the agency's enterprise architecture and requirements • Applies advanced knowledge of software management and how software components are installed, integrated, and optimized when examining software security systems and designs to determine their adequacy in meeting requirements contained in acquisition documents
4 Expert	• Lends expertise on security protection needs (i.e., security controls, architecture, and design) of software and advises others on enterprise-wide security requirements to be included in complex solution-based statements of work and other appropriate large-scale procurement documents • Blends expert knowledge in software architecture principles to provide input to software Certification and Accreditation (C&A) process, activities, and related documentation (e.g., system life-cycle support plans, concepts of operations, operational procedures and sustainment of training materials)

CRITICALITY		
Importance	**Required at Entry**	**Criticality**
Important	Preferred but not required	Important – Preferred, but Not Required at Entry

PROFICIENCY TARGETS		
Project Lead (GS 12/13)	**Senior (GS 14)**	**Director (GS 15)**
3 - Advanced	4 - Expert	4 - Expert

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 Tasks Identified as Part of Competency: • Assesses policy needs by considering the needs of the organization and collaborating with stakeholders and executive leadership • Identifies any problems or issues encountered with established policies or procedures • Provides input into strategic planning and policy development for enterprise-wide applications, systems, and services	
BEHAVIORAL INDICATORS	
1 Basic	• Applies basic understanding of software assurance policies by following established procedures and protocols, as well as, articulating and translating policies, procedures, and protocols to others • Consults organization-specific software and applications systems policy criteria to explain issuances to key stakeholders and assists them in the identification of gaps and deficiencies; supports the organization's adherence to policy by making basic recommendations for gap closure • Identifies any problems or issues encountered with established policies or procedures by keeping a record of occurrences and reporting them and providing recommendations for the creation or revision of policies to supervisors • With direct supervision and guidance, obtains and maintains applicable policies, procedures, and regulations by keeping them current in standard operating procedures (SOPs), reference manuals, and information sources
2 Intermediate	• Applies knowledge of software assurance and information security policies and procedures by preparing and delivering education and awareness briefings to support agency missions to ensure that stakeholders adhere to these systems security policies and procedures • Defines, interprets, and implements policy as related to customer requirements and translates/tailors these policies into a format that is clear to a variety of audiences • Identifies compliance gaps and collaborates with colleagues and leadership to update organizational policies; applies strategic thinking and judgment to determine whether other policies can fill gaps in current policies • Keeps current on new and emerging software assurance and security technologies and applies knowledge of software security principles to review junior level staff's recommendations on software assurance security policies and procedures and recommends the appropriate course of action
3 Advanced	• Applies knowledge of software assurance and security processes and operations to develop policy for compliance and oversight, education, and awareness, performance measures and metrics to move forward in achieving software assurance strategic goals and objectives • Reviews and provides recommendations on issuances by summarizing them so key stakeholders can fully comprehend them, analyze them for gaps, and deficiencies, and provide recommendations • Lends advanced knowledge of software assurance and enterprise architecture to coordinate and collaborate across the organization and serve as a trusted advisor, providing input into strategic planning and policy development for enterprise-wide applications, systems, and services
4 Expert	• Assesses policy needs by considering the needs of the organization and collaborating with stakeholders and executive leadership to develop policies to govern software assurance activities • Evaluates and implements policies by prioritizing them in terms of current organizational, financial and human resource availability • Leverages resources by effectively allocating them based on a thorough understanding of current organizational needs, infrastructure, policies, and future factors that may affect the organization • Lends expertise in software assurance to provide an infrastructure for the SwA community of practice and enable interagency public-private collaboration to increase software assurance awareness through strategic planning and policy development for acquisition processes and capability benchmarking to address security and resilience needs

CRITICALITY		
Importance	**Required at Entry**	**Criticality**

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.	
Important	Preferred, Not Required	Important – Preferred, but Not Required at Entry
PROFICIENCY TARGETS		
Project Lead **(GS 12/13)**	**Senior** **(GS 14)**	**Director** **(GS 15)**
2 - Intermediate	3 -Advanced	4 - Expert

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

Example Tasks Identified as Part of Competency:

- Identifies security and resilience expectations based on target requirements
- Conducts research to understand capabilities that could contribute to secure and resilient software
- Communicates technical information to non-technical audiences and advises staff on information security issues and approaches

BEHAVIORAL INDICATORS

1 Basic	• Supports software testing, assessment and integration processes by conducting research to understand software capabilities; and contributes basic knowledge gained when participating in software assessment strategy meetings • With direct input and guidance, assists in software capability evaluation by documenting test results through meeting minutes and applying basic understanding of software evaluation and validation requirements
2 Intermediate	• Applies knowledge of software functions to understand capabilities of required software and identify security and resilience expectations based on target requirements; communicates technical information to non-technical audiences and advises staff on information security issues and approaches
3 Advanced	• Applies knowledge of software security principles to develop cyber capabilities strategies for custom software based on mission requirements and organizational technology needs • Lends knowledge and experience of software testing and evaluation when facilitating a pre-defined transition and integration process (e.g., guiding research institutions in creating software and working with acquisition and integrators to prepare the environment for the integration of the software)
4 Expert	• Provides technical leadership in all aspects of software assurance and computer systems engineering support, and determines the definition of software integration processes and practices by lending expert knowledge on agency evaluation and validation requirements and software architecture • Blends program management and systems development lifecycle expertise when leading and actively participating in the evaluation and analysis of activities related to all phases of the secure software lifecycle from initial planning, requirements definition, design and development, through integrated system testing and sustainment operations • Lends expert knowledge of strategic and tactical dimensions of software assurance by overseeing software assessment and integration to ensure the software is fulfilling strategic business needs as well as the tactical dimensions of service, information, system quality, and resilience

CRITICALITY

Importance	Required at Entry	Criticality
Important	Preferred, but not required	Important – Preferred, but Not Required at Entry

PROFICIENCY TARGETS

Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
2 - Intermediate	3 - Advanced	4 - Expert

Education and Training	Conducts training of personnel within pertinent subject domain. Develop, plan, coordinate, and evaluate training courses, methods, and techniques as appropriate.
Example Tasks Identified as Part of Competency: • Coordinates with other agencies to develop integration plans for new SwA training courses • Identifies public and private sector performance gaps in education and training by monitoring sector trends • Communicates course requirements to schools and vendors for course creation • Contributes to the development of SwA courseware and materials	
BEHAVIORAL INDICATORS	
1 Basic	• Answers questions and contributes basic software assurance knowledge to coach stakeholders and customers on simple concepts, material or tasks in an informal setting • Contributes basic ability to prepare and support the delivery of software assurance training/briefings by assisting in gathering course development material and content (e.g., research, resources) and coordinating training session(s) logistics • Uses knowledge of communication mediums, target audience characteristics, and security policies and procedures to develop broadcast emails or other messages related to software assurance awareness training • With supervision and guidance, collects course evaluation data and reports findings to management
2 Intermediate	• Applies knowledge of software functions to understand capabilities and resiliency expectations based on target requirements; communicates technical information to non-technical audiences and advises staff on information security issues and approaches • Contributes to continuous improvement of training strategies by supporting or assisting with updates to training material for inclusion in a specific course or course modules that address SwA best practices and or SwA awareness • Demonstrates the ability to develop and deliver education and awareness training and applies knowledge of software security policies and procedures to prepare and deliver/facilitate education and awareness briefings to ensure that software developers are aware of and adhere to software security policies and procedures • Gathers stakeholder interests and needs to determine content for training, and lends knowledge of Instructional Systems Design (ISD) methodologies and modalities to make training recommendations to management • Identifies public and private sector performance gaps in education and training by monitoring sector trends; lends knowledge gained to identify and develop training materials that address required, targeted training for gap closure • Recommends additional and/or supplemental communication or training opportunities for existing and future trainings by evaluating previous, current, and proposed training efforts, and comparing results with procedural, recommended, and organizational needs • Uses knowledge of training and development, software assurance, instructional methods (i.e., instructor led, web-based, written, etc.), training management and standard software packages to design, create, deliver and facilitate training related to software assurance with minimal guidance
3 Advanced	• Applies advanced knowledge in software assurance, information security, ethical hacking, configuration management, integration, and deployment issues to collaborate in the development and publishing of software security content and SwA curriculum courseware focused on integrating security content into relevant education and training programs • Analyzes intended audience and lends software assurance expertise to the development and delivery of training on complex topics; articulates course concepts and information to the audience; develops outline, content, material, and instruction method requirements • Communicates course requirements to schools and vendors for course creation and reviews course materials to ensure they coincide with education and training requirements and needs • Organizes team/program participation in national/ sector-wide efforts, including working groups, tabletop exercises, training initiatives, and other events throughout the sector

Education and Training	Conducts training of personnel within pertinent subject domain. Develop, plan, coordinate, and evaluate training courses, methods, and techniques as appropriate.
4 Expert	• Assesses technical and legal trends that will impact software assurance activities and designs and implements agency-wide software security awareness training program, including content development, event and travel schedule, materials requirements and associated metrics; thereby supporting organizational risk management and mitigation strategies • Coordinates with other agencies to develop integration plans for new SwA training content and courses to be included into existing curricula • Oversees the overall software assurance education and training program by ensuring the program is delivered in a timely and professional manner and is upholding the standards of the National Infrastructure Protection Plan, Homeland Security Presidential Directive 7, and other Federal mandates

CRITICALITY

Importance	Required at Entry	Criticality
Very Important	Definitely Required	Very Important – Definitely Required at Entry

PROFICIENCY TARGETS

Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
3 - Advanced	3 - Advanced	4 - Expert

Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
Example Tasks Identified as Part of Competency: • Provides an infrastructure for the Software Assurance (SwA) Community of Practice (CoP) • Administers the indexing/cataloguing, storage, and access of relevant material • Monitors the usage and maintains SwA knowledge management assets and systems • Supports the improvement of SwA CoP knowledge management lifecycle	
BEHAVIORAL INDICATORS	
1 Basic	• Demonstrates basic understanding of knowledge management by defining its four levels of data, information, knowledge, and wisdom to support knowledge repository end users in basic knowledge management needs • Demonstrates knowledge of various technological tools used to create various content (e.g., wikis, social networking, blog, websites, etc.) by articulating the strengths, weaknesses and best practices for utilization to stakeholders • Draws from basic understating of knowledge management technologies to describe the role of technology in converting data and information into organizational knowledge • With guidance, identifies technological tools used in knowledge management when explaining basic knowledge management solutions to end users
2 Intermediate	• When delivering solutions to end users, demonstrates the ability to apply software security principles, policies, and procedures by implementing appropriate knowledge management repositories and technologies for a given environment; thereby supporting an organization's software assurance and knowledge management strategic goals • Applies skills in data mining and knowledge mapping to administer the indexing/cataloguing, storage, and access of organizational documents • Supports a culture of knowledge sharing, collaboration, and support by using tools (e.g., wikis, social networking, blog, websites, etc.) to implement knowledge management systems • Demonstrates familiarly with passive knowledge capture techniques by identifying opportunities where existing information can be transferred into knowledge and made discoverable through automated means; and applies knowledge of the four levels of knowledge management to support the strategic goals set forth by the organization • Monitors the usage and maintains knowledge management assets and systems by running routine tests, reviewing reports, and solving issues that occur
3 Advanced	• Facilitates the integration of COPs to enhance learning at the intersection of bodies of knowledge from each COPs by collaborating with COP Subject Matter Experts (SMEs) • Analyzes the lifecycle of knowledge management initiatives by aligning agency information flows to its structure and processes and synthesizes this information so that decision makers and users acquire the desired information at the right time • Supports the improvement of knowledge management lifecycle through thorough analysis and evidence-based recommendations to senior leadership
4 Expert	• Evaluates a variety of organizational approaches (security policies, budget, assessment, rewards) that can be used to successfully institutionalize knowledge management processes and selects the best method for creating and implementing a knowledge management solution • Lends expertise in software assurance to provide an infrastructure for the SwA community of practice and enable interagency public-private collaboration to increase software assurance awareness through strategic planning and policy development for acquisition processes and capability benchmarking to address security needs • Lends expertise in software assurance to provide an infrastructure for the SwA COP and enable interagency public-private collaboration to increase software assurance awareness; and enhance development and acquisition processes and capability benchmarking to address security needs

CRITICALITY		
Importance	Required at Entry	Criticality
Very Important	Definitely Required	Very Important – Definitely Required at Entry

Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	
PROFICIENCY TARGETS		
Project Lead (GS 12/13)	Senior (GS 14)	Director (GS 15)
2 - Intermediate	3 - Advanced	4 - Expert