

PRESENTATION

Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training

Bethesda, MD
November 13, 2008

*This document is confidential and is intended solely for the use and
information of the client to whom it is addressed.*



Agenda

- ▶ Background & IS Security Landscape
- ▶ IS Security Qualifications Matrix Initiative
- ▶ IS Security Workforce Policy, Guidance, & Publications
- ▶ Workshop Activities & Objectives
- ▶ Group Discussion
- ▶ Next Steps & Closeout



The Federal Chief Information Officers Council is leading the Information Systems Security Qualifications Matrix initiative

- ▶ The Federal CIO Council is comprised of 5 distinct Committees, 2 of which are directly involved in the development of the Information Systems Security Qualifications Matrix
 - **IT Workforce Committee:** primarily responsible for the actual development of the qualifications matrix
 - **Security and Identity Management Committee:** providing oversight to the qualifications matrix initiative
- ▶ The strategic goal of the IT Workforce Committee is to build ***“a cadre of highly capable IT professionals with the mission critical competencies needed to meet agency goals”***
- ▶ The IT Workforce Committee has objectives for recruitment, retention, and the professional development of the IT workforce



The IS Security Qualifications Matrix is intended to further advance the professionalization of the Governmentwide Information Systems Security workforce

- ▶ The IS Security Qualifications Matrix is closely related to and patterned after the IT Project Management Guidance Matrix developed by the Federal CIO Council to provide standardized, yet flexible qualifications guidance regarding IT project managers
- ▶ Benefits of the IS Security Qualifications Matrix include:
 - It draws from and further builds upon other initiatives that have been done, as well as other policy and guidance that has been developed in the IS Security arena
 - It will provide a standard framework and define a common environment for each of the security roles it addresses
 - It will provide concise guidance, and will be modeled specifically for Agency use and customization
 - It is designed to allow for maximum Agency flexibility in its application



There are several potential key components to the qualifications matrix, as evident in the IT Project Manager Guidance Matrix

Level: Categorizes the project manager role by proficiency levels required for the position

Description/Complexity: Further defines each proficiency level by providing descriptions of the scope of responsibility and experience required for the role at that level

Competencies: Identifies a set of measurable knowledge, skills, abilities, and behaviors that an individual needs to successfully perform work roles or occupational functions.

Federal IT Project Manager Guidance Matrix				
Level	Description/Complexity	Competencies	Suggested Experience	Suggested Education, Training and Development Sources
1	<p>Projects with low-to-moderate complexity and risk.</p> <p>Example:</p> <ul style="list-style-type: none"> •Bureau-level project such as a stand-alone information system that has low-to-moderate complexity and risk. 	<p>As a minimum:</p> <ul style="list-style-type: none"> •An understanding of PM and IT-PM competencies listed in the <i>OPM 2210 Series IT Project Manager Guidance</i> (pages 6,7). •Fundamental PM knowledge, skills and abilities that include an understanding of principles, practices and terminology. •Fundamental IT PM skills in applicable IT-PM competencies. •Skills required for respective bureau or business area. 	<p>As a minimum:</p> <ul style="list-style-type: none"> •1 year previous, successful technical or PM experience 	<ol style="list-style-type: none"> IT employees and supervisors can utilize the IT Workforce Development Roadmap at http://itroadmap.golearn.gov to identify specific competency training requirements and resources. A list of PM training sources can be found in the <i>Project Management Training Directory</i> sponsored by the Federal CIO Council at http://www.cio.gov. <p>Federal PM training sources include:</p> <ul style="list-style-type: none"> •USDA Grant School PM/IT PM courses •OPM-sponsored PM training seminars •GSA STAR Program •DoD's Information Resources Mgmt College (IRMC) •DoD's Defense Acquisition University
2	<p>Projects with high complexity and/or risk which are critical to the mission of the organization.</p> <p>Examples:</p> <ul style="list-style-type: none"> •Projects that are part of a portfolio of projects/systems that impact each other and/or impact mission activities. •Department-wide projects that impact cross-organizational missions, such as an agency-wide system integration that includes large scale Enterprise Resource Planning. 	<p>Built on Level 1:</p> <ul style="list-style-type: none"> •High proficiency in both PM and applicable IT PM competency skills listed in the <i>OPM 2210 Series IT Project Manager Guidance</i> (pages 6,7). --Advanced PM knowledge skills and abilities. --Advanced IT PM skills. •Developed systems perspective delineated in Clinger-Cohen Core Competencies, including life cycle mgmt, capital planning and investment, mission alignment, strategic planning, political ramifications, enterprise architecture, statutory and regulatory reqmts, systems of systems integration, etc. •Agency-specific skills and knowledge, e.g. DoD's Global Information Grid or NASA's Space and Ground Network. 	<p>As a minimum:</p> <ul style="list-style-type: none"> •2-4 years combined previous, successful PM and technical experience, depending on project complexity 	<ol style="list-style-type: none"> Training programs aligned to the ANSI-recognized <i>PMBOK 2000</i> knowledge areas and management processes provide a PM foundation. Additional IT-PM competency requirements, e.g., architecture, capital planning and investment, etc., are outlined in the <i>OPM Interpretive Guidance for Project Management Positions</i>. Training for these IT areas can be found in the IT Workforce Development Roadmap. Clinger-Cohen Core Competency-based training sources include: <ul style="list-style-type: none"> •GSA's CIO University Program •DoD's IRMC certificate programs
3	<p>Projects that have high complexity, and/or risk, and have government-wide impact.</p> <p>Examples:</p> <ul style="list-style-type: none"> •Government-wide initiative <ul style="list-style-type: none"> --E-GOV --President's Management Agenda •High interest projects with Congress, GAO, OMB, or the general public. •Cross-cutting initiative <ul style="list-style-type: none"> --Homeland Security 	<ul style="list-style-type: none"> •Agency-specific skills and knowledge, e.g. DoD's Global Information Grid or NASA's Space and Ground Network. 	<p>As a minimum:</p> <ul style="list-style-type: none"> •2-4 years combined previous, successful PM and technical experience, with prior experience in managing a Level 2 IT Project. 	<ol style="list-style-type: none"> Agencies are expected to identify specific organization and business area training required. This guidance reflects the minimal standard. Due to mission needs or legislative requirements, agencies may need additional credentials for PM validation. Agency credentialing may include other criteria, e.g. continuing education or professional society certifications. Agencies are responsible for validating applicable training for IT Project Managers or issuance of an Agency waiver.

Suggested Education, Training and Development Sources: Provides a list of available resources to facilitate further understanding, enhance or develop a job-related knowledge, skill, or ability, to provide professional and career development opportunities for an individual currently in the role, as well as a person interested in applying for this position

Suggested Experience: Identifies minimum years of experience required for this role at the appropriate proficiency level



Several key policy and guidance publications have been created that address various factors relating to IS Security qualifications and training standards

Publication	Year	IS Security Workforce Impact	Intended Use
OPM GS-2210 Job Family and Qualification Standard	2001	<ul style="list-style-type: none"> ▶ Provides series definitions, titling instructions, detailed occupational information and grading standards for Information Technology Management Series – GS 2210 ▶ Provides qualification standards based on grade levels 	Policy
5 CFR 930.301	1991	<ul style="list-style-type: none"> ▶ Requires each Executive agency to develop a plan for Information Systems Security awareness and training at the awareness level, policy level, implementation level and performance level for executives, program and functional managers, information resources managers, security and audit personnel, automated data processing management, operations, programming staff, and end users 	Policy
NIST SP 800-16	1998	<ul style="list-style-type: none"> ▶ Presents a conceptual framework for providing IT Security Training ▶ Focuses on job functions or roles, not job titles ▶ Distinguishes between IT Security Awareness, Training, and Education ▶ Includes IT Security function-specific training standards by identifying: Training Area, Functional Specialty, and Proficiency Levels (Basic, Intermediate, Advanced) 	Policy
DHS IT Security Essential Body of Knowledge (EBK)	2008	<ul style="list-style-type: none"> ▶ Provides a high-level framework that establishes a national baseline representing the essential knowledge and skills IT security practitioners should possess ▶ Identifies non-industry-specific key IT Security Roles (focuses on IT Security functions versus specific jobs) ▶ Classifies IT Security roles as Executive, Functional, or Corollary ▶ Takes a functional perspective on competencies associated with IT Security roles (Manage, Design, Implement, Evaluate) 	Guidance
DoD Directive 8570.01-M	2004	<ul style="list-style-type: none"> ▶ Provides mandatory requirements for training and certification of DoD Information Assurance (IA) workforce management and technical career personnel ▶ Identifies three proficiency levels based on years of experience: Management and Technical (L1, L2, L3); Identifies specific certifications required. 	Policy (DoD)
CNSS Directive No. 500	2006	<ul style="list-style-type: none"> ▶ Establishes the requirement for federal departments and agencies to establish and implement information assurance (IA) education, training and awareness (ETA) programs for personnel who access, operate, manage, maintain, secure, develop, and acquire National Security Systems (NSS) ▶ CNSS Mar 2008 Report -reiterates existing policy and guidance such as: DoD 8570.01-M; DHS EBK (represents national baseline for ISS standards) 	Guidance
Clinger-Cohen Core Competencies	2006	<ul style="list-style-type: none"> ▶ Provides baseline to assist Federal Chief Information Officers to ensure that the knowledge, skills and abilities represented in each competency are resident within their organization ▶ Contains Information Security/Information Assurance section 	Guidance



Work group activities involve discussing potential qualifications categories and descriptions for an IS Security role...

- ▶ Groups will be discussing and documenting potential qualification guidelines for a specific IS Security-related role in relation to several categories
 - **Proficiency Levels:** quantitative and qualitative descriptors that distinguish between the various levels of performance within the IS Security role
 - **Competencies:** the measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to successfully perform work roles or occupational functions
 - **Education:** the educational specialization areas and levels that relate to the IS Security role
 - **Training & Career Development:** the opportunities (formal and informal) that are available for individuals in the IS Security role to increase their capabilities and manage their career progression
 - **Certifications:** credentials given by accreditation organizations targeting key IS Security positions and/or areas of expertise
- ▶ The similarities and differences that may occur within and between the departments, agencies, and organizations represented in each work group should be documented and discussed



...and evaluating and prioritizing IS Security roles on specific criteria

- ▶ Groups will be rating a set of IS Security roles on three factors:
 - **Importance:** what is the importance of this role with respect to the IS Security function in your organization
 - **Need for Qualifications Guidance:** the roles that would benefit the most from the development of an IS Security Qualifications Matrix
 - **Size of IS Security Workforce:** number of employees associated with the IS Security role within your organization
- ▶ Data will also be utilized to determine the adequacy of existing IS Security roles in describing the functions performed by the IS Security workforce
- ▶ Evaluative feedback and priority ratings will be analyzed in order to manage the roll out for subsequent IS Security Qualifications Matrices



Work group activities are intended to foster dialogue and provide new insights into IS Security roles across a variety of organizations

- ▶ The objectives of the work group activities are to:
 - Develop a deeper understanding of the qualitative criteria relevant to IS Security professionals within your organization
 - Increase awareness of the IS Security function as it exists in other departments, agencies, and/or organizations
 - Gain exposure to examples of evaluative criteria employed by other organizations
 - Address different perspectives on defining critical IS Security roles
 - Provide insights and input into a standard qualifications framework for an IS Security role
 - Network with other training, education, and development professionals within the IS Security community



There are several questions to keep in mind during the work group activities

- ▶ Are there other policy documents or guidance publications that should be considered in the development of qualifications guidelines for IS Security professionals?
- ▶ If so, what are they and how do they relate to the qualifications or capability requirements of IS Security professionals?
- ▶ What are the similarities in IS Security professional qualifications between the organizations represented in your work groups?
- ▶ What are some of the noticeable differences in IS Security professional qualifications between the organizations represented in your work groups?



Work Group Activities & Group Discussion Timeline

- ▶ **10:00 – 10:45 Activity One: Painting a Well-Rounded Picture**
- ▶ **10:45 – 11:00 Activity Two: Prioritizing Critical Roles**
- ▶ **11:00 – 11:50 Group Discussion**
- ▶ **11:50 – 12:00 Next Steps & Closeout**



Next Steps & Contact Information

- ▶ Content developed by work groups will be used to create a draft qualifications matrix for the IT Security Professional role
- ▶ The draft matrix will undergo further development and validation during subject matter expert focus groups
- ▶ The pilot IT Security Professional qualifications matrix guideline will be finalized, and additional IS Security roles that could benefit from qualifications matrix development will be identified
- ▶ If you have any additional questions regarding the materials presented or activities of the day, please contact one of the following individuals

Name	Email Address	Phone Number
Dagne Fulcher	dagnefulcher@verizon.net	703.999.7329
David Ascione	ascione_david@bah.com	703.200.1783
Ruth Kao	kao_ruth@bah.com	703.984.3848

THANK YOU FOR YOUR PARTICIPATION!

