

# CYBERSECURITY WORKFORCE DEVELOPMENT MATRIX RESOURCE GUIDE

October 2011



**CIO.GOV**

CHIEF INFORMATION OFFICERS COUNCIL

## Table of Contents

<b>Introduction &amp; Purpose.....</b>	<b>2</b>
<b>The Workforce Development Matrix Effort .....</b>	<b>3</b>
<b>Introduction to the Project .....</b>	<b>3</b>
<b>Piloting a Workforce Development Matrix.....</b>	<b>4</b>
<b>Human Capital Planning &amp; Workforce Management .....</b>	<b>8</b>
<b>Workforce Planning .....</b>	<b>9</b>
<b>Introduction to Workforce Planning .....</b>	<b>10</b>
<b>Foundational Steps for Creating Workforce Plans .....</b>	<b>11</b>
<b>Recruitment &amp; Selection .....</b>	<b>15</b>
<b>Begin with a Job Analysis.....</b>	<b>15</b>
<b>Strategic Recruitment.....</b>	<b>16</b>
<b>Developing Vacancy Announcements .....</b>	<b>19</b>
<b>Crediting Plans .....</b>	<b>23</b>
<b>Structured Interviews.....</b>	<b>26</b>
<b>Employee Development .....</b>	<b>30</b>
<b>Introduction to Employee Development.....</b>	<b>30</b>
<b>Using the Matrices to Inform Employee Development.....</b>	<b>31</b>
<b>Succession Planning .....</b>	<b>33</b>
<b>Succession Planning in the Federal Government.....</b>	<b>34</b>
<b>Building Pools of Succession Candidates .....</b>	<b>35</b>
<b>Using the Matrices to Engage in Succession Planning.....</b>	<b>36</b>
<b>Conclusion .....</b>	<b>38</b>
<b>Appendix .....</b>	<b>39</b>
<b>Workforce Development Matrices.....</b>	<b>39</b>

CHIEF INFORMATION OFFICERS COUNCIL

## Introduction & Purpose

The field of Cybersecurity continues to undergo rapid expansion and change. Even the name of the field has evolved from a group of terms such as “Information Security,” “Information Assurance,” and “Information Technology Security.” Throughout government, “Cybersecurity” has been adopted as the global term to refer to all these related fields, and will be the term used in this Resource Guide.

Federal agencies are increasingly reliant on computer systems and networks to meet their mission requirements. While this has dramatically increased the speed and efficiency with which federal employees can do their jobs, it also creates vulnerabilities for the United States Government and its citizens. Therefore, Cybersecurity is becoming increasingly important as all agencies work to ensure that their systems are secure and their information remains intact and accessible to the right users.

Due to the critical nature of these fields, many agencies have been developing their Cybersecurity workforces for years. In many ways, however, this growth has outpaced the government’s ability to standardize and regulate expectations and norms for professionals in these fields. Therefore, agencies have engaged in many different efforts to develop their workforces, and translation across agencies and even job titles is difficult. Given these challenges, the IT Workforce Committee of the Federal Chief Information Officers (CIO) Council launched the Cybersecurity Workforce Development initiative. This resource guide is intended to support the initiative by providing agency personnel with a desktop reference for developing human capital and workforce development activities, with a particular focus on their Cybersecurity workforces. Some of these activities include workforce planning, recruitment and selection, employee development, and succession planning. The guide is broadly written to assist line managers, business unit leaders, and hiring managers. The guide is also intended to help these agency stakeholders partner with human capital professionals as they engage in workforce development activities throughout the employment lifecycle. As agency stakeholders strive to attract, hire, train, develop, and deploy people in these professions, this guide will assist them in using best practices to meet these objectives. Therefore, this guide endeavors to provide an initial foundation to help agencies create highly trained workforces with deep leadership benches and advanced technical expertise.

It is important to recognize the critical role of collaborating with the human capital office when developing the workforce. This collective effort is critical to the success of a variety of workforce development activities because policy changes can be so frequent and/or subtle that it is difficult for managers to keep track of the latest procedures and regulations by themselves. Because this guide is intended as a general reference applicable across government agencies, it will not have the specificity to cover each agency’s particular guidelines. Therefore, agency officials wishing to engage in these workforce development initiatives should seek out updates on federal policies, standards, guidelines, and procedures.

The rest of this guide will describe the Workforce Development Matrix initiative, and will demonstrate how agency stakeholders can use the matrices to engage in human capital processes.

CHIEF INFORMATION OFFICERS COUNCIL

## The Workforce Development Matrix Effort

### Introduction to the Project

Cybersecurity Workforce Development Matrices are intended to provide standardized, yet flexible development guidance for Cybersecurity professionals in the Federal Government. Modeled after the IT Project Management Guidance Matrix developed by the Federal CIO Council in 2004, Cybersecurity Workforce Development Matrices:

- Draw from and build upon other initiatives that have been undertaken
- Build upon a foundation of recent policy and guidance that has been developed in the Cybersecurity arena
- Provide a standard framework and define a common operating environment for each of the Cybersecurity roles addressed
- Provide concise guidance modeled specifically for agency use and customization
- Allow for maximum agency flexibility in agency-level application

In 2008, the Matrix Project Team partnered with Cybersecurity Subject Matter Experts (SMEs) to identify, define, and prioritize a list of 11 critical Cybersecurity roles. Workforce Development Matrices were created for four of these roles: Information Security Assessor, Chief Information Security Officer, Systems Operations & Maintenance Professional, and Information Systems Security & Software Development Professional.

It is important to note that this effort has evolved with the field since 2008. Originally called “Information Security Workforce Development Matrices,” the titles of the project and its products changed to use the government-wide “Cybersecurity” term. Further, in 2011, the National Institute of Standards and Technology (NIST) charged the National Initiative for Cybersecurity Education (NICE) to develop a taxonomy of Cybersecurity roles. NICE has a national focus (private and public sectors, including Federal, State, Local, and Tribal government). Rather than duplicate effort, the Matrix Project Team partnered with NICE to share information and integrate its list of roles with the emerging framework. While not yet final, the NICE framework includes 31 specialty areas in the Cybersecurity workforce. Since NIST has been charged with providing a framework for Cybersecurity specialty areas for the nation, the Matrix Project Team will use this emerging framework to select roles for future matrix development, and continues to work with NICE to provide a federal perspective as the role framework develops. Therefore, while the initial matrices produced by this effort are not directly aligned with the framework that NICE subsequently developed, all future matrices will use the NICE framework specialty areas.

The Cybersecurity Workforce Development Matrix initiative does not introduce additional standards for the Cybersecurity workforce. Instead, the matrices should help agencies identify critical requirements, develop uniform Cybersecurity role/function evaluative criteria, create and share career development activities and opportunities, and cultivate human capital strategies and initiatives to increase the capabilities of their Cybersecurity workforce. The matrices are designed to foster a degree of consistency and standardization of the expectations for Cybersecurity -related roles/functions, and to promote the professionalization of the Cybersecurity workforce.

CHIEF INFORMATION OFFICERS COUNCIL

Key Cybersecurity qualification policy (from OPM) and guidance publications are used to provide the foundation upon which the workforce development matrices are built. The matrices endeavor to promote consistency by drawing upon the salient components of guidance publications. Samples of these key publications are listed below in Table 1.

**Table 1. Sample Cybersecurity Publication Classification**

Publication	Year	Cybersecurity Workforce Impact	Intended Use
5 CFR 930.301	1991	<ul style="list-style-type: none"> <li>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 <a href="http://www.gpoaccess.gov/ecfr">www.gpoaccess.gov/ecfr</a></li> </ul>	Policy
NIST SP 800-16	1998	<ul style="list-style-type: none"> <li>Presents a conceptual framework for providing Cybersecurity training</li> <li>Focuses on job functions or roles, not job titles</li> <li>Distinguishes between Cybersecurity Awareness, Training, and Education</li> <li>Includes Cybersecurity function-specific training standards by identifying: Training Area, Functional Specialty, and Proficiency Levels (Basic, Intermediate, Advanced) <a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a></li> </ul>	Policy
OPM GS-2210 Job Family and Qualification Standard	2001	<ul style="list-style-type: none"> <li>Provides series definitions, titling instructions, detailed occupational information and grading standards for the Information Technology Management Series – GS 2210</li> <li>Provides qualification standards based on grade levels <a href="http://www.opm.gov/qualifications/Standards/IORs/gs2200/2210-AltA.asp">http://www.opm.gov/qualifications/Standards/IORs/gs2200/2210-AltA.asp</a></li> </ul>	Policy
DoD Directive 8570.1-M	2004	<ul style="list-style-type: none"> <li>Identifies two overall Information Assurance (IA) workforce career paths, and three proficiency levels based on years of experience: Management and Technical (L1, L2, L3)</li> <li>Identifies specific certifications required based on the individual's function and level</li> <li>Fourteen different certifications in total <a href="http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf">http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf</a></li> </ul>	Policy (DoD)
2007/2008 CNSS Report	2008	<ul style="list-style-type: none"> <li>Provides IA training and education standards for role-based training from National Centers of Academic Excellence in IA Education (CAEIAE)</li> <li>Reiterates existing policy and guidance such as: DoD 8570.01-M, DHS EBK (represents a national baseline for IT Security standards) <a href="http://www.cnss.gov/Assets/pdf/CNSS_Report_07-08.pdf">http://www.cnss.gov/Assets/pdf/CNSS_Report_07-08.pdf</a></li> </ul>	Guidance
DHS IT Security Essential Body of Knowledge (EBK)	2008	<ul style="list-style-type: none"> <li>Provides a high-level framework that establishes a national baseline representing the essential knowledge and skills Presents a conceptual framework for providing Cybersecurity training practitioners should possess</li> <li>Identifies key non-industry-specific Presents a conceptual framework for providing Cybersecurity training roles (focuses on functions versus specific jobs)</li> <li>Classifies Presents a conceptual framework for providing Cybersecurity training roles as Executive, Functional, or Corollary</li> <li>Takes a functional perspective on competencies associated with Presents a conceptual framework for providing Cybersecurity training roles (Manage, Design, Implement, Evaluate) <a href="http://www.us-cert.gov/ITSecurityEBK">www.us-cert.gov/ITSecurityEBK</a></li> </ul>	Guidance

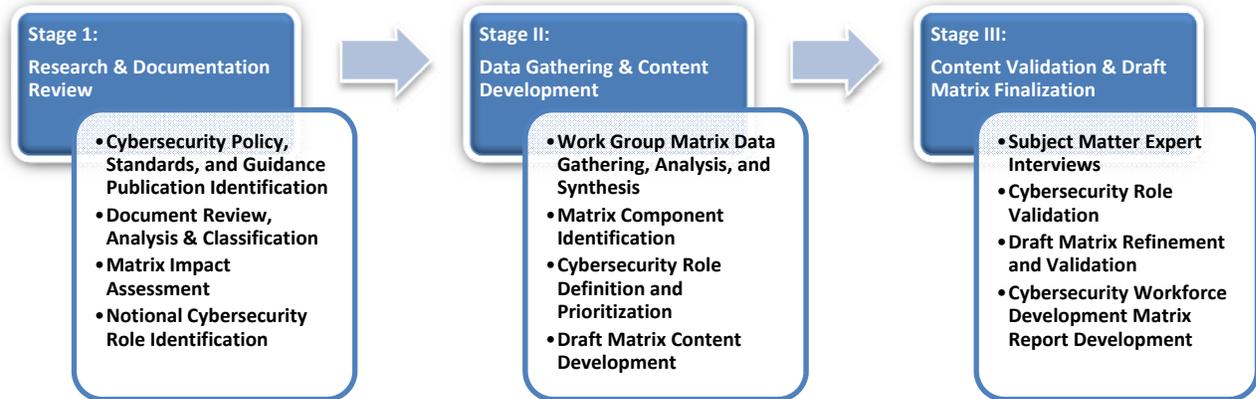
**Piloting a Workforce Development Matrix**

In November and December of 2008, the project team was asked to develop a pilot matrix to determine the utility of creating this type of resource. The team used a three-stage methodology to collect data and create the first workforce development matrix. The stages included: Stage 1: Research & Documentation Review, Stage 2: Data Gathering & Content Development, and Stage 3: Content Validation & Draft Matrix Finalization. The activities associated with each stage of the development approach are listed in *Figure 1* and discussed below. Please refer to the *Information Security Workforce*

CHIEF INFORMATION OFFICERS COUNCIL

*Development Matrix Research & Development Report* (on the OMB MAX Portal for the Federal CIO Council) for additional information on the pilot matrix.

**Figure 1. Cybersecurity Workforce Development Matrix Development Approach**



### Stage 1: Research & Documentation Review

Key Federal Government and private sector publications (e.g., regulations, standards, policies, etc.) were collected and analyzed to determine:

- Which areas of Cybersecurity they addressed
- How they related to standards (e.g., OPM qualifications) for Cybersecurity professionals
- How they might impact the development of the draft Cybersecurity Workforce Development Matrix

These publications were catalogued and organized in preparation for obtaining feedback from subject matter experts (SMEs) during subsequent development activities.

### Stage 2: Data Gathering & Content Development

Once the body of research and documentation had been collected and analyzed, the project team used this information to conduct focus group at the Federal Information Systems Security Educators' Association (FISSEA) workshop. During this workshop, the team created work group activities and facilitated a group discussion to develop matrix content. SMEs included Federal CIO Council customers, stakeholders, and Cybersecurity professionals. The project team then analyzed, synthesized, and integrated this additional qualitative data with the Stage 1 data to create a draft matrix. This draft matrix then served as the foundation for SME interviews conducted in Stage 3.

### Stage 3: Content Validation & Draft Matrix Finalization

Once the pilot matrix was drafted, the project team scheduled follow-up interviews with SMEs. These respondents included FISSEA workshop participants and SMEs identified through the Federal CIO Council's IT Workforce and Information Security & Identity Management Sub-committees. A total of 11 SMEs were interviewed in five separate content development sessions. SME interviews addressed each

## CHIEF INFORMATION OFFICERS COUNCIL

component of the matrix. SMEs provided feedback regarding the content of the matrix, and offered suggestions for improvement and refinement.

**Workforce Development Matrix Components**

The initial pilot role targeted for development was intended to be a general, widely applicable role across the Cybersecurity workforce. The original role identified for development was the Information Security Professional, as defined by the DHS Essential Body of Knowledge (EBK). After speaking with several SMEs, interview data revealed that a general workforce development matrix had limited utility in practice, and a more specific and defined role was preferable. Therefore, the team switched focus to a new role: the Information Security Compliance Professional (now named as Information Security Assessor). Using this as the pilot role, the project team worked with SMEs to define content for each of the six components of the matrix.

The Cybersecurity Workforce Development Matrices are comprised of several important components (*Figure 2*).

1. **Role Title & Definition:** title of selected role and description of associated functions and responsibilities
2. **Performance Levels:** qualitative distinctions in proficiencies and capabilities that exist for the Cybersecurity role presented
3. **Description/Complexity:** further definition of performance levels including descriptions of scope of responsibility, types of work performed, and duties and responsibilities for the role at the performance level
4. **Competencies/Skills:** relevant sets of measurable knowledge, skills, abilities, and behaviors needed to successfully perform work roles or occupational functions
5. **Suggested Credentials:** combination of years of experience, education, or associated certifications recommended for this role at the appropriate performance level
6. **Suggested Learning & Development Sources:** available resources to facilitate further understanding, enhance or develop a job-related knowledge, skill, or ability, to provide professional and career development opportunities for individuals in the role, or those interested in transitioning into this role

CHIEF INFORMATION OFFICERS COUNCIL

Figure 2. Cybersecurity Workforce Development Matrix Components

INFORMATION SECURITY ASSESSOR WORKFORCE DEVELOPMENT MATRIX (v1)\*

1	2	3	4	5	6
INFORMATION SECURITY ASSESSOR: The Information Security Assessor is responsible for overseeing, participating in evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Information Security Assessor provides guidance and autonomous evaluation of the organization to management.	Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
I: Entry	Has a basic understanding of information security compliance with regard to the FISMA Act and its requirements, applicable laws and regulations (e.g., OMB directives, HSPD, HIPAA, Clinger-Cohen), organizational policies, and the information security compliance evaluation process (i.e., initial risk assessment, mitigation recommendations, controls, and applicable security compliance)  Applies compliance knowledge, skills, and abilities with supervision on projects, programs, and initiatives with low threat and scope (i.e., inter-office)	Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below.  <b>Competency/Skill Proficiency Descriptors</b> I-Entry: Basic understanding of concepts addressed in relevant competency/skill models  II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities  III-Advanced: Advanced application and mastery of relevant competency/skill models	0-3 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs  Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE)	<ol style="list-style-type: none"> <li>Development Resources:                             <ul style="list-style-type: none"> <li>IT Workforce Roadmap (IT Roadmap)</li> <li>Graduate Programs, USDA IT Programs</li> <li>GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>UoU UISA Training</li> <li>GSA's CIO University Program</li> </ul> </li> <li>University Information Security Programs                             <ul style="list-style-type: none"> <li>National Defense University-Info College</li> <li>IS/IA Degree Programs-CAEIAE</li> <li>Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>OPM Development Center, The Federal Executive Institute and the Management Development Centers</li> <li>NIST SP 800-16 Key role-based information security body of knowledge topics and concepts including awareness, training, and education</li> <li>DHS IT Security Essential Body of Knowledge: Information security key terms/concepts, functional perspectives, and role-based competencies</li> <li>Participation in coaching/mentoring/job shadowing programs</li> <li>Agency Requirements: organization and business area training identified as required</li> <li>Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIQ) mandate</li> <li>Certifications: agency credentialing may include other criteria (e.g., DoD 8570-01-4), continuing education, or professional society: industry, or vendor certifications                             <ul style="list-style-type: none"> <li>Core: ISC<sup>2</sup> CAP (I); CISA, CISSP (II/III)</li> <li>Related: ISACA CISM, ISC<sup>2</sup> ISSMP, CompTIA SANS GAC</li> </ul> </li> <li>Current and Emerging Legislation (e.g., FISMA, NIST SP-800 series, National Cybersecurity Initiative, FIPS, OMB directives, CNSI No. 4012)</li> </ol>	
II: Intermediate	Applies an understanding of information security compliance when reviewing systems and security documentation, explaining risks to system owners, implementing risk mitigation controls, and enforcing information security policies  Reviews security document artifacts and determines organizational compliance with information security laws/organizational policies  Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (i.e., sub-organization wide)	<b>Relevant Competency/Skill Sources:</b> <ul style="list-style-type: none"> <li>OPM GS-2200 Job Family Standard Competencies</li> <li>Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas</li> <li>DHS EBK Competencies</li> <li>NIST SP 800-37 C&amp;A Process</li> <li>NIST SP 800-53 Control Set and SP 800-53A Control Assessment</li> <li>FISMA Guidance</li> <li>OPM's IT Workforce Roadmap</li> <li>NIST SP 800-16, Revision 1</li> <li>ODNI Cyber Subdirectory Competencies</li> <li>DoQ Directive 8570</li> <li>CNSS Policies, Directives, and Reports</li> <li>OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> </ul>	<ul style="list-style-type: none"> <li>Bachelors Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>Possession and demonstrated application of CISA or CISSP certifications</li> </ul>		
III: Advanced	Designs the organization's working compliance program and creates associated information security policies and programs  Set expectations, determines appropriate compliance measures to be used across the department/agency, and maintains governance over the standards and methodologies for compliance reviews  Independently manages, plans, evaluates, and advocates for information security compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (i.e., agency-wide or inter-governmental)	<ul style="list-style-type: none"> <li>Graduate Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>Demonstrated experience in managing/supervising an Information Security/IA compliance group</li> <li>Possession and demonstrated application CISA and CISSP certifications</li> </ul>			

It is important to note that the criteria included in the matrix are intended only as guidance, and not auditable requirements. The identified criteria are not a replacement for the United States Office of Personal Management (OPM) basic qualifications, as outlined in the relevant occupational and job family qualification standards. The intention of the workforce development matrix is to assist agencies in defining the capability requirements and criteria that are most relevant and applicable to their Cybersecurity workforce. No singular component on its own (e.g., education, years of experience) should be the sole determinant in classifying an individual's performance level. Rather, all aspects of experience, competencies, education, training, and certifications should be considered when making performance level evaluations.

Feedback on the pilot matrix was positive, and three additional matrices were built using the same process for the roles of Chief Information Officer, Systems Operations and Maintenance Professional, and the Information Security Systems and Software Development Professional roles. After these four were complete, NICE began developing its taxonomy of Cybersecurity specialty areas, and two additional matrices were created to correspond with a draft of the framework that was under construction at the time. Those two matrices were for the Information Security Auditor and Information Systems Security Professional roles.

## CHIEF INFORMATION OFFICERS COUNCIL

Having determined that these matrices are valuable, the next step was to develop some guidance on how to use them for conducting workforce development initiatives. This guide is intended to provide that guidance.

The next section will introduce some of the human capital and workforce development activities that many agency stakeholders within the Cybersecurity community are being asked to perform. After a brief introduction to human capital, the resource guide will describe four broad categories of activities that are used to develop employees and workforces: Workforce Planning, Recruitment/Selection, Employee Development, and Succession Planning. After introducing each activity, the guide will inform business unit leaders, line managers, hiring managers, and human capital professionals on how to use the workforce development matrices to carry out human capital and workforce development initiatives. This section will also highlight best practices and recommendations for each broad category of activities.

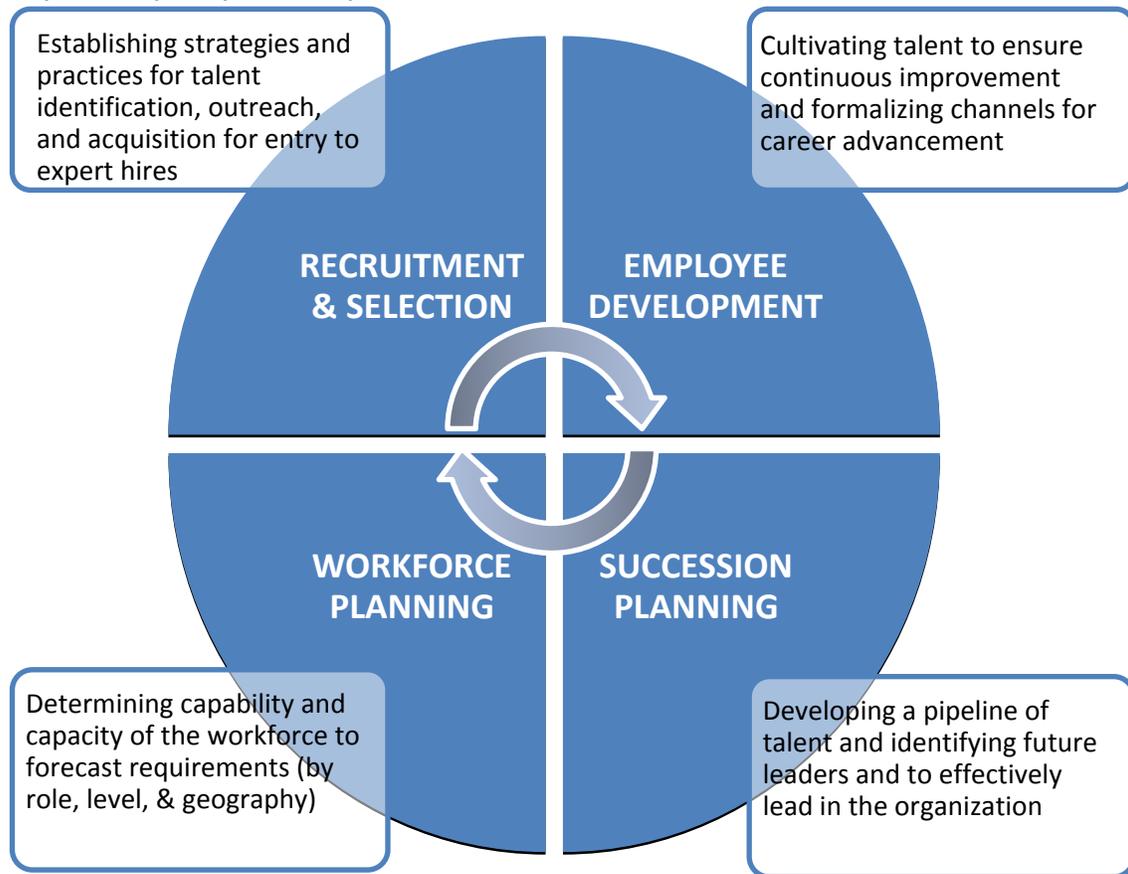
## Human Capital Planning & Workforce Management

The capabilities, competencies, and skills embodied by the federal workforce are vital to the achievement of agency missions. Strategic human capital planning and workforce management are critical linchpins to help the government attract, develop, retain, and motivate highly skilled individuals. These activities also ensure that agencies have sufficient numbers of workers with the appropriate mix of knowledge and skills to meet their missions. Strategic human capital planning and workforce management are systematic processes founded on the notion that managing people assets is like managing other resources (e.g., finances, infrastructure) central to an organization's mission. As "capital," the value of people assets can be enhanced through investment. Engaging in strategic human capital planning is critical to complying with management reforms that have been enacted across the Federal Government.

Four broad themes of human capital planning and workforce management activities particularly relevant to the Cybersecurity professions are (*Figure 3*):

- Workforce Planning
- Recruitment and Selection
- Employee Development
- Succession Planning

CHIEF INFORMATION OFFICERS COUNCIL

**Figure 3. Cybersecurity Workforce Development Matrix Resource Guide Focus Areas**

Each of these themes includes many specific actions that can be taken to build a robust, highly skilled workforce. Although this resource guide is not meant to be exhaustive, the next sections describe each theme, present best practices, recommended activities, and demonstrate how the workforce development matrices can be used to inform many activities within the theme.

## Workforce Planning

In today's complex and challenging work environment, agencies are being asked to do more with less (often with shorter timeframes) to meet changing mission requirements. Workforce planning provides the means for anticipating change and employing strategic methods for addressing present and anticipated workforce issues. Government agencies engage in workforce planning because they are required to conduct a minimum amount of workforce planning to comply with federal standards. To support this need, OPM developed a workforce planning model to guide federal workforce planning activities ([http://www.opm.gov/hcaaf\\_resource\\_center/assets/Sa\\_tool4.pdf](http://www.opm.gov/hcaaf_resource_center/assets/Sa_tool4.pdf)). Despite the prevalence of workforce planning in government organizations, however, effective planning is inherently a challenge because underlying civil service regulations, policies, and culture affect an agency's ability to alter workforce composition quickly in response to mission change.

Workforce planning creates critical links between organizational strategy, environmental demands, and operational action. By engaging in workforce planning, managers can prepare their employees for the

## CHIEF INFORMATION OFFICERS COUNCIL

demands of the work. A workforce plan supports staff by ensuring that the organization has the right number of people with the correct skill sets to perform their duties. Essentially, workforce planning translates business strategy into workforce implications. It shows the connection between how new programs or mission elements affect the number, type, and mix of staff that are needed. Workforce planning also promotes proactive responses to projected and/or impending changes. In this way, it helps organizations acquire the necessary staffing mix *before* any shifts in the work demands.

### Introduction to Workforce Planning

Cybersecurity managers must ensure they have the right amount of talent. With constantly evolving environments, technology, vulnerabilities, and threats, Cybersecurity organizations must ensure that they have the right amount of the correct talent to ensure that the information of the United States government and the American people stays secure, intact, and accessible.

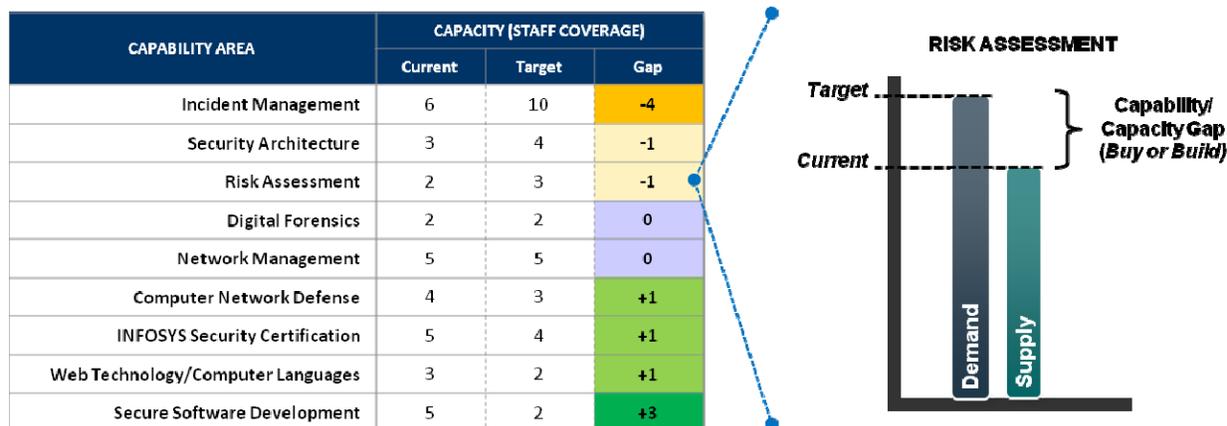
Workforce planning integrates strategic and business planning with an environmental scan to inform budgetary decisions around hiring, training and development, succession planning, and other human capital initiatives. By benchmarking current capabilities and comparing this to environmental indicators of future needs, organizations can identify gaps in their workforce capabilities. These gaps can involve several aspects of the workforce, including:

- Work Load - how much work exists
- Workforce Demand - the skill sets and competencies, and the number of people with these skill sets and competencies, necessary to complete the work successfully
- Workforce Supply - the number of people currently working in the organization with these skill sets and proficiency levels
- Workforce Gaps - the difference between workforce supply and workforce demand

Workforce planning enables comparison of current state of the workforce (workforce supply, work load, and employees' proficiency levels) to the projected future state (workforce demand, estimate future work load, and needed proficiency levels) to identify gaps between the two (*Figure 4*). Workforce planning ensures that the right people with the right skills are in the right place at the right time. It is the responsibility of every manager to support and ensure that effective workforce plans are prepared, implemented with action plans, monitored and evaluated. Managers at all levels have a central role in workforce planning and coordinating and carrying out assignments to successfully implement those plans.

CHIEF INFORMATION OFFICERS COUNCIL

Figure 4. Sample Workforce Capability/Capacity Gap Analysis



### Foundational Steps for Creating Workforce Plans

There are many ways to approach workforce planning, and the correct approach is dependent on the organization’s particular needs, demands, and pressure points. While it is important to customize a workforce plan to get the right mix of people for any particular organization, there are several common foundational steps that will help agency stakeholders set the stage for a robust, tailored workforce plan:

- Step 1: Understand the current capabilities of the workforce
- Step 2: Identify current and future requirements
- Step 3: Identify gaps
- Step 4: Develop strategies to close gaps in the short- and long-term
- Step 5: Monitor, evaluate and revise workforce plan

**Step 1 - Understand the Current Capabilities of the Workforce:** The first step is creating a baseline understanding of what is currently happening within the workforce. It is important at this step to get a true depiction of how the work is actually being done, regardless of how policy states the work should be done. Often, when work processes deviate from policy, the reason is an unidentified workforce planning gap. Therefore, agency stakeholders should strive to assess the work load, flows, and processes as objectively as possible. It may be helpful to speak with subject matter experts about how things get done.

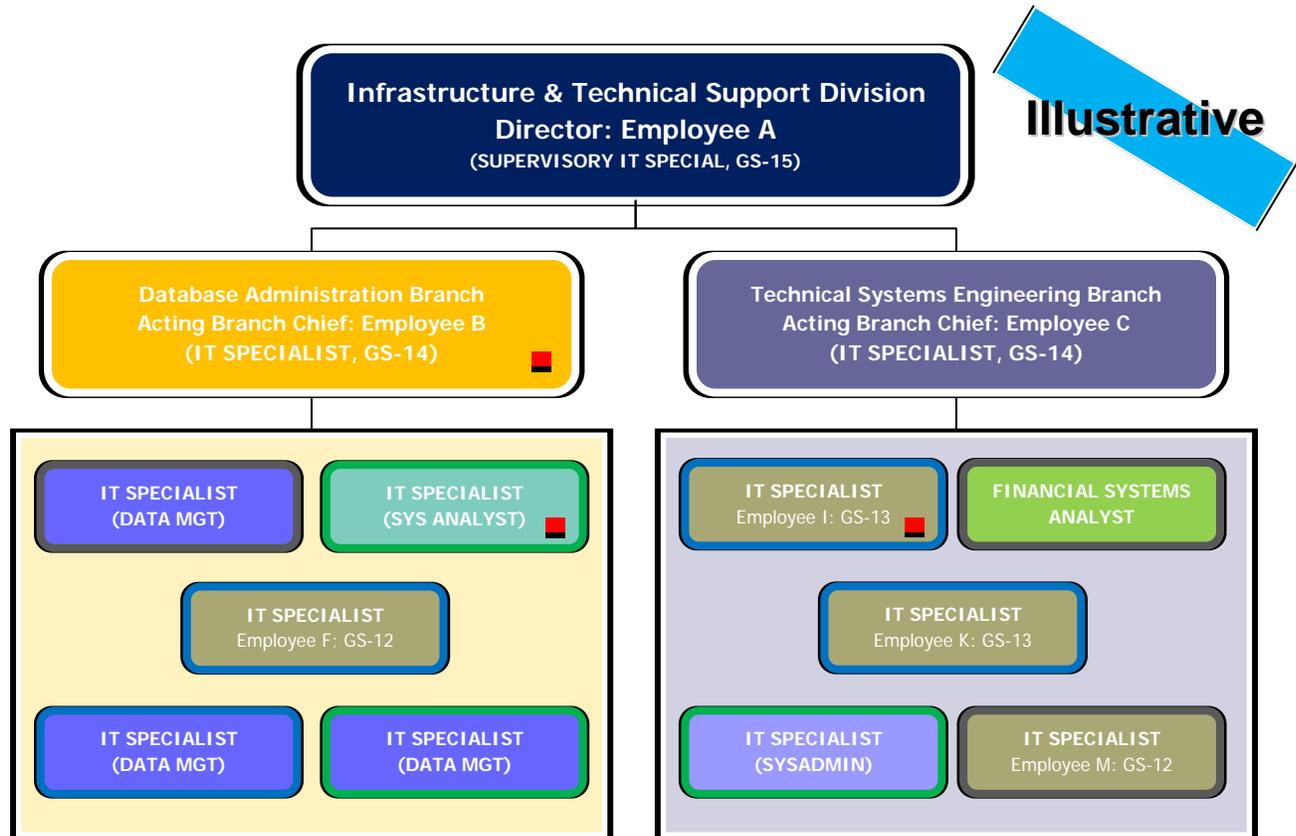
The workforce development matrices provide helpful information for understanding the responsibilities and tasks of people filling each of the roles. This information can help managers understand the current and future needs of the workforce and use these needs to identify gaps that workforce planning can fill.

One useful way of capturing the information provided by the matrices is using a workforce map. Workforce maps are visual dashboards that describe how work is accomplished and who accomplishes the work. Given the unique work in many organizations, it is important to customize and tailor workforce maps to display relevant information. One organization may, for example, depict the number of federal employees versus contractors performing the various job duties. Another organization may be

CHIEF INFORMATION OFFICERS COUNCIL

concerned about impending retirements and highlight the employees who are or are almost retirement eligible. Still other organizations may care about where the work is being done, and could depict people in the organization by location. High-quality workforce maps display several factors at once, such as the example below. This workforce map shows job function by color, location by border, and retirement eligibility by the red squares.

Figure 5. Illustrative Workforce Map



Workforce maps are one way to capture the current state of the workforce, and may be more appropriate for some organizations than others. The critical foundation of all workforce planning, however, is high-quality data. So long as organizations maintain updated, accessible databases with relevant data points about who is doing the work and how they do it, workforce plans can be designed to make focused suggestions for organizational improvement.

**Step 2 - Identify Current and Future Requirements:** Once managers understand the current, actual state of their workforces, they can shift focus to the ideal state and/or future projected state. This will allow them to identify areas that are not successfully being covered by the current state. It can also identify new job duties that are likely to arise with evolving technology, policy, or environmental and societal trends (e.g., telecommuting).

One way to begin this step is to review the workforce development matrices for the skills, competencies, and suggested criteria listed for each role. Given the rapid change in the field and the

## CHIEF INFORMATION OFFICERS COUNCIL

variety of backgrounds from which Cybersecurity professionals come, these standards may already highlight gaps. The matrices can help managers understand current requirements for successful execution of each role. For example, the Systems Operations and Maintenance Professional matrix describes three different levels of experience. As the experience level increases, the need for independence, autonomy, and individual responsibility increase as well. Agency stakeholders can use the matrices to establish the current and future skills needed in the workforce, along with the level at which those skills must be performed to meet their missions.

In addition, agency stakeholders can think about shifts in priorities, new technology, recent policy changes, and other shifting pressures in the environment. How might new rules/regulations, technological advances, and vulnerabilities/threats change the way the type and amount of work? How might these change the ways the work is completed? Will the skills and competencies needed to complete the work change as a result of these environmental shifts? Answering these questions can help identify a “to be” state that can be compared to the current state to identify gaps.

For example, the environment can change in a way that is not directly related to Cybersecurity roles. For example, telecommuting demonstrates societal changes that are evolving the way people are completing their work. It may be possible for many Cybersecurity professionals to work, at least part of the time, from remote locations. Telecommuting can benefit both individuals and organizations by reducing commuting time and stress, increasing employee commitment, reducing sick leave (since employees can work from home while recovering), and boosting morale. Many organizations are even promoting telecommuting as a “green” initiative to reduce environmental impact. As people from many professions begin telecommuting more often, however, what will be the Cybersecurity implications for communicating virtually and collaborating from multiple work sites? Not only might Cybersecurity professionals work remotely and require the technology and virtual leadership to do so, but they may also be asked to support a much broader and more complex information system as other professionals in their agencies telecommute in kind. As agency stakeholders think of the breadth of changes on the horizon, they can begin comparing the competencies and skills needed to complete work with these new demands.

**Step 3 - Identify Gaps Between Current State and Ideal Current/Future State:** Once a clear depiction is created about the projected future state of the work, it can be compared to what is currently happening within the organization. Identifying gaps will allow agency stakeholders to make decisions about how to focus time and resources on closing gaps. Given the different aspects of work that could be implicated by shifts in demand, stakeholders may notice different types of gaps. They may find that employees currently do not possess the skills sets needed to complete work in the future. They could determine that employees have the skills, but the organization does not have enough employees. Alternatively, agency stakeholders may realize that the composition of employees (e.g., the mix of federal employees and contractors) is a risk. Some federal agencies contract out entire sections of work, creating a potential vulnerability if contractors turn over or the organization needs to increase its capacity in that area. Finally, gaps may be identified by the workforce demographic data, which could highlight impending retirements of key individuals. Usually, a workforce planning gap analysis finds a combination of these types of gaps, and plans multifold mitigation strategies accordingly.

## CHIEF INFORMATION OFFICERS COUNCIL

**Step 4 - Develop Strategies to Close Gaps:** The subsequent step to identifying gaps is developing strategies to fill the gaps. A gap in workforce states represents risk. This is particularly true in Cybersecurity roles. Therefore, agency stakeholders should review identified gaps to assess the level of risk that each one possesses, then prioritize gaps to fill and determine the best way to do so. Some gaps are simple to fill and may only require a small shift in job duties or a change in how responsibilities are divided among team members. Alternatively, gaps may require significant restructuring, organizational redesign, and sometimes even geographic relocation. Each organization will have its own boundary conditions that shape the gaps and constrain the potential solutions, but it is important to recognize the full spectrum of workforce planning mitigation strategies.

**Step 5 – Monitor, Evaluate and Revise Workforce Plan:**

Continuous monitoring and feedback is important for the success of any endeavor, especially workforce planning. Work demands, pertinent regulations, and even mission requirements constantly shift, so strategies that were devised and implemented several years ago may not still be appropriate. Therefore, agencies should frequently review of their workforce planning initiatives to make necessary adjustments.

Conducting this review can be a relatively simple process, and may only involve a quarterly or bi-annual meeting among organizational leadership to discuss any changes in the work supply, work demand and mission requirements. Sample questions to discuss at such meetings could include:

1. Have the workforce planning strategies we previously implemented been successful?
2. Have there been any relevant changes in federal or agency policy that affects the composition of our workforce?
3. Are there any new anticipated changes to the work load or mission requirements that we have not previously addressed?
4. Are there any new risks or changes to our work supply (e.g., impending retirements, increased attrition, etc.)?

If there is an affirmative answer to any of these questions, then agency stakeholders should return to steps 1 through 4 to reassess and update their workforce planning strategies.

Ultimately, workforce planning mitigates risk. By proactively identifying and mitigating gaps in the workforce's abilities to meet projected work demands, organizations with workforce plans prepare for the future before employees are over-burdened. This increases commitment and engagement of employees, bolstering retention and reducing the need to spend time and resources refilling current positions. In addition, workforce planning helps employees understand potential career paths within

**Figure 6: Example of Workforce Plan Mitigation Strategy**

The Internal Revenue Service worked to convert paper tax returns to electronic filing. In two years, the number of Americans using e-file technology jumped more than 50%. This meant fewer people were needed to process paper claims, but more were needed to service the technology of e-filing. The IRS therefore engaged in a significant restructuring to retrain and redeploy paper claims adjusters to IT roles.

This is an extreme, but successful, case of workforce planning. Organizational goals, powered by technology, changed the nature of work for thousands of employees. So they, and their organization, had to adjust to meet the new demands.

## CHIEF INFORMATION OFFICERS COUNCIL

their organizations, which can clarify long-term career trajectories. Workforce planning ensures organizations have proper amounts of employees with necessary skills to meet their current and future missions.

The next section describes how agency stakeholders can prepare for future leadership vacancies by using the matrices to develop deep benches of emerging leaders among current employees.

## Recruitment & Selection

The following section of the Resource Guide addresses strategies for developing and posting vacancy announcements, enhancing strategic recruitment efforts to attract Cybersecurity job applicants, and techniques for evaluating, rating, and ranking job candidates using crediting plans and structured interviews. To ensure that the organization's people practices meet federal law, rules, regulations, and merit systems principles, a collaborative approach with human resources/human capital representatives is necessary for adopting the recommendations in this section.

### Begin with a Job Analysis

Before engaging in recruitment and selection activities, it is important to create standardized position descriptions that are based on a thorough job (or occupational) analysis. Many positions have already undergone job analysis, so line managers and hiring managers can begin with standardized position descriptions. For positions that do not yet have standardized and/or current position descriptions, job analysis is the foundational first step.

A comprehensive job analysis will include an inventory of the duties and tasks performed in a position, as well as the associated competencies and skills that are required to perform those duties and tasks successfully. Typically, the job analysis will also articulate which duties, tasks, and competencies are critical to each grade level for the position of study.

The job analysis is a necessary component in identifying the proper occupational series, grade level, and minimum standards for candidates as they enter the position. Further, a job analysis helps identify the relevant talent pools from which to recruit candidates. This step also ensures that the vacancy announcement and the evaluation criteria of candidates are customized to support the agency-defined competencies, knowledge, skills, and abilities for the position of study. Job analyses are critical for developing assessment tools, like crediting plans and structured interviews. The resource guide will cover these assessment tools in a later section.

Job analyses require proper implementation of approved methodologies (e.g., Position Analysis Questionnaire) in accordance with the *Uniform Guidelines on Employee Selection Procedures* (1978). Therefore, qualified human resources representatives should work with functional subject matter experts to conduct the job analysis. The rest of this section will describe activities related to recruitment and selection, with the assumption that legally defensible job analyses have already been conducted.

## CHIEF INFORMATION OFFICERS COUNCIL

**Strategic Recruitment**

The quantity and quality of Cybersecurity professionals entering the government can be tied to the quality of recruiting and hiring efforts. Unfortunately, these efforts often involve ill-defined job descriptions, unclear essential skills requirements, and unappealing incentive structures. As a result, top Cybersecurity professionals are likely to take positions in the private sector. The workforce development matrices can assist agencies in developing strategic recruitment strategies to identify top talent. An effective strategic recruitment plan contains a clearly defined value proposition. To develop a value proposition, agencies should ask questions such as: *What can our agency offer prospective candidates? What types of opportunities are cyber professionals seeking? Are we aligning the agency's career opportunities to the values of the talent pool?* There is a wealth of opportunity for individuals who decide to launch a career in the Federal Government, but agencies must develop compelling messages delivered through channels that reach the best candidates. Agencies can utilize the workforce development matrices to develop an effective strategic recruitment strategy consisting of three essential components: Program, Message, and Channels (*Figure 7*).

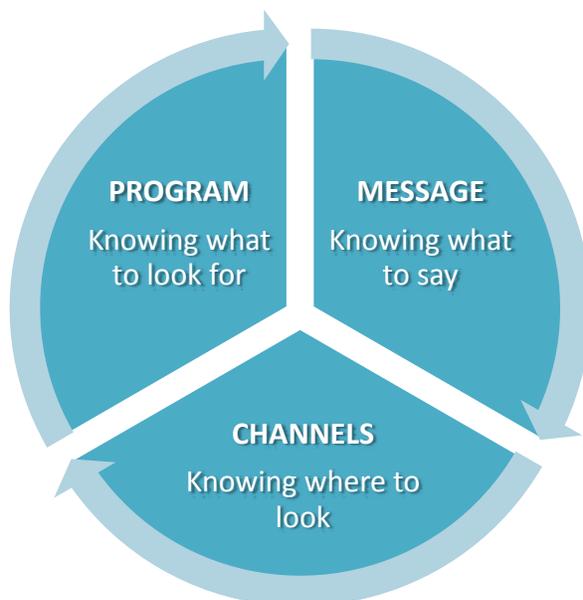
**Program – Knowing what to look for:** To build a pool of job candidates that best meet position requirements, agency stakeholders must first understand their need. One way to do this is identifying the competencies and skills that the new hire should possess upon entry. Then, using this information, stakeholders, including hiring managers and human capital professionals, can devise strategic recruitment strategies to find Cybersecurity professionals with those competencies and skills.

To help stakeholders begin this process, the matrices provide information on competency and skills models that are important for each Cybersecurity role. In addition, a recent, valid job analysis on the

position should provide detailed information on the necessary skills levels. Because job openings may exist at different GS grades, the matrices describe different levels of complexity for Cybersecurity professionals at entry, intermediate, and advanced performance levels.

Agency stakeholders can use the matrices and other resources to develop a specific set of requirements for the candidates, and can identify the best sources of talent that possess these skills. It is important to recognize that while these roles are highly technical, the competencies and skills needed to succeed within them also included non-technical, “soft” skills and business acumen. Stakeholders should focus on both technical and non-technical skills (e.g., communications skills, writing ability, ability to make persuasive arguments, ability to present to non-technical audiences, ability to

**Figure 7: Recruitment Strategy Components**



## CHIEF INFORMATION OFFICERS COUNCIL

communicate with upper management, etc.) when creating position requirements. The workforce development matrices include these non-technical skills as well, and provide a good foundation for writing position descriptions and vacancy announcements.

Additionally, the matrices identify suggested credentials for Cybersecurity professionals. By outlining the suggested experience, educational backgrounds, and certification requirements that may be relevant to each role, the matrices can help agency stakeholders assess candidate resumes to identify relevant skill-building experiences.

The matrices can be used to develop strategic recruitment strategies that help pinpoint individuals possessing the competencies, skills, education, and experience that are required to perform each role successfully. Agencies stakeholders can then quickly scan resumes and identify candidates with the desired skill sets, saving time and resources during the recruitment process.

**Message – Knowing what to say:** According to the *NetGeneration: Preparing for Change in the Federal Information Technology Workforce* report, “NetGener,” 18- to 31-year-olds who have grown up around technology their entire lives, will replace current agency Cybersecurity professionals who are retiring from the Federal Government (NetGeneration, p. 34). These young professionals prefer to avoid the bureaucracy of large organizations and tend to make frequent transitions across organizations to look for better career opportunities. Young Cybersecurity professionals also expect autonomy and challenging job duties and responsibilities (NetGeneration, p. 40). The NetGeneration report can be found at <http://www.cio.gov/Documents/NetGen.pdf>.

To recruit young Cybersecurity professionals into the federal government, agencies should use the matrices to create marketing materials for recruiting events that highlight the amount of autonomy, complex job duties, and important responsibilities required for these Cybersecurity positions. Regardless of the demographic characteristics of Cybersecurity professionals, agencies should use the matrices to develop marketing materials for recruiting events that clearly lay out career paths and their benefits. Agencies can create Cybersecurity career paths by using the matrices to distinguish between performance levels for Cybersecurity roles (e.g., entry, intermediate, and advanced). Matrices can be used to distinguish characteristics of work requirements and to highlight benefits associated with each performance level (e.g., increased autonomy at the advanced level). When creating marketing materials for these career paths, agencies can use the matrices to suggest learning and development resources useful for candidates to pursue to enhance their competencies and skills to the level required for these advanced roles.

Along with using the matrices to develop marketing materials for recruiting events, agencies should recruit using high-touch communication with candidates. High-touch communication involves agencies keeping candidates abreast about where they stand in the hiring process, and answering any questions candidates may have in a timely manner. Today’s job candidates expect frequent updates about their status in the recruitment process, and agencies can improve acceptance rates simply by sending more information to candidates. Would-be employees also expect a high degree of “integrity” in the recruitment process. “Integrity” in this context means that along with accurate vacancy announcements,

## CHIEF INFORMATION OFFICERS COUNCIL

agencies should communicate to applicants exactly what role they will serve in the Cybersecurity positions. Agencies can use the workforce development matrices to ensure that they are relaying accurate information about the job duties and complexity of Cybersecurity positions to applicants.

**Channels – Knowing where to look:** For agencies to engage in strategic recruiting, they have to know where to find the right talent. With increasing focus on Cybersecurity education and career development, colleges and universities are developing Cybersecurity programs, and these institutions are producing candidates who are ready for successful careers in the Federal Government. The private sector targets gifted students at these colleges and universities long before their expected graduation dates. For the Federal Government to meet Cybersecurity talent needs, agency stakeholders need to aggressively target these students through effective advertising, which will be discussed later in this guide.

Additionally, agencies must understand which activities Cybersecurity professionals enjoy and how they search for jobs. Many of these professionals are not actively looking for new employment opportunities, so agencies must create a marketing brand that caters to passive job seekers. The Internet is typically the first interaction candidates have with an organization, and this is particularly true of younger Cybersecurity professionals. Websites with a clean visual look, strategic messaging, social media tools, and online engagement that tech-savvy people expect from Web interaction are much more likely to be effective for attracting top-quality candidates. Although some agencies may not be able to add online engagement capabilities to their web pages (e.g., Live Chat), for those that can, this technique is a useful way of attracting top Cybersecurity talent because it shows how the agency values technology and implements it to improve communications, collaboration, and efficiency.

Many Cybersecurity professionals use various forms of social media to communicate with friends and colleagues, perform daily activities (e.g., shopping), and to search for jobs. These media are extremely important resources for reaching Cybersecurity talent. Platforms like Facebook, Twitter, LinkedIn, and Second Life are not only effective, but have become expected platforms for linking open positions with qualified candidates. For agencies that are able to use these websites, they are helpful tools for establishing brand awareness and identity within these online media to reach relevant talent pools.

Agencies can use the matrices to identify offline communities, like universities and professional networking organizations, which can serve as important recruiting channels. Agencies should also develop and host their own recruiting mechanisms, such as recruiting events and referral systems, to achieve broad Cybersecurity talent acquisition goals. The power of referrals, particularly within the Cybersecurity community, cannot be overstated. People want to hear about career opportunities from people they trust. Employees' networks of colleagues are extremely valuable talent pools, and agencies should encourage current employees to refer candidates to the recruitment process. Creating tangible incentives for current employees to bring external Cybersecurity talent into the agency is an important component of any agency's recruitment strategy.

Having discussed the three critical components of recruitment strategies, there are several additional factors to consider.

## CHIEF INFORMATION OFFICERS COUNCIL

**Length of Hiring Process:** When building strategic recruitment plans, agency stakeholders must consider the amount of time it takes to hire professionals into their agencies. Job candidates can become very frustrated with the cumbersome federal hiring process. To reduce the complexities and overall time of the hiring process, agencies should leverage existing federal scholarship, internship, and student experience programs (for additional information, go to <http://www.opm.gov>). Using these hiring flexibilities, agencies can work around the lengthy hiring process and directly acquire Cybersecurity talent.

Additionally, agencies should assess whether their Cybersecurity job vacancies fall within OPM's 2210 series or within the Acquisition profession. If they fall under these categories, agencies can use direct-hire authority to fill associated vacancies within their agencies.

The Office of Personnel Management is also undertaking several initiatives under the Hiring Reform effort to increase the efficiency of the federal hiring process. This includes identifying the competencies required for various occupational series, developing applicant assessment tools, and sharing best practices employed across the government to foster greater collaboration between organizations and utilization of these practices. Once agencies have developed strategic recruitment plans, it is important to support these plans by tailoring vacancy announcements to fit the particular specifications of the positions.

### Developing Vacancy Announcements

Much like a commercial advertisement, the vacancy announcement is a critical, and sometimes the only, tool for communicating accurate information about the position to job applicants. Vacancy announcements also communicate the organization's expectations of candidates applying for the job. The objective in creating a vacancy announcement for Cybersecurity positions are to 1) clearly communicate information about the job and its duties and requirements, and 2) attract job applicants whose experiences and background are aligned with the organization's requirements for the position. Done effectively, the vacancy announcement plays an important role in positioning the right candidates for hire into the organization.

The challenge in creating a targeted vacancy announcement is clearly presenting important information about the position among all of the procedural and legal information that must also be included in fulfilling public notice requirements for federal government positions. The list below is taken from the Office of Personnel Management's (OPM) Delegated Examining Unit (DEU) Handbook (<http://www.opm.gov/deu>), and presents an inventory of items that are required to be included in a vacancy announcement. Although all of these items are important in developing vacancy announcements, managers can shape the position by focusing on three of these components: *Title of the Position*, *Description of Duties*, and *Qualifications Requirements*.

- Agency Name
- Announcement Number
- **Title of the Position**
- Series, Grade(s) (or equivalent), & Entrance Pay
- Open & Closing Dates
- Duty Location & Number of Vacancies

## CHIEF INFORMATION OFFICERS COUNCIL

- [Description of Duties](#)
- [Qualification Requirements \(Competencies/KSAs required, per OPM guidance\)](#)
- Basis for Rating
- Type of Rating Procedure (numeric rating or category rating)
- Type of Assessment(s) to be Used
- Interview Scoring (if interview is used; pass/fail or scored)
- Description of Each Quality Category (if using category rating)
- Drug Testing Requirements
- How to Apply & What to File
- Agency's Definition of "Well-Qualified" (CTAP/ICTAP)
- Information on How to Claim Veterans' Preference
- Equal Employment Opportunity Statement
- Reasonable Accommodation Statement

**Title of the Position:** At the most basic level, the title of the position is an important aspect that potential candidates will use to determine their interest in learning more about and applying for the position. The position title should align with and generally describe the type of work performed by the incumbent. Further, the title should be recognizable to potential candidates seeking to apply to jobs of this type. When determining how to announce the vacancy, an analysis of the position and its functions should be performed to determine the appropriate occupational series. The workforce development matrices describe Cybersecurity roles without referring to specific occupational series or job titles. This feature of the matrices allows for agency-level interpretation in determining which occupational series is most appropriate for the position being filled.

Choosing the right title depends, in part, on selecting the correct occupational series. Not all Cybersecurity positions have to be announced using the Information Technology Management - 22XX occupational series. Given the breadth of capabilities performed by Cybersecurity professionals, these positions can be announced using the Intelligence - 0132, Management and Program Analysis - 0343, Computer Engineering - 0854, Electrical/Electronics Engineering - 0855/0856, Cryptography/Cryptanalysis - 1540/1541,

Computer Science - 1550, and Criminal Investigation - 1811 series, among others. Since OPM's basic qualifications criteria (i.e., education and/or years of experience) are dependent upon the occupational series, selecting the appropriate series is important. There may be limitations on the ability to modify position titles based on the occupational series that is being announced. For example, if hiring for a position in the 2210 IT Specialist occupational series, there are 11 parenthetical titles that can be used to describe the type of work that will be performed in the position. The position may be announced using parenthetical descriptions like "IT Specialist (Cybersecurity)" as opposed to a general "IT Specialist."

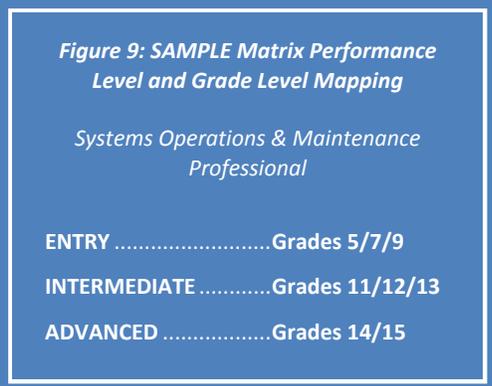


CHIEF INFORMATION OFFICERS COUNCIL

The amount of flexibility in selecting the appropriate position title varies by occupational series and agency. Review the role definitions and descriptions of work performed in the workforce development matrices to select the series and title that aligns most with the type of position being filled. Create a listing of occupational series and position titles that could be used to announce positions of that type. When ready to announce the position, select the series and position title that aligns most with the job.

**Description of Duties:** The description of duties provides potential candidates with better insight into the actual job duties and responsibilities that are expected by the position. This insight allows candidates to determine whether the requirements of the job meet their capabilities and expectations.

The matrices include several components that can assist in drafting the vacancy announcement’s description of duties. First, the role definition provides an overall summary of the job functions and responsibilities. This high-level overview of the role and its primary functions can be used to summarize the position and how it supports the organization. Second, the Description/Complexity provides further definition about job functions specific to the performance level of the position (e.g., Entry, Intermediate, or Advanced; as applicable). This can be used to tailor the description of duties as appropriate for the level of position that is being announced. For example, if the position is being announced at the GS-5 or GS-7 levels (or equivalent pay bands/pay scales), the Description/Complexity for the Entry performance level is likely most appropriate for the position.



When developing the description of duties, consider the grade level (or equivalent) of the position and determine which matrix performance level and associated description is most appropriate. Similar to the position titles, consider creating a mapping of performance levels and grade levels for the position (Figure 9). As the specific position duties, functions, and levels of complexity vary from agency to agency, determine the appropriate performance and grade level mapping for the position as it exists within the organization, and use the matrices to write the description of duties to accurately reflect the work performed in the position.

**Qualification Requirements (Competencies/KSAs required):** The Qualification Requirements is one of the most important sections of the vacancy announcement. This section defines the minimum education, experience, or combination education and experience requirements. There are two components of the qualifications requirements: the minimum federal qualifications requirements and the competency/KSA requirements.

The minimum federal qualifications requirements are established by OPM and are defined for particular occupational groups and series. These requirements specify the minimum education and experience candidates must possess to be considered qualified for the position for which they are applying. Additionally, these requirements are dependent upon the grade level (or equivalent) for which the

CHIEF INFORMATION OFFICERS COUNCIL

candidate is applying. Although agencies must follow OPM’s minimum qualifications requirements for the occupational series and grade level, there is flexibility in defining exactly what some of the requirements will be for each agency.

Table 2 presents OPM’s minimum qualifications for the Information Technology Management 2210 occupational series. The table displays the minimum education and experience requirements for the 2210 occupational series at each associated grade level. For example, to qualify at GS-5, candidates must possess a Bachelor’s degree in one of the specified areas of study, IT-related experience demonstrating the identified competencies, or a combination of education and experience factors.

**Table 2. Information Technology Management Series 2210 Qualification Standard\***

This standard allows eligibility through meeting either requirements specified in the section and titled **Education** or the requirements specified in the section titled **Experience**.

Grade Level	Education	Experience
GS-5 (or equivalent)	Bachelor's degree	IT-related experience demonstrating each of the four competencies listed below. The employing agency is responsible for identifying the specific level of proficiency required for each competency at each grade level based on the requirements of the position being filled. <ul style="list-style-type: none"> <li>▪ Attention to Detail</li> <li>▪ Customer Service</li> <li>▪ Oral Communication</li> <li>▪ Problem Solving</li> </ul>
GS-7 (or equivalent)	1 full year of graduate level education or Superior Academic Achievement	One year of specialized experience at the next lower GS-grade (or equivalent). Specialized experience is experience that has equipped the applicant with the particular competencies/ knowledge, skills, and abilities to successfully perform the duties of the position and is typically in or related to the work of the position to be filled. Such experience is typically gained in the IT field or through the performance of work where the primary concern is IT. The employing agency is responsible for defining the specialized experience based on the requirements of the position being filled.
GS-9 (or equivalent)	Master's degree or equivalent graduate degree or 2 full years of progressively higher level graduate education leading to a master's degree or equivalent graduate degree	
GS-11 (or equivalent)	Ph.D. or equivalent doctoral degree or 3 full years of progressively higher level graduate education leading to a Ph.D. or equivalent doctoral degree	

\* When this qualification standard is used, agencies must have documentation based on a job analysis to substantiate that the position requires IT-related education and/or IT-related experience upon entry.

*Undergraduate or Graduate Education:* Degree in computer science, engineering, information science, information systems management, mathematics, operations research, statistics, or technology management or degree that provided a minimum of 24 semester hours in one or more of the fields identified above and required the development or adaptation of applications, systems or networks.

*Experience:* Experience must be IT related; the experience may be demonstrated by paid or unpaid experience and/or completion of specific, intensive training (for example, IT certification), as appropriate.

<http://www.opm.gov/qualifications/Standards/IGRS/gs2200/2210-AltA.asp>

The key to leveraging the flexibility provided by OPM lies in determining the required competencies/KSAs, identifying the necessary proficiency level in these competencies/KSAs, and defining the specialized experience (according on the agency’s requirements) necessary for success in

## CHIEF INFORMATION OFFICERS COUNCIL

the position. The workforce development matrices provide references that can assist agencies in translating their role requirements to the vacancy announcement.

The matrices provide descriptions of the duties and functions performed by various Cybersecurity roles. These descriptions can be used to develop more specific examples of specialized experience that job applicants would have to demonstrate to be qualified for the position. Additionally, the matrices provide sources of competency and skill models that are relevant to the capability requirements of the associated roles. The job analysis and competency/skill models can be used to identify the specific capability requirements to determine minimum qualifications for job applicants. Review these available resources and work with the agency's human resources professionals to determine the competencies and skills that will be used to address agency-specific capability requirements.

### Crediting Plans

Once a pool of job applicants has met minimum qualifications for the position, agency stakeholders must evaluate the applicants to identify those whose capabilities and experiences are most relevant to the position being filled. This process is known as the rating and ranking process. Rating and ranking involves the application of various assessment tools to identify the candidate(s) with the greatest potential for success in the position. Assessment tools used to rate and rank include crediting plans, structured and behavioral event interviews, situational judgment tests, job knowledge tests, assessment centers, and work samples. Since agencies aim to select the best-qualified candidate(s) for the job, rating and ranking is an important stage of the selection process. Agency stakeholders must collaborate to ensure that their assessment-related activities meet federal laws, rules, and regulations.

A crediting plan (or rating schedule) is an assessment tool used to make evaluations of applicants' job-related competencies/KSAs. It is an index of job-related qualifications criteria relevant to applicants' backgrounds (e.g., job experience, positions held, levels of responsibility, accomplishments, job-related education, certifications, etc.). Applicants are evaluated against these criteria by a qualified rater, or through their self-assessment narrative or multiple-choice responses. Ratings are compared to crediting plan criteria. The following table (*Table 3*) is taken from OPM's DEU Handbook, and provides an overview on the use of crediting plans for evaluating job applicants.

CHIEF INFORMATION OFFICERS COUNCIL

**Table 3. Overview of Crediting Plan Assessment Tools**

Strengths	Considerations	Example
<ul style="list-style-type: none"> <li>▪ Inexpensive</li> <li>▪ Can be developed quickly</li> <li>▪ Multiple choice crediting plan is easy to score</li> </ul>	<ul style="list-style-type: none"> <li>▪ Verifying the applicant’s responses will help reduce the possibility of “inflated” self-ratings.</li> <li>▪ Multiple choice rating schedules can be scored quickly, but also limit the opportunity for an applicant to demonstrate his or her competencies.</li> <li>▪ Crediting plans using a narrative response format can take more time to score than rating schedules. Automating the collection and scoring of a crediting plan will reduce the resources needed.</li> </ul>	<p>A web-based assessment as part of the application process where the individuals rate their own experience on job-related competencies, tasks, activities, etc.</p>

Workforce development matrices offer a great deal of material that can be incorporated into the development of a crediting plan. Effective crediting plans will cover the breadth of candidate experiences relevant to the position being filled. The descriptions of performance, competencies, education, and credentials found in the matrices can be used to identify the depth and breadth of capabilities to be included in this type of assessment.

The following are some steps to take while developing a crediting plan for Cybersecurity positions:

**1. Review matrix components to identify content areas to be included in the crediting plan:** There are several sections of the matrix that might be used to create a framework for evaluating applicant backgrounds in the crediting plan. Suggestions include the Description/Complexity, Competencies and Skills, and Suggested Credentials. These sections provide the raw materials that will be used identify the important competencies/KSAs, and to create associated descriptions of quality levels in the crediting plan. For example, the Description/Complexity section describes the primary functions and responsibilities performed in the position at the associated performance level. Additionally, the Competency/Skill section provides sources of competencies that are required for successful performance in the job or role. This information is valuable in identifying the important areas of performance that should be addressed in the crediting plan. A review of the matrix will serve to identify all of the areas of performance that are appropriate or necessary to evaluate in the crediting plan.

**2. Select the competency/KSA areas:** Once the matrices have been reviewed and applicant qualifications content has been identified, select from the job analysis and matrix the set of competencies/KSAs that will be used to evaluate the applicant’s background. The competencies/KSAs should be comprised of a representative set of capability areas that are important to successful performance in the position. The competencies/KSAs represent key areas of performance, and will be further defined in the next step. For example, in developing a crediting plan for the Systems Operations & Maintenance Professional role, competencies/KSAs to consider may include Cybersecurity Program Management, Compliance Assessment & Evaluation, Systems Operations Procedures, and Systems Maintenance Practices. Remember, the competencies/KSAs used for the crediting plan must be grounded in a robust job analysis. If the desired competencies/KSAs are not represented in the job analysis, agency stakeholders should work with human resources representatives on an appropriate solution. Agencies have the ability to develop and define their own unique competencies through this process, and should take advantage of this flexibility.

## CHIEF INFORMATION OFFICERS COUNCIL

**3. Identify and describe quality levels for each competency/KSA:** Detailed descriptions of each competency/KSA should be written once they have been selected. Descriptions should be written for distinct levels of quality associated with the competency/KSA (e.g., Exceptional, Good, and Minimally Qualifying). Descriptions of duties performed, competency/skill proficiencies, and role-related experiences from the matrices can be used to develop these quality level descriptions (*Figure 10*). Evaluators can use these descriptions to review applicants' resume and narrative responses and determine which level most appropriately reflects applicants' qualifications in the associated competency/KSA.

**Figure 10: SAMPLE Crediting Plan Qualification Level Descriptions**

**SAMPLE Crediting Plan Qualification Level Descriptions**

**Competency/KSA: Cybersecurity Program Management**

**Exceptional Experience:** Demonstrated experience independently managing, planning, and evaluating Cybersecurity compliance systems; Experience developing program objectives and managing associated budgets; Experience managing complex projects, programs, and initiatives with high threat and large scope (e.g., inter-governmental); Experience reporting on progress and milestones to agency/external representatives; Possesses multiple certifications in various Cybersecurity-related areas

**Good Experience:** Experience leading components of Cybersecurity compliance projects, programs, and initiatives; Experience working on projects, programs, and initiatives with medium-threat and moderate scope (e.g., agency-wide); Experience developing reports for program leadership; Possesses one Cybersecurity-related certification

**Minimally Qualifying Experience:** Experience as a supporting team member on security compliance projects, programs, and initiatives; Experience working on projects, programs, and initiatives with low threat and scope (e.g., inter-office); Experience recording/tracking data for report development and program evaluation

Once the crediting plan has been developed using the steps outlined above, it is recommended that the plan be reviewed by a sampling of subject matter experts familiar with the position and its requirements. The subject matter experts can make additional recommendations for revising and refining the crediting plan content so that it is most effective in identifying the candidates whose background and experience lend themselves most to the requirements of the position being filled.

Often, the use of the crediting plan is incorporated as part of the online application process. In these situations, the crediting plan content needs to be transformed into candidate self-assessment rating questions with associated point values. To perform this transformation, look at the quality level descriptions that were created for each of the competency/KSA areas. Write self-assessment questions that reference the competency/KSA descriptions, including response options from which the applicants will select. Assign point values to each response option, making sure to look across all self-assessment items to ensure that point values are distributed proportionally across items and competencies/KSAs (*Figure 11*).

CHIEF INFORMATION OFFICERS COUNCIL

**Figure 11: SAMPLE Applicant Self-Assessment Crediting Plan Questions**

**SAMPLE Applicant Self-Assessment Crediting Plan Questions**

**Competency/KSA: Cybersecurity Program Management**

**1. Which statement most accurately describes your experience in Cybersecurity program management?**

- I have independently managed, planned, and evaluated Cybersecurity compliance systems (5 pts)
- I have lead components of Cybersecurity compliance projects, programs, and initiatives (3 pts)
- I have served as a team member on security compliance projects, programs, and initiatives (1 pt)
- I have no experience in Cybersecurity program management (0 pts)

**2. Which statement most accurately describes the highest level of Cybersecurity work in which you have been directly involved?**

- I have worked on complex Cybersecurity projects, programs, and initiatives with high threat and large scope (e.g., inter-governmental) (5 pts)
- I have worked on Cybersecurity projects, programs, and initiatives with medium-threat and moderate scope (e.g., agency-wide) (3 pts)
- I have worked on Cybersecurity projects, programs, and initiatives with low threat and scope (e.g., inter-office) (1 pt)

**3. Consider the following certifications: MCSE, CCNA, CCNP, ISC<sup>2</sup> CAP, CISSP, CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC, PMP. Which of the following statements is true?**

- I possess active certifications in five or more of the above areas (5 pts)
- I possess active certifications in two to four of the above areas (3 pts)
- I possess active certifications in one of the above areas (1 pt)
- I do not possess active certification in any of the above areas (0 pts)

It is recommended that the use of crediting plans be combined with another assessment tool (e.g., structured interview or situational judgment test) for maximum precision in evaluating the full spectrum of applicant capabilities. Additional guidance on using crediting plans as part of the candidate selection process can be found on OPM's Hiring Reform website (<http://www.opm.gov/HiringReform>).

### Structured Interviews

Structured interviews are another method of evaluating applicants in the rating and ranking process. They are one of the most common assessment tools that are used to evaluate candidate qualifications against job requirements. Structured interviews are often a preferred method of assessing candidates, as it allows for a face-to-face dialogue between the hiring manager and prospective employee. Many would agree that only so much can be learned about an applicant from a resume, responses to online rating and ranking questions, or job knowledge test scores. Structured interviews allow for observing behavioral competencies and interpersonal communication styles, factors that are as important to successful job performance as technical or functional expertise.

Structured interviews are comprised of questions that address the candidate's job knowledge, work sample assessments and work requirements based on the competencies/KSAs critical to successful performance in the position being filled. Responses to structured interview questions are rated using established criteria, benchmarks, or indicators that describe behavioral-based examples of high, medium, and low levels of competency/KSA proficiency. A properly developed structured interview is an effective tool for probing into the candidate's background and experience to gain additional information

CHIEF INFORMATION OFFICERS COUNCIL

about their potential in filling the position. The following table (*Table 4*) is taken from OPM’s DEU Handbook, and provides an overview on the use of structured interviews for evaluating job candidates.

**Table 4. Overview of Structured Interviews**

Strengths	Considerations	Sample Interview Question
<ul style="list-style-type: none"> <li>▪ High validity and reliability</li> <li>▪ Low adverse impact</li> <li>▪ Viewed as fair by the applicant</li> <li>▪ Comprehensive competency measurement</li> <li>▪ Short administration time (1 hour)</li> <li>▪ Difficult for applicants to "fake" responses</li> </ul>	<p>A structured interview usually requires involvement of management and subject matter experts for panel participation. Preparing and scheduling participants in advance will significantly reduce the resources required to conduct a structured interview. Reducing the size of the applicant pool through recruitment and/or assessment will help decrease the number of interviews needed.</p>	<p>"Describe a situation in which you identified a problem and evaluated the alternatives to make a recommendation or decision."</p>

Similar to the process outlined for developing crediting plans based on workforce development matrix components, the matrices can be leveraged in the development of structured interviews by identifying critical functional areas, and crafting interview questions and responses that will be used to evaluate the candidate.

Follow these steps in developing a structured interview for Cybersecurity positions:

**1. Review matrix components to identify content areas to be addressed through the structured interview:** There are several sections of the matrix that might be used to create a framework for evaluating applicant backgrounds in the interview. Suggestions include the Description/Complexity, Competencies and Skills, and Suggested Credentials. This content be used identify the important competencies/KSAs that will form the basis of the interview questions that evaluate candidate experience and capabilities in those areas. For example, the Description/Complexity section describes the primary functions and responsibilities performed in the position at the associated performance level. Additionally, the Competency/Skill section provides sources of competencies that are required for successful performance in the job or role. This information is valuable in identifying the important areas of performance that should be addressed in the interview. A review of the matrix will serve to identify all of the areas of performance that are appropriate or necessary to evaluate in the interview.

**2. Select the competency/KSA areas:** Once the matrices have been reviewed, select from the job analysis and matrix the set of competencies/KSAs that will be used to evaluate the candidate in the interview. The competencies/KSAs should be comprised of a representative set of capability areas that are important to successful performance in the position. The competencies/KSAs represent key areas of performance, and will be used to develop the actual interview questions and rating criteria. Remember, the competencies/KSAs used for the structured interview must be part of the job analysis. If the desired competencies/KSAs are not represented in the job analysis, work with agency human resources representatives on an appropriate solution.

**3. Write interview questions:** For each competency/KSA selected, develop one or a series of interview questions that could be used to evaluate candidates’ capabilities or proficiency levels in the area. The matrices offer descriptions of work activities and functions that can be used as the basis for interview questions. For example, one of the descriptions for the Information Security Assessor role is that

## CHIEF INFORMATION OFFICERS COUNCIL

individuals in this role “*apply an understanding of Cybersecurity compliance when reviewing systems and security documentation, explaining risks to system owners, implementing risk mitigation controls, and enforcing Cybersecurity policies.*” A structured interview question based on this important activity might be, “Tell me about a time when you were responsible for implementing or evaluating a risk mitigation control. In your response, please describe your role, the action you took, and the result.” Identify additional duties performed in the position that require the selected competencies/KSAs and develop interview questions that relate to the candidate’s experience performing similar duties.

Another method for developing interview questions is to use content of the matrices to identify personal experiences or situations related to the associated information or cybersecurity position where significant observations of positive or negative performance have been made. A structured interview question might be developed based on that experience/observation to assess and evaluate how the candidate would perform in a similar situation. For example, an interview question for Systems Operations & Maintenance Professional candidates might be, “What immediate steps would you take if you noticed that a critical security application had malfunctioned? What considerations did you make when determining your response?”

These techniques can be used to develop interview questions for each of the competencies/KSAs selected for assessment. Evaluate the series of questions developed to ensure that the competencies/KSAs are proportionally represented. In other words, the most critical competencies/KSAs should have greater representation than those that are still important, but perhaps less critical. When determining the appropriate number of interview questions to develop, consider the number of competencies/KSAs being assessed and the amount of time planned for each interview.

**4. Develop interview question response rating criteria:** Once interview questions have been developed, agency stakeholders should define the criteria they will use to evaluate candidate responses. The definition of rating criteria is an important activity to perform as part of the structured interview development. Whether interviewing one or many candidates, rating criteria allow for consistent evaluations across interview responses. Consistency in ratings is necessary to reliably identify the candidates who are most likely to be successful in the position.

For each structured interview question, identify the key factors or elements that would determine superior, acceptable, and poor responses. Describe and document these factors and elements under the appropriate rating category. Superior responses should address all of the key factors identified. Often, a poor response to an interview question is not about the things the candidate included in the answer, but instead reflects things the candidate left out of the response. Include these in the rating criteria as well. *Table 5* provides an example of a structured interview question, rating categories (e.g., Exceptionally Strong, Strong, Moderate, etc.), and the specific rating criteria that are associated with each category.

CHIEF INFORMATION OFFICERS COUNCIL

**Table 5. SAMPLE Competency/KSA-based Structured Interview Question & Rating Criteria**

Competency/KSA: Problem Solving			
<b>Lead Question:</b>	Describe a time when you were asked to assess or evaluate an information or cybersecurity-related program.		
<b>Probe(s):</b>	<ul style="list-style-type: none"> <li>▪ How did you determine the relevant information to collect?</li> <li>▪ What analysis techniques did you use to build findings?</li> <li>▪ On what grounds did you draw conclusions from your findings?</li> <li>▪ How did you build recommendations from your conclusions?</li> <li>▪ What was the outcome of your assessment or evaluation?</li> </ul>		
Rating Criteria			
Poor Response	Moderate Response	Strong Response	Exceptional Response
<ul style="list-style-type: none"> <li>▪ Explains which resources were used to investigate problems but does not explain solutions reached and implemented</li> <li>▪ Cannot explain tools (e.g., diagnostic tools, quantitative/qualitative data analysis techniques) used to make decisions</li> <li>▪ Cannot explain an approach for structuring information</li> </ul>	<ul style="list-style-type: none"> <li>▪ Structure information and breaks down the issues into logical categories</li> <li>▪ Explains a variety of tools used to assist in his/her evaluation and decision making (e.g., diagnostic tools, quantitative/qualitative data analysis techniques)</li> <li>▪ Explains how he/she identifies a problem and explains how he/she solves it independently or goes through the proper channels to solve the problem</li> </ul>	<ul style="list-style-type: none"> <li>▪ Describes experience using a range of diagnostic tools, qualitative and quantitative data analysis techniques, and demonstrates the ability to draw conclusions based on the data gathered</li> <li>▪ Explains how he/she solves problems by utilizing available resources and follows through by developing and implementing a solution</li> <li>▪ Explains how he/she anticipates and mitigates problems</li> </ul>	<ul style="list-style-type: none"> <li>▪ Communicate with others about why a certain approach was taken and impact to the organization</li> <li>▪ Describes a thinking process that demonstrates creativity and logical thinking in developing solutions</li> <li>▪ Draws appropriate conclusions based on data obtained through multiple qualitative and quantitative data analysis techniques</li> </ul>

It is recommended that rating criteria be developed for between three and five rating categories to allow for enough distinction and variability between candidates and their responses. This distinction will be necessary to separate the best-qualified candidates from those who may be moderately or just adequately qualified. Agency assessment development experts can assist in using the defined rating criteria to develop overall structured interview scoring methodologies that will identify the most qualified candidates for the position.

Following these recommendations regarding strategic recruitment and hiring will help agency stakeholders attract and acquire qualified individuals for the Cybersecurity workforce. Once these individuals join the organization, they must be trained, managed, deployed, and perhaps developed for future leadership roles. Agency stakeholders, especially line managers and business unit leaders, are responsible for many workforce development initiatives once people have joined their organizations. The next sections of this resource guide will describe additional human capital activities that many agency stakeholders are likely to pursue.

CHIEF INFORMATION OFFICERS COUNCIL

## Employee Development

One of the most critical functions that managers perform is developing the talents of their employees. Employee development not only benefits the individual subordinates by increasing their skill levels, but it also promotes organizational productivity and flexibility. Employees that have honed a variety of skills can often work more quickly, more independently, and more effectively than employees who have not engaged in development activities. By increasing the capabilities of employees, leaders are relieved from being mired in the details of each project, and can have a strategic focus. They worry less about daily duties and concentrate more on driving the organization forward. In addition, employees that have undergone development are more likely to have broad knowledge and experience, and can fill in when needed. This flexibility means the organization will be more prepared for shifting circumstances and new initiatives. In the Cybersecurity field, with its constantly evolving priorities and threats, such flexibility is essential.

### Introduction to Employee Development

While most managers understand the critical role that development plays for increasing the capabilities of their employees, many are unsure how to make the development meaningful. This section describes several strategies to help increase the buy-in for and utility of developmental actions. The workforce development matrices provide information on the skills and competencies that Cybersecurity professionals need to succeed. Further, the matrices list training and development resources to help managers and employees select opportunities to develop those skills and competencies. As agency stakeholders identify potential opportunities for their employees to develop their skills, they should remember three key elements of successful development: Relevance, Acceptance, and Transfer.

**Relevance:** Most people can identify with the experience of attending training classes that have little or nothing to do with their careers. In fact, one of the most common complaints of employees is being forced to attend irrelevant seminars that only succeed in wasting their time. Therefore, for developmental experiences to be useful, they must be tied directly to the job duties that employees are performing or expected to perform in the near future.

**Acceptance:** One of the most important elements of successful employee development is the willingness of the individual employees to actively participate in and learn from the experience. People who are not interested in developing their skills are less likely to derive meaningful learning from training or developmental experiences. Even if they do learn new things, they are less likely to transfer that knowledge to their daily duties. Therefore, it is important to work with employees to get their buy-in for any suggested developmental actions.

**Transfer:** Organizations and managers invest resources to develop employees because they expect the employees to apply the developmental outcomes to their job duties and increase performance. One of the most challenging elements of training and development programs, however, is “transfer of training.” Transfer of training refers to the extent to which developmental learning outcomes are applied to the job. If employees fail to make the transfer, then performance will not change, regardless of the amount of learning.

CHIEF INFORMATION OFFICERS COUNCIL

## Using the Matrices to Inform Employee Development

To help promote relevance, acceptance, and transfer, an essential best practice is for agency stakeholders to collaborate with employees to identify and select training and developmental experiences together. The following steps are helpful guides for using the workforce development matrices to collaborate with employees to promote development:

- Step 1 – Understand Training/Development Needs
- Step 2 – Identify Training/Development Options
- Step 3 – Set Goals for Training/Development
- Step 4 – Follow Up on Goals

**Step 1 - Understand Training/Development Needs:** The only way to ensure relevance of training is to understand what the current training and development needs are. Analyzing the training needs is a matter of comparing the current skill levels possessed by employees to the required skill levels necessary for successful completion of their duties. For Cybersecurity professionals working in an evolving environment, there is almost always a skills gap. The software, hardware, and policies related to Cybersecurity change so rapidly that it is difficult for anyone to stay completely current. The primary challenge for agency stakeholders, then, is identifying the most critical skills gaps that present the greatest risks.

The workforce development matrices provide information on skills and duties of people in Cybersecurity roles. The matrices also present different levels of complexity associated with varying levels of seniority within the roles, and list the competencies and skills needed to succeed. This information is a good place to start to analyze talent gaps. In addition to the matrices, managers can use other resources, such as employee performance plans and IDPs, to identify training and development needs. These needs are often part of the performance management process, so managers can leverage the effort they have already taken in writing assessments to use this information for identifying development actions.

Finally, another critical source of information is the employees themselves. A best practice would be for managers to share the matrices with employees, review the descriptions of the employees' roles together, discuss current challenges, and use this conversation to highlight possible training and development needs. By having this direct conversation with employees and using the matrices as a foundation, managers are likely to identify training and development needs that are both pertinent to the job and relevant to the employee. Because employees will have played a part in selecting the training needs, they are more likely to accept the suggestions of the supervisor and feel engaged in the developmental actions.

**Step 2 - Identify Training/Development Options:** Once managers have worked with employees to select training and development needs, the next step is to identify ways to meet those needs by filling skill gaps. There are many types of training and development opportunities that employees can take, so it is important that agency stakeholders promote appropriate options to meet critical needs. Some gaps can be filled with self-paced learning, some with on-the-job experience, and others require more formal instruction that results in certificates or degrees. The workforce development matrices were designed to

## CHIEF INFORMATION OFFICERS COUNCIL

include certifications, educational backgrounds, and other developmental activities that would benefit employees in each role. While not exhaustive, the information in the matrices was provided by subject matter experts in the field that have identified these experiences and learning resources as good indicators of relevant knowledge and skill. Therefore, supervisors and employees can begin by reviewing this section of the matrix to identify training and learning options that may be helpful.

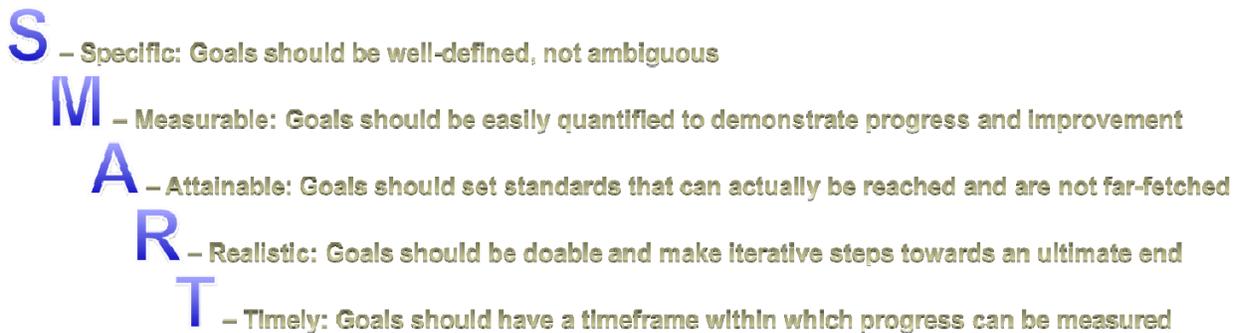
Given the time and expense of many formal learning programs, and given the nature of some needs that require more on-the-job experience, agency stakeholders may need to be more creative in identifying developmental experiences. For example, it may be appropriate for employees to engage in temporary details in other units of the organization, or to do job shadowing or mentoring. These types of efforts not only keep employees on the job, but they are also low-cost ways of broadening employee skill sets that foster greater understanding of how all the different units of an organization work together to support the mission.

Regardless of which training and development activities are selected, agency stakeholders should try to include employees in the process. This will increase employee acceptance and engagement, and is likely to promote measurable improvements in job performance.

**Step 3 - Set Goals for Training/Development:** One thing many managers neglect to do is set goals with their employees regarding the expected outcomes of the training. Often times, managers are concerned that employees will not want to participate in training, so they do not want to create additional burden by establishing expectations for employee performance once the training is complete. Recently, however, leading-edge organizations are finding that managers who set goals with their employees before training, and follow up with them afterward, actually increase the commitment of those employees to actively learn and apply their new skills. By investing in training, the organization and the manager have invested in the employees. By setting goals and following through with them, employees return the investment.

Agency stakeholders should work with employees to prepare for training and development by setting goals for what types of skills to hone, what knowledge to learn, and how to apply this learning to the job. The goals do not have to be extensive. In fact, the most effective goals are often quite simple. However, they should be established, documented, and reviewed after the training. To make goals effective, best practices recommends that people use the SMART method (*Figure 12*):

CHIEF INFORMATION OFFICERS COUNCIL

**Figure 12. SMART Goals**

**Step 4 - Follow Up on Training/Development Goals:** Once employees have completed training and development actions, appropriate agency stakeholders (e.g., managers, training directors) should meet with them to review their progress toward the goals set before training began. Provided the goals were set using the SMART criteria, there should be an easily identifiable timeframe in which to review the goals, and the goals should be tied to quantitative outcomes that can demonstrate progress.

Just as managers can use performance assessments and IDPs to identify and track training and development actions, the workforce development matrices and associated employee development actions can also be used to inform the performance management tools. As managers are approaching performance reviews, they should consider using the matrices to identify the skills, competencies, and developmental resources that are commonly associated with people in these roles. The matrices can be used as an objective source of standards to inform developmental components of performance reviews.

While employee development focuses on building the skills and competencies of individuals, the next section on workforce planning describes how to develop an entire workforce.

## Succession Planning

Succession planning is a process whereby organizations prepare to fill critical leadership positions. Often, these leadership positions become available through retirement or other turnover actions, but they can also result from organizational restructuring or expansion, during which new leadership positions are created. Regardless of how leadership positions become available, it is important for organizations to fill them quickly with qualified candidates that are well-prepared for success.

The Cybersecurity fields are expanding, and federal agencies will continue to recruit and hire more people in these occupations. This expanding workforce will create increased demand for qualified leaders that are equipped to manage, develop, and deploy these new workers. Leadership and management skills will therefore become increasingly important to Cybersecurity roles. Succession planning enables organizations to develop the leadership and management competencies of their employees and prepare them to assume and execute leadership responsibility.

## CHIEF INFORMATION OFFICERS COUNCIL

In addition to being an important initiative in its own right, succession planning also supports other workforce development efforts. By assessing current leadership talent to identify potential gaps, succession planning informs performance management, the creation of IDPs, and recommended training and development activities. Results of a succession planning initiative can inform strategic visioning by highlighting projections of future risks and needs. This can also inform budgetary decisions about funds needed to hire/promote and train new managers. Succession initiatives are often connected to knowledge management processes to ensure that critical technical and institutional knowledge is captured and transferred before people retire. Most importantly, however, succession planning reduces risk by developing a pipeline of employees that are preparing for leadership roles. Then, when vacancies occur, these employees are ready with the managerial skills and institutional knowledge needed to seamlessly continue the work of their organizations.

### Succession Planning in the Federal Government

The Federal Government, along with many organizations in the private sector, has greatly increased its focus on succession planning in recent years. In December 2009, OPM amended the Federal Workforce Flexibility Act of 2004 (Pub. L. 108-411) in an effort to improve the management and leadership skills of supervisors and employees in the public sector. The revised law includes language that mandates all federal agencies to develop succession plans.

There are, however, some unique challenges for implementing succession initiatives in the federal sector. Regulations about personnel decisions in the Federal Government require succession initiatives to be unique from those in private companies. Succession planning in the Federal Government therefore involves specific design considerations to comply with merit-based principles.

**Compliance with Merit-Based Principles:** Federal Government personnel decisions are based on merit principles. Some managers fear that implementing succession plans violates these principles by “pre-selecting” some individuals for leadership positions. However, this is not the case. Best practices for succession planning focus on preparing staff for higher leadership responsibility, not for particular positions. Further, succession planning helps employees improve their skills so that they may be more competitive for available positions in the future. Succession planning does not guarantee employees promotions, pay raises, or any other benefits; it simply enables employees to build additional skills and improve proficiencies so that they will be more attractive candidates during fair and open job competitions.

**Fair and Open Competition:** Positions in the Federal Government are filled after sponsoring agencies host fair and open competitions. Succession planning participants that seek promotion must apply for available positions during the open application period, and must compete for these positions like all other applicants. Succession planning does not guarantee participants a promotion or specific jobs. Rather, it prepares employees for open competitions by providing opportunities for them to increase their proficiencies with leadership and management skills. If these competencies are enhanced in current staff, there will be a better chance that internal candidates will be qualified to fill leadership positions as they become vacant. Nominating employees as “heirs-apparent” to certain positions is a

CHIEF INFORMATION OFFICERS COUNCIL

form of pre-selection, which is not permitted in the government. All selections to available positions must be made after a fair and open competition of potential candidates.

**Building Pools of Succession Candidates**

To avoid issues of pre-selection and to comply with federal regulations, there are two models that most federal agencies use to build pools of succession participants. Given the unique structure and broad mission of some federal agencies, using a combination of these two models may also provide an effective way of implementing succession planning across the agency while still customizing the process to each unit’s needs (Figure 13).

**Figure 13: Models for Developing Succession Participant Pools**

	DESCRIPTION	BENEFITS	POTENTIAL DRAWBACKS
<b>COMPETITIVE SELECTION MODEL</b>	<ul style="list-style-type: none"> <li>▶ A fair and open competition (similar to a job search) is conducted to choose a select cohort of participants in the succession process.</li> <li>▶ The selection process is advertised and open to all interested parties, and decisions are made based on pre-determined, objective criteria.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Focuses resources on a small group of highly-motivated employees</li> <li>▶ Employees must actively demonstrate an aspiration for leadership by making an effort to apply for participation in the program</li> <li>▶ Participation in the process can become coveted, and a motivator in and of itself</li> </ul>	<ul style="list-style-type: none"> <li>▶ Effort required from agency leadership to establish criteria, advertise process, review applications, and make selections</li> <li>▶ May cause frustration among those that are not selected</li> <li>▶ May create perceptions of pre-selection, unfairness, or inequity</li> </ul>
<b>GRADE-LEVEL CUT-OFF OR JOB SERIES INCLUSIVE MODEL</b>	<ul style="list-style-type: none"> <li>▶ All employees at or above a certain pay grade, or that fall within certain job categories, are automatically included in the succession process. Employees that do not aspire to leadership roles may choose to opt out of participating.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Requires little effort from senior leadership, with no need for establishing criteria, advertising selection process, or reviewing applications</li> <li>▶ Avoids concerns about pre-selection, unfairness, or inequity by including all employees in certain categories</li> </ul>	<ul style="list-style-type: none"> <li>▶ More resources are needed for a larger participant pool, which may include disinterested employees</li> <li>▶ Does not capture employee aspiration for leadership because little effort is required to enter the participant pool</li> <li>▶ Participation in the process is not unique and may not be coveted or motivational</li> </ul>
<b>HYBRID MODEL</b>	<ul style="list-style-type: none"> <li>▶ A combination of the selection model and the inclusive model is used to suit different parts of the organization.</li> <li>▶ A fair and open competition is conducted for certain groups of employees, and other groups are automatically included in the process.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Allows customization for each unit, job category, etc.</li> <li>▶ All stated in (I) and (II) for areas in which these models are implemented</li> </ul>	<ul style="list-style-type: none"> <li>▶ Effort required from leadership to select which model to apply to each section of the agency</li> <li>▶ All stated in (I) and (II) for areas in which these models are implemented</li> </ul>

**Competitive Selection Model:** Many agencies use a competitive selection model to build a pool of succession participants. This model mirrors the job search process in many ways: criteria are established for selection, these criteria are made measurable and applied equally across all applicants, the application process is advertised and open to all interested parties, applications are received and reviewed according to the pre-set criteria, and participants are selected. The competitive model allows agencies to select a small group of highly motivated employees that express interest in assuming leadership responsibilities, aspire to develop their skills, and demonstrate the capability to succeed in learning additional skills. By selecting this small group for further development, the competitive model allows the organization to focus its resources on employees that are likely to maximize the benefits of the training and development investment.

## CHIEF INFORMATION OFFICERS COUNCIL

However, the competitive model requires significant effort from agency stakeholders to establish the criteria, advertise the process, review the applications, and make selections. Due to the nature of a competitive model that usually involves some employees not being selected for immediate participation, it can sometimes generate frustration among those employees that do not get chosen. Finally, if the process is not made transparent and/or communicated effectively across the organization, there may be a perception of unfairness or inequity. Most of these drawbacks can be mitigated with careful, clear communication about the process.

**Grade-Level Cut-Off / Job-Series Inclusive Model:** Another model that federal agencies use is a grade-level / job-series cut-off model. This model is more inclusive, and rather than hosting an open competition, involves selecting a pay grade or job series, and automatically including all employees that fall into the selected categories. For example, an agency may choose to include all employees at the GS-14 pay grade and above, or may choose to include all employees in occupational series 2210. This inclusive model allows organizations to more easily avoid perceptions of unfairness or inequity by including everybody in certain categories. This model requires less effort from agency stakeholders because they only select the categories of employees to include, and do not need to develop, advertise, and carry out a competitive selection process. Finally, the inclusive model builds large cohorts of succession participants, and provides many employees in the agency opportunities for further development.

The inclusive model has several disadvantages. It does not completely avoid perceptions of unfairness, for employees may question why certain categories and not others were chosen to be included in the process. In addition, developing a large group of participants represents a significant commitment of resources, and organizations must be prepared to provide training, development, mentoring, and other leadership development opportunities to a large group of employees. This expenditure may result in using resources less efficiently, especially since this model includes employees that may not have any interest or aspiration for leadership roles. Therefore, the organization may spend resources on employees that will choose not to benefit from the additional training and development. Finally, the inclusive model may create frustration later in the process when more employees have undergone training and development and there are only a few available leadership positions. Although all succession processes should clearly communicate that there are no guarantees of promotion or advancement, employees often expect some outcome after completing the process, and this model includes many more employees who may have some expectations.

**The Hybrid Model:** A hybrid model is simply a combination of the competitive and inclusive models described above, and indicates that different segments of the organization use different models depending on their needs and staffing structures. All of the advantages and disadvantages remain the same, but the hybrid model allows agency stakeholders to determine which model fits each unit most appropriately, and then customize the succession process for that unit.

### Using the Matrices to Engage in Succession Planning

Succession planning can, in many ways, be an extension of the activities that agency stakeholders already perform. Therefore, it does not have to involve large investments of time or money. To help

## CHIEF INFORMATION OFFICERS COUNCIL

Cybersecurity managers, the workforce development matrices are useful tools for informing succession planning.

There are five basic steps to succession planning:

- Step 1. Identify leadership talent needs
- Step 2. Evaluate onboard leadership talent
- Step 3. Identify gaps
- Step 4. Define and implement strategies to fill gaps
- Step 5. Follow up on mitigation strategies

**Step 1 – Identify Leadership Talent Needs:** Managers can use the matrices to identify the skills and competencies that are associated with leadership and management. For example, many of the matrices include references to communications skills, ability to translate technical information into lay terms for reports to agency stakeholders, and understanding budgetary implications of security needs. These managerial skills can help managers understand what skills are needed to manage Cybersecurity professionals. Additional key activities are suggested below:

*Key Activities:*

- Use matrices to identify leadership competencies
- Use workforce plans to understand number of potential leadership vacancies
- Review organizational strategy to determine if leadership ranks will be expanding
- Interview current employees and managers to ask them what is needed with regard to leadership and management
- Integrate this information to document both current and future leadership needs

**Step 2 – Evaluate Onboard Leadership Talent:** During Step 2, organizations should use the leadership needs identified in Step 1 to pinpoint the critical leadership skills and competencies that are needed. Once these are identified, organizations can assess current employees on these skills to understand onboard leadership talent. It is important to clarify that the assessment is purely for developmental purposes and not intended to be connected to performance appraisals, current job openings, or other specific outcomes. Rather, the assessment provides a baseline for the organization to identify current talents and to compare this with project needs to highlight any gaps.

*Key Activities:*

- Identify specific leadership skills and competencies needed now and in the future
- Conduct a leadership skills inventory based on the specific skills to understand current talent levels

**Step 3 – Identify Gaps:** During Step 3, organizations can compare the results of the leadership skills assessment in Step 2 to the projected needs in Step 1. This activity produces an understanding of any gaps and identifies areas for training, development, or possibly recruitment.

*Key Activities:*

- Compare results of leadership skills assessment with projected leadership needs

## CHIEF INFORMATION OFFICERS COUNCIL

- Identify leadership skill gaps

**Step 4 – Define and Implement Strategies to Fill Gaps:** Using the results of the gap analysis, agency stakeholders can then develop strategies to fill these gaps. Some gaps may be filled through traditional classroom training exercises while others may require more intense leadership coaching and mentorship. Given the nature of the Cybersecurity work, some gaps may be more technical in nature and can be filled with temporary details, on-the-job learning, or job rotations.

*Key Activities:*

- Analyze and summarize results of leadership gap analysis
- Develop strategies to fill any identified gaps

**Step 5 – Follow Up on Mitigation Strategies:** A critical element of succession planning is periodic review of progress. Therefore, agency stakeholders should follow up on the mitigation strategies they implement. They can meet with emerging leaders to learn how their training and developmental activities are proceeding. Stakeholders can also periodically repeat the leadership skills assessment to document progress and identify areas that still need attention. Finally, by following up on mitigation strategies, succession planning becomes a part of agency stakeholders' regular duties and not a one-time effort.

*Key Activities:*

- Review progress on mitigation strategies
- Repeat leadership skills assessment
- Document progress and highlight areas that have not shown improvement
- Revise mitigation strategies as needed
- Build succession planning into regular managerial duties

## Conclusion

The workforce development matrices can help agency stakeholders and employees collaborate to identify the individual and organizational human capital needs, and the resources needed to meet them. By engaging in workforce initiatives such as recruitment, selection, employee development, workforce planning, and succession planning, agency stakeholders can ensure that they will have the people with the skills and resources needed to continue supporting their agency's missions now and in the future.

## Appendix

### Workforce Development Matrices

Criteria included in the matrices are provided as guidance only. These criteria are not a replacement for OPM basic qualifications as outlined in the relevant occupational qualification standards. The intention of the qualifications matrix is to assist departments/agencies in defining the qualifications criteria that are most relevant and applicable to their IT Security workforce. No singular qualification component on its own (i.e., education) should be the sole determinant in classifying an individual's proficiency level. Rather, all aspects of experience, competencies, education, and training/certifications should be considered when making performance level evaluations.

The role descriptions provided are specific to the Cybersecurity function and environment.

**SYSTEMS OPERATIONS & MAINTENANCE PROFESSIONAL:** The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.

Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
<b>I: Entry</b>	<p>Has a basic understanding of computer systems and related Cybersecurity software and hardware components</p> <p>Ability to perform basic security system administration duties including software and hardware installation, troubleshooting, system backup, network component maintenance</p> <p>Basic understanding of tools and methods for identifying anomalies in system behavior; develops ability to recognize anomalies</p> <p>Applies skills and abilities with supervision on projects, programs, and initiatives with low threat and scope (e.g., inter-office)</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below.</p> <p><b>Competency/Skill Proficiency Descriptors</b></p> <p>I-Entry: Basic understanding of concepts addressed in relevant competency/skill models</p> <p>II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities</p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p><b>Relevant Competency/Skills Sources:</b></p> <ul style="list-style-type: none"> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>▶ DHS EBK Competencies</li> </ul>	<ul style="list-style-type: none"> <li>▶ Bachelors Degree (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management); OR 0-3 years experience involving work directly related to systems operations and maintenance (e.g., help desk)</li> <li>▶ Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE)</li> </ul>	<ol style="list-style-type: none"> <li>1. Development Resources: <ul style="list-style-type: none"> <li>▶ Graduate Programs, USDA IT Programs</li> <li>▶ GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>▶ CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>▶ DoD DISA Training</li> <li>▶ GSA's CIO university Program</li> </ul> </li> <li>2. University Cybersecurity Programs: <ul style="list-style-type: none"> <li>▶ National Defense University- IRM College</li> <li>▶ IS/IA Degree Programs- CAEIAE</li> <li>▶ Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>3. OPM Development Center: The Federal Executive Institute and the Management Development Centers</li> <li>4. Participation in coaching/mentoring/job shadowing programs</li> <li>5. Agency Requirements: organization and business area training identified as required</li> <li>6. Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate</li> <li>7. Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012)</li> <li>8. Training by external vendors for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)</li> </ol>
<b>II: Intermediate</b>	<p>Applies an understanding of the Cybersecurity operational characteristics of a variety of computer platforms, networks, software applications, and operating systems</p> <p>Ability to explain to others the methods and techniques used in installation, testing, network debugging, troubleshooting, and maintenance of PCs, servers, printers, and related equipment</p> <p>Automates repetitive processes (e.g., log reviews, configuration testing) to facilitate Cybersecurity operations</p> <p>Evaluates and assesses operating practices to determine adequate risk management and compliance standards, with on-going systems monitoring</p> <p>Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (e.g., sub-organization wide)</p>	<ul style="list-style-type: none"> <li>▶ FISMA Guidance</li> <li>▶ NIST SP 800-16, Revision 1</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ DoD Directive 8570</li> <li>▶ CNSS Policies, Directives, and Reports</li> </ul>	<ul style="list-style-type: none"> <li>▶ Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> <li>▶ Core: MCSE, CCNA, CCNP, ISC<sup>2</sup> CAP</li> <li>▶ Related: CISSP, CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC, PMP</li> </ul> </li> </ul>	
<b>III: Advanced</b>	<p>Effectively communicates technical information to non-technical audiences; influences others to comply with policies and conform to standards and best practices</p> <p>Designs the organization's working Cybersecurity systems operations and maintenance strategy and methodology to comply with the organization's standards and mission</p> <p>Understands the needs of the organization and establishes appropriate vendor relationships to manage the proposal and purchasing process</p> <p>Attends and participates in professional conferences to stay abreast of new trends and innovations in the field of information systems</p> <p>Independently manages, plans, evaluates, and advocates for Cybersecurity compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (e.g., agency-wide or inter-governmental), with on-going systems monitoring</p>		<ul style="list-style-type: none"> <li>▶ Bachelors Degree and 3+ years experience (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>▶ Demonstrated experience in managing/supervising a systems operations and maintenance group</li> <li>▶ Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> <li>▶ Core: MCSE, CCNA, CCNP, ISC<sup>2</sup> CAP</li> <li>▶ Related: CISSP, CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC, PMP</li> </ul> </li> </ul>	

**INFORMATION SECURITY ASSESSOR:** The Information Security Assessor is responsible for overseeing, participating in evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Information Security Assessor provides guidance and autonomous evaluation of the organization to management.

Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
<b>I: Entry</b>	<p>Has a basic understanding of Cybersecurity compliance with regard to the FISMA Act and its requirements, applicable laws and regulations (e.g., OMB directives, HSPD, HIPAA, Clinger-Cohen), organizational policies, and the Cybersecurity compliance evaluation process (i.e., initial risk assessment, mitigation recommendations, controls, and applicable security compliance)</p> <p>Applies compliance knowledge, skills, and abilities with supervision on projects, programs, and initiatives with low threat and scope (i.e., inter-office)</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below.</p> <p><b>Competency/Skill Proficiency Descriptors</b></p> <p>I-Entry: Basic understanding of concepts addressed in relevant competency/skill models</p> <p>II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities</p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p><b>Relevant Competency/Skill Sources:</b></p> <ul style="list-style-type: none"> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas</li> </ul>	<ul style="list-style-type: none"> <li>▶ 0-3 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>▶ Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE)</li> </ul>	<ol style="list-style-type: none"> <li>1. Development Resources: <ul style="list-style-type: none"> <li>▶ Graduate Programs, USDA IT Programs</li> <li>▶ GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>▶ CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>▶ DoD DISA Training</li> <li>▶ GSA's CIO university Program</li> </ul> </li> <li>2. University Cybersecurity Programs: <ul style="list-style-type: none"> <li>▶ National Defense University- IRM College</li> <li>▶ IS/IA Degree Programs- CAEIAE</li> <li>▶ Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>3. OPM Development Center: The Federal Executive Institute and the Management Development Centers</li> <li>4. NIST SP 800-16: Key role-based Cybersecurity body of knowledge topics and concepts including awareness, training, and education</li> <li>5. DHS IT Security Essential Body of Knowledge: Cybersecurity key terms/concepts, functional perspectives, and role-based competencies</li> <li>6. Participation in coaching/mentoring/job shadowing programs</li> <li>7. Agency Requirements: organization and business area training identified as required</li> </ol>
<b>II: Intermediate</b>	<p>Applies an understanding of Cybersecurity compliance when reviewing systems and security documentation, explaining risks to system owners, implementing risk mitigation controls, and enforcing Cybersecurity policies</p> <p>Reviews security document artifacts and determines organizational compliance with Cybersecurity laws and organizational policies</p> <p>Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (i.e., sub-organization wide)</p>	<ul style="list-style-type: none"> <li>▶ DHS EBK Competencies</li> <li>▶ NIST SP 800-37 C&amp;A Process</li> <li>▶ NIST SP 800-53 Control Set and SP 800-53A Control Assessment</li> <li>▶ FISMA Guidance</li> <li>▶ NIST SP 800-16, Revision 1</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ DoD Directive 8570</li> <li>▶ CNSS Policies, Directives, and Reports</li> <li>▶ OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> </ul>	<ul style="list-style-type: none"> <li>▶ Bachelors Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>▶ Possession and demonstrated application of CISA or CISSP certifications</li> </ul>	<ol style="list-style-type: none"> <li>8. Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate</li> <li>9. Certifications: agency credentialing may include other criteria (e.g., DoD 8570-01-M), continuing education, or professional society, industry, or vendor certifications <ul style="list-style-type: none"> <li>▶ Core: ISC<sup>2</sup> CAP (I); CISA, CISSP (II/III)</li> <li>▶ Related: ISACA CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC</li> </ul> </li> <li>10. Current and Emerging Legislation (e.g., FISMA, NIST SP-800 series, National Cybersecurity Initiative, FIPS, OMB directives, CNSSI No. 4012 )</li> </ol>
<b>III: Advanced</b>	<p>Designs the organization's working compliance program and creates associated Cybersecurity policies and programs</p> <p>Sets expectations, determines appropriate compliance measures to be used across the department/agency, and maintains governance over the standards and methodologies for compliance reviews</p> <p>Independently manages, plans, evaluates, and advocates for Cybersecurity compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (i.e., agency-wide or inter-governmental)</p>	<p>Designs the organization's working compliance program and creates associated Cybersecurity policies and programs</p> <p>Sets expectations, determines appropriate compliance measures to be used across the department/agency, and maintains governance over the standards and methodologies for compliance reviews</p> <p>Independently manages, plans, evaluates, and advocates for Cybersecurity compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (i.e., agency-wide or inter-governmental)</p>	<ul style="list-style-type: none"> <li>▶ Graduate Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>▶ Demonstrated experience in managing/supervising an Cybersecurity /IA compliance group</li> <li>▶ Possession and demonstrated application CISA and CISSP certifications</li> </ul>	<ol style="list-style-type: none"> <li>8. Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate</li> <li>9. Certifications: agency credentialing may include other criteria (e.g., DoD 8570-01-M), continuing education, or professional society, industry, or vendor certifications <ul style="list-style-type: none"> <li>▶ Core: ISC<sup>2</sup> CAP (I); CISA, CISSP (II/III)</li> <li>▶ Related: ISACA CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC</li> </ul> </li> <li>10. Current and Emerging Legislation (e.g., FISMA, NIST SP-800 series, National Cybersecurity Initiative, FIPS, OMB directives, CNSSI No. 4012 )</li> </ol>

**CHIEF INFORMATION SECURITY OFFICER:** The Chief Information Security Officer (CISO) is responsible for the Cybersecurity strategy within an organization. The CISO establishes, implements, and monitors the development and subsequent enforcement of the organization's Cybersecurity program (i.e., policies, procedures, security architecture standards, security awareness and training program, IT contingency plans, IT security compliance issues). The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements, while understanding security threats and vulnerabilities to operations and the organization's environment. The CISO is responsible for Cybersecurity risk management (e.g., determines risk impact, establishes risk mitigation plans and programs, works with business owners to devise processes for risk assessment) within the organization. The CISO manages the incidents response program (e.g., identifies, reports, and remediates incidents).

Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
<p><b>III: Advanced</b></p>	<p>Demonstrates an in depth understanding of enterprise-wide, multi-platform operating systems security, network security, application security, database security, regulatory compliance, incident and risk management</p> <p>Identifies, understands, manages, and interprets Cybersecurity risks and threats as it affects the business and aligns the Cybersecurity strategy to achieve organizational mission</p> <p>Designs the organization's Cybersecurity governance framework to facilitate the implementation of the organization's Cybersecurity strategy</p> <p>Sets expectations, determines appropriate security measures to be used across the department/agency, and maintains governance over the standards and methodologies for Cybersecurity risk management and compliance reviews</p> <p>Independently manages, plans, evaluates, and advocates for Cybersecurity solutions, plans, and functions, and is responsible for the management of complex projects, program, and initiatives with high threat and large scope (e.g., organization-wide or inter-governmental)</p> <p>Leads, enables, and is accountable for the implementation and integration of solutions to ensure Cybersecurity within the organization</p> <p>Understands mechanisms for securing new technologies; understands the impact of new and emerging technologies on the Cybersecurity environment, as well as tools and methods for mitigating risks</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below</p> <p><b>Competency/Skill Proficiency Descriptors</b></p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p><b>Relevant Competency/Skill Sources:</b></p> <ul style="list-style-type: none"> <li>▶ NIST SP 800-100 Information Security Handbook: A Guide for Managers</li> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas</li> <li>▶ DHS EBK Competencies</li> <li>▶ FISMA Guidance</li> <li>▶ NIST SP 800-16, Revision 1</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ DoD Directive 8570</li> <li>▶ CNSS Policies, Directives, and Reports</li> <li>▶ OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> <li>▶ Additional Key Competencies identified for this role (for senior management positions):                             <ul style="list-style-type: none"> <li>• Leadership &amp; People Management</li> <li>• Written &amp; Oral Communication</li> <li>• Creative Problem Solving</li> <li>• Budget Formation &amp; Allocation</li> <li>• Project/Program Management</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▶ Graduate Degree and 5+ years experience (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 8+ years of experience involving work with transferable skills related to Cybersecurity, incident and risk management</li> <li>▶ Demonstrated experience in leading an Cybersecurity /IA compliance group</li> <li>▶ Possession and demonstrated application of relevant certifications                             <ul style="list-style-type: none"> <li>▶ Core: CISSP, CISM, GISA, GSLC</li> <li>▶ Related: ISSMP, CIW-Security, CAP, COMPTIA</li> </ul> </li> <li>▶ Security clearance commensurate with organizational requirements</li> </ul>	<ol style="list-style-type: none"> <li>1. University Cybersecurity Programs:                             <ul style="list-style-type: none"> <li>▶ National Defense University- IRM College</li> <li>▶ IS/IA Degree Programs- CAEIAE</li> <li>▶ Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>2. OPM Development Center: The Federal Executive Institute and the Management Development Centers</li> <li>3. Attendance at industry conferences, work groups, and briefings (i.e., DHS- GFirst; FIA; Black Hat; RSA; ISACA; SANS FIRE; CAISSWG; AFCEA)</li> <li>4. Development Resources:                             <ul style="list-style-type: none"> <li>▶ Graduate Programs, USDA IT Programs</li> <li>▶ GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>▶ CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>▶ DoD DISA Training</li> <li>▶ AFCEA (<a href="http://www.afcea.org">www.afcea.org</a>)</li> <li>▶ CAISSWG</li> <li>▶ GSA's CIO University Program</li> </ul> </li> <li>5. Participation in coaching/mentoring/job shadowing programs</li> <li>6. Agency Requirements: organization and business area training identified as required</li> <li>7. Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4011 &amp; 4012)</li> <li>8. Training by external vendors (e.g., Sans Institute , ISC<sup>2</sup>, ISACA, MIS)</li> </ol>

**INFORMATION SECURITY SYSTEMS & SOFTWARE DEVELOPMENT PROFESSIONAL:** The Information Security Systems and Software Development Professional is responsible for secure design, development, testing, integration, implementation, sustainment, and/or documentation of software applications (web based and non-web) following formal secure systems development lifecycle processes and using security engineering principles.

Perf. Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
I: Entry	<p>Basic understanding of computer systems and related Cybersecurity software and hardware components, network systems and databases, and information systems security safeguards</p> <p>Capable of articulating software/system abuse and misuse cases; understands practices and tools for mitigating exploitable software weaknesses</p> <p>Writes code in different programming languages (e.g., Java, C, C++)</p> <p>Integrates off-the-shelf products with information assurance safeguards (e.g., implementing network firewalls and routers)</p> <p>Participates in small teams performing software development and Cybersecurity software-oriented tasks</p>	<p><b>Recommended Competencies and applicable performance levels</b> (Entry, Intermediate, Advanced):</p> <ul style="list-style-type: none"> <li>▶ Software Development (E, I, A)</li> <li>▶ Written &amp; Oral Communication (E, I, A)</li> <li>▶ Creative Problem Solving (E, I, A)</li> <li>▶ Cybersecurity /Information Assurance (E, I, A)</li> <li>▶ Critical Thinking and Analytical Skills (E, I, A)</li> <li>▶ Software Engineering (I, A)</li> <li>▶ Project/Program Management (I, A)</li> <li>▶ Leadership &amp; People Management (I, A)</li> </ul>	<ul style="list-style-type: none"> <li>▶ <b>Relevant work experience</b> refers to work directly related to secure network design, database design and security, and secure coding and testing techniques</li> <li>▶ <b>Computer Science-related fields</b> include computer science/engineering, database/information management, information assurance/security, software assurance/security, information systems management</li> <li>▶ Associates Degree from an accredited program in a Computer Science-related field;</li> </ul> <p style="text-align: center;"><b>OR</b></p> <ul style="list-style-type: none"> <li>▶ 1 year of relevant work experience</li> </ul>	<ol style="list-style-type: none"> <li>1. University Programs (e.g., UMD, GMU, Stevens Institute of Technology, Carnegie-Mellon, UMUC, UMBC)</li> <li>2. Relevant Course Topics (e.g., IT Software Development, Project / Risk Management)</li> <li>3. Formal Training Programs (e.g., Shon Harris Ethical Hacking, SANS Institute)</li> <li>4. Government agency courses (e.g., IRM-NDU virtual university, USDA-graduate school, NSA certifications)</li> <li>5. Government courses on related topics (e.g., Project Management, Government Technical Representation, COTR)</li> <li>6. Participation in agency coaching/mentoring/job shadowing programs</li> <li>7. Training by external vendors for software development (e.g., Microsoft, Cisco Systems)</li> <li>8. Federal internship programs (e.g., Cyber Corps, and CAEIA)</li> </ol>
II: Intermediate	<p>Advanced understanding of information systems security, ethical hacking, multiple network analysis, configuration management, integration and deployment issues</p> <p>Designs secure software systems from requirements within the software development lifecycle; derives additional security requirements based on the deployment environment</p> <p>Communicates technical information to non-technical audiences and advises staff on Cybersecurity issues and approaches</p> <p>Applies knowledge of Cybersecurity aspects (e.g., coding, operating systems, programming languages, databases, federal and agency policies and procedures)</p> <p>Performs static and dynamic analysis to identify vulnerabilities in applications, across databases, networks, network-based environments, and operating systems, and directs remediation as appropriate</p> <p>Creates protocols, procedures, and guidelines to mitigate security risks</p>	<p><b>Relevant Sources</b> (as determined by the department/agency):</p> <ul style="list-style-type: none"> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on Technical, Desktop Technology Tools, and IT Security/Information Assurance competency areas</li> <li>▶ Essential Bodies of Knowledge (EBK) for IT Security Professionals (e.g., DHS and DOE)</li> <li>▶ NIST Special Publications (e.g., NIST SP 800-16, Revision 1, 800-37, 800-53, 800-53A)</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> <li>▶ Resources from DHS Software Assurance Community Resources and Information Clearinghouse (<a href="https://buildsecurityin.us-cert.gov/swa/">https://buildsecurityin.us-cert.gov/swa/</a>)</li> <li>▶ Software Assurance in Education, Training, and Certification Pocket Guide</li> </ul>	<ul style="list-style-type: none"> <li>▶ Bachelors Degree from an accredited program in a Computer Science-related field;</li> </ul> <p style="text-align: center;"><b>OR</b></p> <ul style="list-style-type: none"> <li>▶ 6 years relevant work experience</li> <li>▶ Possession and demonstrated application of relevant certifications (as determined by the department/agency):                             <ul style="list-style-type: none"> <li>▶ Information systems security certifications (e.g., ISC<sup>2</sup> CSSLP and CISSP, various SANS certs, EnCase Cybersecurity suite), network engineering certifications (e.g., EnCase forensics suite, CCIE, GSEC), software/systems administration/engineering certifications, software development certifications, DBMS, and relevant programming languages</li> </ul> </li> </ul>	<ol style="list-style-type: none"> <li>1. University Programs (e.g., UMD, GMU, Stevens Institute of Technology, Carnegie-Mellon, UMUC, UMBC)</li> <li>2. Relevant Course Topics (e.g., IT Software Development, Project / Risk Management)</li> <li>3. Formal Training Programs (e.g., Shon Harris Ethical Hacking, SANS Institute)</li> <li>4. Government agency courses (e.g., IRM-NDU virtual university, USDA-graduate school, NSA certifications)</li> <li>5. Government courses on related topics (e.g., Project Management, Government Technical Representation, COTR)</li> <li>6. Participation in agency coaching/mentoring/job shadowing programs</li> <li>7. Training by external vendors for software development (e.g., Microsoft, Cisco Systems)</li> <li>8. Federal internship programs (e.g., Cyber Corps, and CAEIA)</li> </ol>
III: Advanced	<p>Expert understanding of information systems security, ethical hacking, multiple network analysis, configuration management, integration and deployment issues</p> <p>Serves as senior advisor to the architectural design and development of enterprise-wide applications, systems, and services</p> <p>Serves as senior advisor to procurement and contract management in support of system and software acquisition</p> <p>Coordinates/ collaborates across organizational and dept./agency lines; influences others to comply with security policies, standards, and best practices</p> <p>Integrates policies and procedures across government agencies; participates in the update of the agency's knowledge of federal security policies, procedures, and guidelines</p>	<p><b>Relevant Sources</b> (as determined by the department/agency):</p> <ul style="list-style-type: none"> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on Technical, Desktop Technology Tools, and IT Security/Information Assurance competency areas</li> <li>▶ Essential Bodies of Knowledge (EBK) for IT Security Professionals (e.g., DHS and DOE)</li> <li>▶ NIST Special Publications (e.g., NIST SP 800-16, Revision 1, 800-37, 800-53, 800-53A)</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> <li>▶ Resources from DHS Software Assurance Community Resources and Information Clearinghouse (<a href="https://buildsecurityin.us-cert.gov/swa/">https://buildsecurityin.us-cert.gov/swa/</a>)</li> <li>▶ Software Assurance in Education, Training, and Certification Pocket Guide</li> </ul>	<ul style="list-style-type: none"> <li>▶ Masters Degree from an accredited program in a Computer Science-related field plus 5 years experience;</li> </ul> <p style="text-align: center;"><b>OR</b></p> <ul style="list-style-type: none"> <li>▶ Bachelor's degree plus 10 years relevant work experience and project management experience</li> <li>▶ Possession and demonstrated application of relevant certifications (as determined by the department/agency):                             <ul style="list-style-type: none"> <li>▶ PMP, information systems security certifications, network engineering certifications, software/systems administration/engineering certifications, software development certifications, DBMS, and relevant programming languages</li> </ul> </li> </ul>	<ol style="list-style-type: none"> <li>1. University Programs (e.g., UMD, GMU, Stevens Institute of Technology, Carnegie-Mellon, UMUC, UMBC)</li> <li>2. Relevant Course Topics (e.g., IT Software Development, Project / Risk Management)</li> <li>3. Formal Training Programs (e.g., Shon Harris Ethical Hacking, SANS Institute)</li> <li>4. Government agency courses (e.g., IRM-NDU virtual university, USDA-graduate school, NSA certifications)</li> <li>5. Government courses on related topics (e.g., Project Management, Government Technical Representation, COTR)</li> <li>6. Participation in agency coaching/mentoring/job shadowing programs</li> <li>7. Training by external vendors for software development (e.g., Microsoft, Cisco Systems)</li> <li>8. Federal internship programs (e.g., Cyber Corps, and CAEIA)</li> </ol>