Draft NISTIR 8193

National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators

Indicators for Performing Work Roles

Daniel Stein
Benjamin Scribner
Noel Kyle
William Newhouse
Clarence Williams
Baris Yakin

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8193

National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators

Indicators for Performing Work Roles

Daniel Stein
Benjamin Scribner
Noel Kyle
Cybersecurity Education and Awareness Branch
Department of Homeland Security

William Newhouse
Clarence Williams
Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology

Baris Yakin
Booz Allen Hamilton, Inc.
McLean, VA

November 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8193
98 pages (November 2017)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *November 8, 2017* through *December 8, 2017*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: cybersecurityworkforce@hq.dhs.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The national need for a common lexicon to describe and organize the cybersecurity workforce and requisite knowledge, skills, and abilities (KSAs) led to the creation of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) [1]. The NICE Framework defines the spectrum of cybersecurity work as well as tasks and knowledge, skills, and abilities (KSAs) for over 50 common Work Roles. While the Work Roles have made the NICE Framework easier to associate to specific positions, they do not provide organizations with guidance on how to determine if a cybersecurity worker can perform a Work Role. This report provides capability indicators which are intended to help organizations address this challenge. Capability indicators are recommended education, certification, training, experiential learning, and continuous learning that could signal an increased ability to perform a given Work Role. Though capability indicators are not formal qualification requirements, they provide a menu of characteristics recommended by subject matter experts (SMEs) that should be customized by each organization based on need and incorporated into hiring and employee development efforts (e.g., recruiting, building career paths). Overarching findings pertaining to capability indicators across Work Roles and proficiency levels are also provided in this report.

Keywords

Capability indicators; certification; continuous learning; education; learning; NICE Framework; qualifications; training; Workforce Framework; Work Roles; career paths; cybersecurity careers; cybersecurity jobs; cybersecurity careers

Audience

The audience for the capability indicators is primarily leadership-level executives, cybersecurity hiring managers, and human capital and human resource professionals supporting the cybersecurity workforce.

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from SMEs and organizations whose participation in focus groups and interviews and thoughtful comments improved the quality, thoroughness, and usefulness of the recommendations in this report. We also wish to thank Kristen Paasch, Christopher Rogers, and Andrea Solomon for their efforts in drafting the report and collecting data. We also thank the Health and Human Services (HHS)

Office of the Chief Information Officer (OCIO) and the Department of Defense (DOD) Chief Information Office (CIO) for their close partnership and dialogue throughout this project.

Note to Reviewers

The authors invite you to provide any input you may have to this report. There are numerous opportunities to contribute your perspective to the final publication.

For example, we welcome feedback on capability indicators (education, training, certification, and learning recommendations) for any Work Role, and especially for Work Roles that do not currently have recommendations.

The authors intend for the public comment period to serve as a form of validation for capability indicators. As such, we strongly encourage and depend on reviewer input.

Executive Summary

Numerous efforts and requirements have been enacted to quantify and strengthen the cybersecurity workforce through the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) [1]. In March 2017, the Department of Homeland Security (DHS) Cybersecurity Education and Awareness (CE&A) Branch launched an effort to collect input from Federal Government subject matter experts (SMEs) on capability indicators (e.g., education, training, learning, and credentials/certifications) for the individual Work Roles in the NICE Framework. The effort intends to provide additional understanding of the qualities or accomplishments cybersecurity workers possess that can indicate a greater likelihood of success in their role(s). Establishing capability indicators that can help organizations build formal qualification requirements for each Work Role in the latest version of the NICE Framework will aid organizations in meeting cybersecurity workforce development goals.

The need for capability indicators to build strong cybersecurity teams is evident in the recently released Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017) [2], which emphasizes that a robust workforce is critical to strengthening the long-term cybersecurity defenses and capabilities of our nation. Because capability indicators provide recommendations on qualities to look for in cybersecurity workers, they help make adoption of the NICE Framework within an organization easier. These indicators will help organizations move beyond using the NICE Framework only for inventorying their workforce to using it for recruitment (e.g., writing job descriptions), development (e.g., creating career paths), and retention efforts.

SMEs across the Federal Government received an invitation to participate in the capability indicator effort. SME input was solicited for capability indicators across three proficiency levels for each Work Role: Entry, Intermediate, and Advanced. Feedback and content from focus group sessions, phone interviews, table questionnaires, and supplemental data were aggregated, and a number of common themes across all Work Roles were identified:

- Higher education is not always necessary to enter the cybersecurity field.
- Certifications and training are relied upon for skill development and are considered indicators of ability.
- On-the-job experience is essential for higher-level proficiency.
- Risk is the most frequently recommended topic for training and certifications.
- Continuous learning is required at almost all levels.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Background

1.1 NICE Framework Overview

The NICE Framework [1], NIST Special Publication 800-181, provides a common language to define cybersecurity work, as well as Tasks and Skills required to perform that work. The NICE Framework was developed through a partnership with the National Institute of Standards and Technology (NIST), DHS, the U.S. Department of Defense (DoD), and other federal government organizations and is the culmination of many years of collaboration among industry, government, and academia.

The NICE Framework provides a fundamental reference in support of a workforce capable of meeting an organization's cybersecurity needs by using a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role.

The NICE Framework comprises seven Categories and 33 Specialty Areas, as well as Work Roles, Tasks, and Knowledge, Skills, and Abilities (KSAs):

- **Category:** A high-level grouping of common cybersecurity functions
- **Specialty Area:** Distinct areas of cybersecurity work
- **Work Role:** Specific KSAs required to perform a set of Tasks – Work Roles fall in the layer below Specialty Areas; each Specialty Area contains one or more Work Roles
- **Task:** A specific work activity that could be assigned to someone working in a position
- **KSAs:** Attributes required to perform Tasks; generally demonstrated through relevant experience or performance-based education and training

The NICE Framework provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work. By defining the cybersecurity workforce and using standard terminology, academia and employers can synchronize education, recruitment, and development to establish a robust talent pipeline and sustain a highly qualified workforce.

2 Introduction

Since the original publication of the NICE Framework, incremental improvements have been made to refine the descriptions and ease the adoption process. The inclusion of Work Roles in the NICE Framework makes it easier for organizations to align their positions to the NICE Framework. However, the NICE Framework does not provide recommendations on how organizations determine if an employee can perform in a Work Roles. To collect this information on capability indicators for NICE Framework Work Roles, the DHS Cybersecurity Education and Awareness (CE&A) Branch convened focus groups, conducted interviews, and gathered individual input and supplemental data from cybersecurity SMEs across the federal space.

2.1 Need for Capability Indicators

As previously discussed, Work Roles provide the most detailed level of information in the NICE Framework; they are more detailed than Specialty Areas and worded to more closely resemble position titles. Tasks help organizations understand the kinds of job duties that must be carried out, and KSAs describe the knowledge, skills, and abilities required to do so. However, the NICE Framework does not help determine what qualities or accomplishments indicate that someone is suitable to perform a particular job or activity. These qualities are defined in Table 1 of this report as "capability indicators" that cover education level, training, credentials/ certifications, experiential learning, and continuous learning.

For example, the NICE Framework conveys what a Security Control Assessor is expected to do (defined in Tasks) and the requisite attributes (defined in KSAs), but it does not suggest experience or recommend education, training topics, or certifications that would indicate an ability to perform the Work Role. If a manager is trying to hire someone to perform the duties of an Intermediate (mid-level) Security Control Assessor or offer his or her employees a career pathway toward becoming one, capability indicators provide expert-recommended qualification and development benchmarks.

The need for capability indicators to build strong cybersecurity teams is evident in the recently released EO 13800 (May 11, 2017). This EO places much needed emphasis on building a stronger cybersecurity workforce, recognizing that a robust workforce is critical to strengthening the long-term cybersecurity defenses and capabilities of our nation. The increasing risk of cybersecurity threats and likelihood of attacks also affect the federal cybersecurity workforce. With this increased risk comes a growing demand for qualified employees to help prevent and respond to such threats and attacks. Work Role capability indicators will allow academia and public and private sector organizations to determine the experience they need to provide so that cybersecurity talent is equipped for mission success.

Because they provide recommendations on qualities to look for in cybersecurity workers, capability indicators also help make an organization's adoption of the NICE Framework easier. For the past several years, CE&A has worked to increase awareness, understanding, and acceptance of the NICE Framework. Because of the combined efforts of CE&A, NIST, DoD, OPM, and others—as well as mandated government adoption via the Federal Cybersecurity Workforce Assessment Act of 2015—agencies have started progressing from acceptance to adoption.

The capability indicators will help organizations move beyond simply inventorying their workforce with the NICE Framework to performing other aspects of the human capital (HC) lifecycle, such as recruitment, development, and retention (Figure 1). For this report, adoption of the NICE Framework is defined as applying it to all aspects of the HC lifecycle. Equipped with language to describe the work and guidance to qualify roles and proficiency levels, organizations can begin using the NICE Framework in recruitment (e.g., writing job descriptions), development (e.g., creating career paths), and retention efforts.

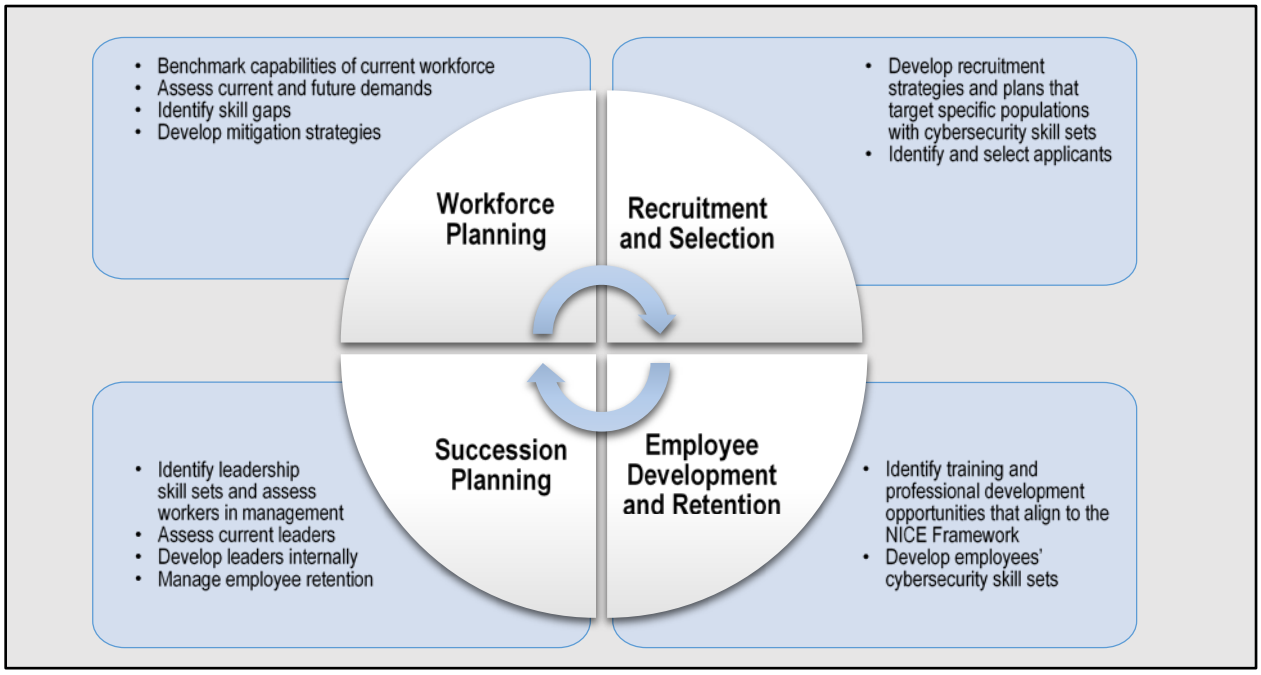

Figure 1 – Human Capital Management Lifecycle

Specifically, capability indicators aid cybersecurity workforce development in numerous ways:

- **Workforce Gaps**: As organizations evolve, so will the cybersecurity functions needed to support their workload. Organizations will need to determine the type and number of cybersecurity workers and proficiency levels they require. If organizations use the NICE Framework, Work Roles will help define the kinds of positions needed, and capability indicators will help gauge skill gaps by providing a benchmark for professional qualifications.
- **Hiring**: Talent acquisition can often heavily rely on a hiring manager's subjective preferences or gut feeling when interviewing candidates. Capability indicators help organizations pick the qualifications to look for in candidates instead. They can use the recommendations in this document as a menu from which to select and customize their own formal qualification requirements.
- **Employee Development**: Capability indicators recommend education and training topics, example certification topics, and continuous development opportunities that organizations can encourage their staff to pursue to strengthen skills and performance.

- **Career Pathways**: Capability indicators are organized by proficiency levels in each Work Role, offering a clear set of development recommendations that will help workers progress in their chosen area.

2.2 Understanding Capability Indicators

As already stated, capability indicators are qualities or accomplishments that could be used to show someone is suitable for a particular job or activity. They are the education, training, certification(s), and experiential and continuous learning that indicate a cybersecurity worker is likely able to perform a specific Work Role at a certain proficiency level. Table 1 defines the capability indicators used for this effort. SME input was solicited for capability indicators across three proficiency levels for each Work Role: Entry, Intermediate, and Advanced. Proficiency is not aligned to position level or to pay scale such as the General Schedule (GS) for government employees. For the purposes of this report, proficiency is used to indicate a degree of capability or expertise in a specific knowledge, skill, or domain that allows one to function independently in performing that knowledge or skill. Table 2 defines the proficiency levels in more detail.

Table 1 – Capability Indicator Definitions

Capability Indicator	Definition
Education	Education above the high school level completed in a U.S. college, university, or other educational institution that has been accredited by one of the accrediting agencies or associations recognized by the Secretary, U.S. Department of Education *(source: OPM)*
Training	The process of providing for and making available to an employee, and placing or enrolling the employee in, a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in scientific, professional, technical, mechanical, trade, clerical, fiscal, administrative, or other fields which will improve individual and organizational performance and assist in achieving the agency's mission and performance goals *(source: U.S.C. via OPM)*
Experiential Learning	The process of learning through experience, and is more specifically defined as learning through reflection on doing. Work such as internships, field work, and cooperative education that provide the program, regulatory, or procedural knowledge to perform the work *(source: OPM)*
Continuous Learning	Refers to the ongoing development of skills, abilities, and knowledge through different means (including work on the job, experiences, communications, etc.), and is part of an individual's ongoing professional life at work and outside of work *(source: Bersin)*
Credentials/ Certification	Registration, licenses, or certifications that are necessary for satisfactory job performance *(source: OPM)*

Table 2 – Proficiency Level Definitions

Level	Definition
Entry	An individual must have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance. An individual must be able to perform successfully in routine, structured situations.
Intermediate	An individual must have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance. An individual must be able to perform successfully in non-routine and sometimes complicated situations.
Advanced	An individual must have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance. An individual must be able to serve as a resource and provide guidance to others. An individual must also be able to perform successfully in complex, unstructured situations.

Capability indicators are not qualification requirements; rather, they are recommendations from SMEs that will help organizations understand the kinds of qualities they may want to look for or develop in cybersecurity workers. Organizations should establish their own formal qualification requirements, and can use some, none, or all of the recommendations depending on their needs.

3 Data Collection – Methodology & Analysis

The data collection process aimed to identify capability indicators for each NICE Framework Work Role across three proficiency levels (Entry, Intermediate, and Advanced). It also aimed to produce guidance to help organizations set consistent knowledge and skill requirement baselines and better determine when a cybersecurity worker is considered "qualified or capable" to perform a given Work Role.

3.1 Process Overview

Feedback and content from three focus group sessions, phone interviews, table questionnaires, and supplemental data were aggregated. The four-step data analysis approach was as follows:

1. **Pre-Focus Group Activities**: As invitations were distributed to potential SMEs, a standard protocol was developed. This protocol served as a roadmap for focus group and interview facilitators to clearly guide conversations and ask a variety of questions on each capability indicator by proficiency level for the relevant Work Role(s). In addition, read-ahead slides were sent to SMEs to provide additional information on the effort and the type of information to be collected.
2. **Transcription of Raw Data:** At least one facilitator and one notetaker participated in each interview and focus group. Notes from each focus group session and interview, as well as input received through email, were transcribed and aggregated in full written form to ensure overall quality and translated into capability indicator tables (see the Appendix).
3. **Theme Analysis:** As capability indicator data was analyzed, input from diverse sources was combined and summarized to reflect consensus. One-off data points that represented one person's opinion were not included unless there was no other data available in a given section.
4. **Detailed Findings:** Capability indicators for Work Roles were translated into tables (see the Appendix).

3.2 Methodology

To gather the most robust data possible from the greatest number of SMEs, the team conducted outreach to more than 1,000 potential SMEs across the Federal Government. For this effort, a SME was defined as someone with extensive experience or knowledge of the field. SMEs varied; some possessed extensive cybersecurity technical education and trainings, while others offered more hiring and management expertise. Given Paperwork Reduction Act (PRA) regulations limiting polling of the public (e.g., private industry, nonprofits, government contractors), participation in this effort was limited to federal employees. Potential SMEs were sought via:

- Previous NICE Framework focus group attendee lists
- Federal Virtual Training Environment (FedVTE) rosters (students who completed advanced- and expert-level training)

- CE&A stakeholder network (e.g., Department of Transportation, Department of Health and Human Services [HHS], Department of Labor, DHS internal organizations)
- Article describing the focus groups posted as the featured story for several weeks on the National Initiative for Cybersecurity Careers and Studies website
- DHS communications channels, including the homepage of FedVTE, National Protection and Programs Directorate Vision newsletter, May 2nd edition of *The Partnership Bulletin*, Office of Cybersecurity and Communications Wire Blog, DHS Connect Page, and Stop.Think.Connect. Campaign partners.

Capability indicator data was captured using four approaches: focus groups, phone interviews, table questionnaires (via email), and third-party supplemental data. Thirty-one SMEs from sixteen federal departments and agencies contributed data through these collection methods. SMEs represented the Department of Transportation, DHS, Internal Revenue Service, Social Security Administration, Department of Veterans Affairs, Department of Education, U.S. Postal Service, Nuclear Regulatory Commission, HHS, Department of Labor, National Aeronautics and Space Administration, National Geospatial-Intelligence Agency, U.S. Peace Corps, Department of Commerce, U.S. Patent and Trademark Office, and Federal Bureau of Investigation.

Focus Groups

Focus groups with approximately 4–8 SMEs each were conducted offsite at nongovernmental facilities. Three focus groups addressing five Work Roles were conducted; each session lasted no longer than 3 hours, with 1.5 hours allotted for each Work Role. Most focus group SMEs attended in person, with two participating via teleconference.

DHS CE&A staff welcomed SMEs, and an external, objective contracting team moderated the sessions. After introductions, the moderators facilitated discussion on the five capability indicators (education, training, credentials/certifications, experiential learning, continuous learning) across three proficiency levels (Entry, Intermediate, Advanced). The moderator asked SMEs to brainstorm their inputs independently and then discuss them as a group.

Phone Interviews and Table Questionnaires

To attract additional SMEs, a flexible data capture approach was used. Potential SMEs were given the option of providing capability indicator data for specific Work Roles in a table via email and/or a 30-minute phone interview. Overall, 24 email table questionnaire submissions and 20 phone interviews were conducted, addressing 20 Work Roles.

Potential SMEs received an email request to participate, which included the Work Roles in which they identified interest and instructions for filling out an embedded table and/or scheduling a phone interview.

Supplemental Data

To further enhance the data collected from individuals, supplemental data was collected from cybersecurity career path-related efforts conducted at DHS and partner agencies, including HHS. The Department of the Navy shared data it had gathered on workforce qualifications and skills across proficiency levels for each Work Role in the NICE Framework. A data comparison with counterparts at the DoD Chief Information Officer (CIO) was also applied to understand similarities or discrepancies between the civilian and military domains regarding the data-gathering approach and feedback. Supplemental data was used for all Work Roles for which it existed. Given no SME input, supplemental data was used exclusively for 18 Work Roles. Other sources used to enhance the findings include CyberSeek's [3] interactive career pathway tool, which shows "key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role".

3.3 Analysis

As discussed, capability indicator data was collected from four sources: focus groups, phone interviews, table questionnaires, and supplemental data. Upon receiving the data, the team first scrubbed it for any SME-identifying features (e.g., agency-specific qualifications) and vendor- or agency-specific trainings, listing learning by topic.

Next, the team analyzed the data for consensus. If there was more than 50 percent agreement among the data sources, that finding was inputted into the final capability indicator table. However, if there was no consensus, the team noted any caveats (e.g., bachelor's degree may be beneficial but not necessary). Overly vague inputs were also removed.

Time permitting, facilitators sought answers to broader thematic questions regarding cybersecurity workforce development in addition to completing the capability indicator matrix.

4 Findings

4.1 Themes

Through focus group sessions, phone interviews, questionnaires, and supplemental data, several common themes emerged.

1. **Higher education is not always necessary to enter the cybersecurity field:** The Entry level is the first performance level in any given Work Role. At this level, workers generally are in learning mode, needing greater supervision and less job complexity to succeed. They also need to learn skills that are the baseline for their chosen area. As such, associate's and bachelor's degrees were generally deemed sufficient, or certain years of experience or certifications were deemed a substitute for education altogether. Broad training and certification topics were also commonly recommended, such as systems administration, information assurance, awareness, and software security.

   This finding underscores the need for increased awareness of federal hiring qualification requirements and eligibility guidelines for cybersecurity positions. In the Federal Government, OPM's well-established GS drives qualification requirements for most positions. Job series (e.g., 2210) into which cybersecurity workers are frequently hired often do not have a minimum educational requirement [4]. SME recommendations for education capability indicators also show that some Work Roles do not require a bachelor's degree to enter into the field – yet, a bachelor's degree is often advertised as a minimum requirement for jobs. Managers and applicants alike may not know that for certain job series, general and/or specialized prior work experience may substitute education. Lack of awareness of this option can lead the government to face challenges when recruiting top talent. For example, a hiring manager may submit a job requisition that indicates a bachelor's degree is the minimum requirement. Those in the internal approval chain (e.g., HR) may not question the manager's choice for that minimum requirement, whereas the job manager may have simply assumed a bachelor's degree is required. This may lead those without a bachelor's degree to not apply for an entry level Government position, and instead seek employment in the private sector.

   The Federal Government could better compete for entry level talent by increasing awareness that OPM does not require a bachelor's degree for certain job series and that certifications and work experience may substitute for education in certain types of roles (as detailed in this report). Given the shorter hiring process in the private sector, government hiring managers need to be cognizant of exactly what options they have at their disposal (e.g., minimum OPM requirements, pay flexibilities for cybersecurity positions).

   Coupling this increased awareness with the Government's unique mission and work that other sectors cannot provide will enable the Government to compete more effectively in the talent marketplace.

2. **Certifications and training are relied upon for skill development and are considered indicators of ability:** Common academic degrees recommended include computer science, cybersecurity, IT, software engineering, information systems, and computer engineering.

However, degrees in these areas were often mentioned in the same breath as certifications and training. Often, SMEs recommended certifications over education as a way for workers to acquire new skills and progress their careers. Given that certifications often take less time and money than an academic degree, the appeal is understandable. If a particular skills gap is identified, staff and managers can consider pursuing certifications that address particular skills. The recommendations in the Appendix may help identify the topics and skills to target based on which Work Role is performed.

In addition to being a source of skill development, certifications are also considered indicators of ability. For instance, when being recruited into a position, an employee's certifications are often assumed to indicate ability in specific topics (based on the certification type). Once that employee is in the job, whether or not his/her performance meets expectations is a topic of debate. Nevertheless, this assumption was described by SMEs as being pervasive.

Also, as a retention incentive, OPM authorizes agencies to offer pay increases for cyber personnel who hold certifications in "highly-desired cybersecurity skills [5]." OPM policy [5] states: The agency may approve a retention incentive of up to 25 percent of basic salary to an individual GS cybersecurity employee or a retention incentive of up to 10 percent of basic salary to a group of GS cybersecurity employees with highly-desired certifications or credentials.**Error! Bookmark not defined.**

If certifications are not preferred because of budgetary limitations or time away from the job, viable alternatives such as training, mentoring, or job shadowing opportunities may be internally offered, as well as external training. For example, a Security Architect with 3-5 years of experience may be able to design enterprise/systems security throughout the development lifecycle with security professional and enterprise architecture training instead of a formal certification. Job shadowing and mentoring from a more experienced security architect also provides valuable learning. Further, government personnel can access free online cybersecurity skills training via the FedVTE [6].

3. **On-the-job experience is essential for higher-level proficiency**: According to SMEs, to manage effectively or perform more advanced technical work, prior experience is often a requisite. Particularly within the government, specific regulations and systems require at least several years of hands-on experience (often much more) to learn. To give entry and mid-level talent the on-the-job experience to become future leaders and experts, the government must offer clear career paths. These paths should outline the kinds of on-the-job experiences (and other qualifications) that staff will need to progress to higher proficiency levels.

Cybersecurity career paths are not readily found in most government organizations because of the new and rapidly evolving nature of the cybersecurity field. However, the NICE Framework and capability indicator recommendations provide the baseline standard for defining which cybersecurity positions and proficiency levels an organization may need. These standards act like a menu for developing career paths – organizations can pick Work Roles their organization needs and begin populating requirements at each proficiency level by referring to the capability indicators and setting their own formal qualification

requirements. Also, in the absence of a career path, workers will not know what on-the-job experiences they need in order to progress within an agency, and they may seek a career outside the government that offers clearer options. Ultimately, developing career paths will help the government retain cybersecurity talent and keep its pipeline for higher-level positions strong.

4. **Risk is the most frequently recommended topic for training and certifications:** Variations on the topic of risk were the most frequently recommended for training and certifications (e.g., risk management, identification, measurement, analysis, monitoring). This finding was seen across disparate technical and non-technical areas. For example, understanding risk is important not only for technical cybersecurity workers on the front lines but also for instructional designers who teach cybersecurity or leaders who set strategy.

   This theme underscores how critical risk is in cybersecurity and the need for risk analysis to be integrated into cybersecurity workforce decisions around hiring, development, and retention. For example, government organizations should regularly inventory their workforce using the NICE Framework and see where they have gaps (based on their unique workload and risks). If a mission-critical skill is missing from a team, then that skill can become a recruitment priority. Similarly, when deciding how to develop existing talent, organizations can look at where they have gaps and identify training that targets specific skills. Staff with skills needed to mitigate cybersecurity risks may also be selected for retention (e.g., agencies are authorized to increase pay for employees who possess skills and certifications that are deemed critical). Evaluating risk is also important for those running organizations who need to determine where to allocate resources – if a mission-critical function has an increased cybersecurity risk, a greater amount of cybersecurity workforce investment may be justified.

   (NOTE: Other training and certification topics frequently recommended by SMEs include secure software/development, network infrastructure, security engineering, and information assurance.)

5. **Continuous learning is required at almost all levels**: Continuous learning is particularly important to cybersecurity because of the fast pace of change in the field, the emergence of new technology, and constantly evolving threats. Continuous learning—including mentoring, job shadowing, detail and job rotations, and professional conferences—were recommended at all levels across almost all Work Roles. However, there are some differences between levels. For instance, at the Entry level, it is expected that workers receive guidance and expand their skills outside of their day-to-day responsibilities via conferences and workshops. At the Advanced level, expectations focus on mentoring junior staff, researching new concepts, publishing and presenting new solutions to the broader cybersecurity community, and having exposure to more diverse and complex projects.

   This finding emphasizes the importance of engagement in continuous learning by cybersecurity workers to keep their skills, knowledge, and abilities up to date. Capability indicators help define a set of baseline measures for evaluation of continuous learning activities. Government organizations can consider applying indicators against details and offering an increase in inter- and intra-agency job rotation programs, so workers expand their

skills and use of diverse methods of analysis and response. Organizations can also encourage a culture of mentoring in their cybersecurity functions at all levels, either through one-on-one sessions or mentoring circles where staff exchange ideas and advice in a group setting. Mentoring or job shadowing can help increase learning, overcome the knowledge loss from attrition, and yield close working relationships which can increase staff retention.

Capability Indicator by Work Role Detailed Findings

Capability indicator data for 43 Work Roles was gathered, analyzed, and consolidated. These detailed findings are captured in the Appendix.

Following a systematic process, DHS obtained thorough data from SMEs via four approaches (e.g., focus group sessions, phone interviews, email, and supplemental data). The supplemental data gathered from agency partners was systematically blended with SME inputs from the other activities for each Work Role.

As can be expected in a data gathering effort of this scale, occasional gaps occurred. Particularly due to challenges with obtaining responses from intelligence and law enforcement SMEs, capability indicator data was unable to be obtained for the following nine Work Roles:

Category: Oversee and Govern

- Privacy Compliance Manager

Category: Analyze

- Exploitation Analyst
- Missions Assessment Specialist
- Target Developer
- Target Network Analyst
- Multi-Disciplined Language Analyst

Category: Collect and Operate

- All-Source Collection Manager
- All-Source Collection Requirements Manager
- Cyber Operator

Appendix A - Capability Indicator Tables by Work Role

All capability indicator recommendations provided by SMEs are captured in this appendix. As discussed earlier, these indicators are recommendations, not formal requirements to be used as-is without customization for qualifying individuals. Organizations can use these capability indicator recommendations as a baseline from which to begin defining their own formal qualification requirements based on their unique cybersecurity workforce needs.

For credentials/certifications capability indicators, there are many recommended topics for most Work Roles. However, cybersecurity workers do not need to have certifications that address all the recommended topics. Their type of work will determine which and how many certifications they need. Note that certificates and certifications are not the same thing, and the Federal Government does not pay for or validate certificates, only certifications.

Therefore, when interpreting these recommendations, please note that no single capability indicator alone is a requirement to perform a Work Role. Capability indicators should be considered a menu of suggestions from which organizations can gain inspiration and ideas and begin their own qualification development.

Also, please note that in some instances, data was not able to be gathered for all capability indicators. These fields are noted with an "N/A," which stands for "not available."

Use the information on the following pages to navigate the Work Role capability indicator tables. The following page contains a sample table with example data that breaks down each part (i.e., a legend for the subsequent 43 tables). A table on pages 21-22 provides hyperlinks to each Work Role table to ease navigation. Hyperlinks are not included for the nine Work Roles for which no capability indicator data was obtained.

Sample Work Role Capability Indicator Table

Use the explanations in red text/example columns in this sample table to understand the capability indicator data provided in the Appendix.

NICE FRAMEWORK WORK ROLE TITLE Definition: NICE Framework Work Role's Definition (Work Role identifier information) *CATEGORY:* ***WORK ROLE'S NICE FRAMEWORK CATEGORY*** *SPECIALTY AREA:* ***WORK ROLE'S NICE FRAMEWORK SPECIALTY AREA***			
(Proficiency Levels)	**Entry**	**Intermediate** EXAMPLE	**Advanced** EXAMPLE
EDUCATION	▪ *Recommended*: If education is recommended, "Yes"; if not, "No"; if optional, "Not essential but may be beneficial"; if data is not available, "N/A" ▪ *Example Types*: When recommended, example types of degrees will be provided ("Bachelor's, master's") ▪ *Example Topics*: Example topics are academic fields of study for the recommended degrees	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: If training is recommended, "Yes"; if not, "No"; if optional, "Not essential but may be beneficial"; if data is not available "N/A" ▪ *Example Topics*: When recommended, example topics that the training must address are provided; organizations can identify training courses (internally or from external vendors) that teach the recommended topics	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced information systems security management, programing, cryptography
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: If certifications (or other credentials) are recommended, "Yes"; if not, "No"; if optional, "Not essential but may be beneficial"; if data is not available, "N/A" ▪ *Example Topics*: When recommended, topics that certifications may address for this Work Role are provided; every listed topic does not need to be addressed; organizations can identify specific vendors that offer certifications in the recommended topics	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address application vulnerabilities, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, operations, and maintenance	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications that address advanced risk management, asset security, identity and access management, security assessment, and incident management
EXPERIENTIAL LEARNING	▪ *Recommended*: If experiential learning is recommended, "Yes"; if not, "No"; if optional, "Not essential but may be beneficial"; if data is not available, "N/A" ▪ *Examples*: When recommended, examples of experiences are provided; Note – in some instances, partial data was gathered (e.g., years of experience / experiential learning not available for all Roles)	▪ *Recommended*: Yes ▪ *Examples*: 5 years of hands-on data analytics; 2+ years planning complex activities in an IT environment, requirement vetting and developing	▪ *Recommended*: Yes ▪ *Examples*: Prior experience as Information System Security Officer (ISSO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), CIO, Chief Risk Officer (CRO), and/or Privacy Official
CONTINUOUS LEARNING	▪ *Recommended*: If continuous learning is recommended, "Yes"; if not, "No"; if optional, "Not essential but may be beneficial"; if data is not available, "N/A" ▪ *Examples*: When recommended, examples of continuous learning are provided	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, conferences, rotations, developing publications)	▪ *Recommended*: N/A

Navigating Work Roles

Click the Work Role in the table below to quickly navigate to the capability indicators for that Work Role.

Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official/Designating Representative Security Control Assessor
	Software Development	Software Developer Secure Software Assessor
	Systems Architecture	Enterprise Architect Security Architect
	Technology Research and Development	Research and Development Specialist
	Systems Requirements Planning	Systems Requirements Planner
	Test and Evaluation	System Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer Systems Developer
Operate and Maintain	Data Administration	Database Administrator Data Analyst
	Knowledge Management	Knowledge Manager
	Customer Service and Technical Support	Technical Support Specialist
	Network Services	Network Operations Specialist
	Systems Administration	System Administrator
	Systems Analysis	Systems Security Analyst
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor *Privacy Officer/Compliance Manager**
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer Cyber Instructor
	Cybersecurity Management	Information Systems Security Manager Communication Security (COMSEC) Manager
	Strategic Planning and Policy	Cyber Workforce Developer and Manager Cyber Policy and Strategy Planner
	Executive Cyber Leadership	Executive Cyber Leadership

Category	Specialty Area	Work Role
	Program/Project Management and Acquisition	Program Manager IT Project Manager Product Support Manager IT Investment/Portfolio Manager IT Program Auditor
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist
	Incident Response	Cyber Defense Incident Responder
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst
Analyze	Threat Analysis	Threat/Warning Analyst
	Exploitation Analysis	*Exploitation Analysis**
	All-Source Analysis	All-Source Analyst *Mission Assessment Specialist**
	Targets	*Target Developer** *Target Network Analyst**
	Language Analysis	*Multi-Disciplined Language Analyst**
Operate and Collect	Collection Operations	*All-Source Collection Manager** *All-Source Collection Requirements Manager**
	Cyber Operational Planning	Cyber Intel Planner Cyber Ops Planner Partner Integration Planner
	Cyber Operations	*Cyber Operator**
Investigate	Cyber Investigation	Cyber Crime Investigator
	Digital Forensics	Law Enforcement/Counterintelligence Forensics Analyst Cyber Defense Forensics Analyst

*Work Roles without capability indicator data.

AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE Click to Return to Work Role List			***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: RISK MANAGEMENT***
Definition: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing information assurance, critical infrastructure protection, enterprise information security, and risk management may substitute education)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's/M.B.A. ▪ *Example Topics:* Information assurance or risk management (certifications addressing Approval to Operate [ATO] processes, cybersecurity law, critical infrastructure protection, and continuity of operations [COOP] may substitute education)	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Information assurance or risk management (certifications addressing ATO processes, cybersecurity law, critical infrastructure protection, and COOP may substitute education)
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Systems administration and internal, organization-specific certifying officer training	▪ *Recommended*: Yes ▪ *Example Topics*: Network security and vulnerabilities, information systems security management, and advanced network analysis	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced information systems security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure, as well as system security, access control, cryptography, assessments/audits, organizational security, authentication, security testing, intrusion detection/prevention, incident response and recovery, cryptography, malicious code countermeasures, mobile devices, hardware evaluation, and operating systems	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address FedRAMP, risk management, categorization of information systems, selection of security controls, security control implementation/ assessment, authorization, risk identification/ assessment/evaluation, risk response/ monitoring, reducing production costs, application vulnerabilities and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal, network types/media, Transmission Control Protocol/Internet Protocol (TCP/IP), IP addressing/routing, and WAN technologies	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications that address advanced security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, categorization of information systems, selection of security controls, security control implementation, security control assessment, information system authorization, information security governance, information security program development and management, and information security incident management

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Service desk, network technology, systems administration, and supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Federal Information Security Management Act (FISMA) assessment, penetration testing, contingency testing, incident response testing, risk management, business impact analyses, supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Prior experience as an ISSO, CSO, CISO, CIO, CRO, and/or Privacy Official
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include shadowing, attending conferences, rotations, professional memberships)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include formal training, conferences, rotations, developing publications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include conference speaking, rotations, publications, providing mentoring, and development of new ideas/methods)

SECURITY CONTROL ASSESSOR	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: RISK MANAGEMENT***
Definition: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an IT system to determine the overall effectiveness of the controls (as defined in NIST 800-37).		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's (minimum) ▪ *Example Topics:* Information systems security	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Advanced systems management, systems administration, information systems security, system certification, risk analysis (certifications addressing these topics may substitute education)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Information technology, information security, instructional systems design, communications
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Systems administration	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, information systems security, and advanced network analysis	▪ *Recommended*: Yes ▪ *Example Topics*: Information systems security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, and cryptography	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, managing network environments, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, system security, network infrastructure, access control, cryptography, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident management, integration of computing/ communications/business disciplines and enterprise components, change management/incident handling for managers, common attacks and malware, security policy, disaster recovery and contingency planning, total cost of ownership, physical security and facility safety, privacy and web security, risk and ethics, protecting intellectual property, network infrastructure, quality and growth of the security organization, wireless security, network and endpoint security technologies, network protocols for managers, project management, managing the mission

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training in information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

610

SOFTWARE DEVELOPER Click to Return to Work Role List

CATEGORY: SECURELY PROVISION
SPECIALTY AREA: SOFTWARE DEVELOPMENT

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

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types:* Associate's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended:* Yes ▪ *Example Types:* Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended:* N/A
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing reducing production costs, application vulnerabilities and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing reducing production costs, application vulnerabilities and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing reducing production costs, application vulnerabilities and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

SECURE SOFTWARE ASSESSOR	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: SOFTWARE DEVELOPMENT***
Definition: Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's (optional) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (optional) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. (optional) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Software programming	▪ *Recommended*: Yes ▪ *Example Topics*: Software programming	▪ *Recommended*: Yes ▪ *Example Topics*: Software programming
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing application vulnerabilities and delivery delays, and secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition	▪ *Recommended*: Yes (optional) ▪ *Example Topics*: Certifications addressing software programming/development, reducing production costs, application vulnerabilities and delivery delays, and secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition	▪ *Recommended*: Yes (optional) ▪ *Example Topics*: Certifications addressing software programming/development, reducing production costs, application vulnerabilities and delivery delays, and secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 2+ years apprenticeship assessing software security	▪ *Recommended*: Yes ▪ *Examples*: 3+ years apprenticeship assessing software security	▪ *Recommended*: Yes ▪ *Examples*: 5+ years apprenticeship assessing software security
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

612

ENTERPRISE ARCHITECT Click to Return to Work Role List		***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: SYSTEMS ARCHITECTURE***
Definition: Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.		
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: N/A (not an Entry-level role)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident response, research and analysis, integration of computing, communications, and business disciplines, as well as technical integration of enterprise components, reducing production costs, application vulnerabilities, and delivery delays, secure software concepts, requirements, design, implementation/ coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition, IT service management/lifecycle, and change management	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, systems security engineering, certification and accreditation (C&A)/risk management framework (RMF), technical management, U.S. government information assurance-related policies and issuances, access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology-related business continuity planning (BCP) and disaster recovery planning (DRP), physical security considerations, IT service management/lifecycle, and change management
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

613

SECURITY ARCHITECT	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: SYSTEMS ARCHITECTURE***
Definition: Designs enterprise and systems security throughout the development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Annual awareness training, enterprise architecture, security professional training	▪ *Recommended*: Yes ▪ *Example Topics*: Role-related (specialized) training, annual awareness training, enterprise architecture, security professional training	▪ *Recommended*: Yes ▪ *Example Topics*: Role-related (specialized) training, annual awareness training, enterprise architecture, security professional training
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes (certifications may not be required with more than 3 years of experience) ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident response, research and analysis, integration of computing, communications, and business disciplines, as well as technical integration of enterprise components, reducing production costs, application vulnerabilities, and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition, IT service management/ lifecycle, and change management	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, systems security engineering, C&A/RMF, technical management, U.S. government information assurance-related policies and issuances, access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology-related BCP and DRP, physical security considerations, IT service management/lifecycle, and change management

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 2–3+ years, hands on, role-related experience, security-related apprenticeship	▪ *Recommended*: Yes ▪ *Examples*: 3–5 years on-the-job training or role-related experience	▪ *Recommended*: Yes ▪ *Examples*: 5–9+ years role-related experience
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Conferences (attending to learn), association membership, job shadowing	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (conferences, association membership, job shadowing, mentoring)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

614

RESEARCH AND DEVELOPMENT SPECIALIST Click to Return to Work Role List			***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: TECHNOLOGY RESEARCH AND DEVELOPMENT***
Definition: Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's, master's ▪ *Example Topics:* Systems engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer systems engineering	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Computer systems engineering, doctorate-level specialization in critical systems
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Apprenticeship/hands-on training; systems administration	▪ *Recommended*: Yes ▪ *Example Topics*: 2+ years of apprenticeship or supervised on-the-job training involving integrating different areas of knowledge to create a practical solution to a security problem; network security vulnerabilities, information system security, advanced network analysis	▪ *Recommended*: Yes ▪ *Example Topics*: 4+ years of apprenticeship/hands-on training involving integrating different areas of knowledge to create a practical solution to a security problem; information systems security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, business continuity and disaster recovery, cloud computing security, cryptography, incident management, IT governance, risk management, securing communications, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, managing network environments, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, business continuity and disaster recovery, cloud computing security, cryptography, incident management, and securing communications	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident management, change management/incident handling for managers, common attacks and malware, security policy, disaster recovery and contingency planning, total cost of ownership, operational security, physical security and facility safety, privacy and web security, ethics, protecting intellectual property, network infrastructure, quality and growth of the security organization, cryptography, vulnerabilities, wireless security, network and endpoint security technologies, network protocols for managers, project management, managing the mission, enterprise security, integration of computing, communications, and business discipline, and technical integration of enterprise components

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Hands-on experience with close supervision in information assurance	▪ *Recommended*: Yes ▪ *Examples*: 2+ years of experience, successful completion of three distinct projects	▪ *Recommended*: Yes ▪ *Examples*: Hands-on experience; successful completion of five distinct projects with outstanding results; increased variety and complexity of experience
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (tutorials, seminars, workshops)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (seminars, workshops)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (seminars, workshops)

615

SYSTEMS REQUIREMENTS PLANNER	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: SYSTEMS REQUIREMENTS PLANNING***
Definition: Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial (4 years on-the-job experience may substitute education) ▪ *Example Types*: No degree, associate's, bachelor's ▪ *Example Topics:* Systems engineering, IT, and business fields	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* IT and business fields; systems engineering; coursework in communications, liberal arts, and sciences may be beneficial	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Systems engineering; coursework in communication, liberal arts, sciences, security management, and IT leadership may be beneficial
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Apprenticeship/hands-on training; business systems requirements documentation, introductory project management with risk management emphasis	▪ *Recommended*: Yes ▪ *Example Topics*: Minimum 2 years of apprenticeship/hands-on training; systems requirements documentation	▪ *Recommended*: Yes ▪ *Example Topics*: Hands-on training in complex systems requirements planning and project management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing IT service management/lifecycle, change management, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing IT service management/lifecycle, change management, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, and project management (initiating, planning executing, monitoring and controlling, closing)
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 5 years of relevant experience (a master's may substitute for 2 years of experience); minimum 5 years of hands-on data analytics; 2+ years planning complex activities in an IT environment, requirement vetting and developing, technical formatting; three projects successfully completed demonstrating independent project management capabilities	▪ *Recommended*: Yes ▪ *Examples*: 15+ years of relevant experience, developing and refining requirements among a variety of stakeholders, documenting and presenting requirements for technical and non-technical audiences, including senior management; experience with large-scale complex systems, stakeholder negotiations; successful completion of five diverse projects with outstanding results

CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Job shadowing, receiving mentoring, tutorials, seminars, or workshops	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include 0.5–3-day seminars; mentoring an Entry-level coworker with a more advanced manager in the mentoring circle)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include 0.5–3-day seminars; providing mentoring to others)

616

SYSTEM TESTING AND EVALUATION SPECIALIST	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: TEST AND EVALUATION***
Definition: Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements and analyzes/reports test results.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Computer science or IT security (certificate in information systems security may substitute an associate's degree)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science or IT security (certifications in systems management, systems administration, system certification, and risk analysis may substitute for a bachelor's degree)	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Computer science or security (advanced certifications in systems management, systems administration, system certification, and risk analysis may substitute a graduate degree)
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Essentials of cybersecurity, systems administration	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, information system security manager, advanced network analysis	▪ *Recommended*: Yes ▪ *Example Topics*: Information system security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, new attack vectors (emphasis on cloud computing technology, mobile platforms, and tablet computers), new vulnerabilities, existing threats to operating environments, network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network environments, risk management, categorization of information systems, selection and monitoring of security controls, security control implementation and assessment, and information system authorization	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, information, security program development and management, information security incident management, change management/incident handling for managers, common attacks and malware, managing access control, security policy, disaster recovery and contingency planning, total cost of ownership, operational security, physical security and facility safety, privacy and web security, protecting intellectual property, network infrastructure, quality and growth of the security organization, cryptography, vulnerabilities, wireless security, network and endpoint security technologies, network protocols for managers, project management, managing the mission, integration of computing, communications, and business discipline,

			technical integration of enterprise components; information systems audit process, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Experience in development and/or testing; supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Advanced knowledge and implementation experience of the Software Development Lifecycle (SDLC); on-the-job experience in information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include regular cybersecurity news alerts and industry newsletters, receiving mentoring, job shadowing)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include boot camps, tool-specific workshops)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include speaking at security conferences to share knowledge and learn from others, learning new and emerging tools)

617

INFORMATION SYSTEMS SECURITY DEVELOPER	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION SPECIALTY AREA: SYSTEMS DEVELOPMENT***
Definition: Designs, develops, tests, and evaluates information systems throughout the systems development lifecycle.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Information technology, information security, instructional systems design, communications	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Information technology, information security, instructional systems design, communications
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, information systems, cryptography, Linux, network security, troubleshooting, security operations, Unix, TCP/IP	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, information systems, cryptography, Linux, network security, troubleshooting, security operations, Unix, TCP/IP
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, protection of information assets, information security governance, information, security program development and management, incident management, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, protection of information assets, information security governance, information security program development and management, incident management, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

618

SYSTEMS DEVELOPER	Click to Return to Work Role List	***CATEGORY: SECURELY PROVISION*** ***SPECIALTY AREA: SYSTEMS DEVELOPMENT***
Definition: Designs, develops, tests, and evaluates information systems throughout the systems development lifecycle.		
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Information technology, information security, instructional systems design, communications	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Information technology, information security, instructional systems design, communications
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, information systems, cryptography, Linux, network security, troubleshooting, security operations, Unix, TCP/IP	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, information systems, cryptography, Linux, network security, troubleshooting, security operations, Unix, TCP/IP
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets, information security governance, security program development and management, information security incident management, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications assessing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets, information security governance, security program development and management, information security incident management, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

DATABASE ADMINISTRATOR — Click to Return to Work Role List — ***CATEGORY: OPERATE AND MAINTAIN*** ***SPECIALTY AREA: DATA ADMINISTRATION***			
Definition: Administers databases and/or data management systems that allow for the storage, query, and utilization of data.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's (2–5 years of experience in database management support may substitute education; certifications addressing planning, security, database objects, DB2 data using SQL, DB2 tables, views, and indexes, and data concurrency may substitute education) ▪ *Example Topics:* Computer science, computer networking, information science	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's, master's (7–18 years of experience in database management support may substitute education; certifications addressing planning, security, databases and database objects, DB2 data using SQL, DB2 tables, views, and indexes, and data concurrency may substitute education) ▪ *Example Topics:* Computer science, computer networking, information science, networking, and/or information science	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Master's, Ph.D. (15–20 years of experience in IT operations, data architecture, and/or infrastructure may substitute education) ▪ *Example Topics:* IT management, information science
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Enterprise IT environment, enterprise architecture, and data architecture	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Writing, communications, and interpersonal skills
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls, honeypots, ICMP, incident handling fundamentals, intrusion detection overview, IP packets, IPS overview, IPv6, legal aspects of incident handling, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and scanning, network	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls, honeypots, ICMP, incident handling fundamentals, intrusion detection overview, IP packets, IPS overview, IPv6, legal aspects of incident handling, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and

	environments, planning, security, working with databases and database objects, working with DB2 data using SQL, working with DB2 tables, views, and indexes, data concurrency	protocol, policy framework, protecting data at rest, public key infrastructure (PKI), reading packets, risk management, securing server services, SIEM/Log management, steganography overview, TCP, UDP, virtual private networks, viruses and malicious code, vulnerability management overview, vulnerability scanning, web application security, auditing and forensics, network security overview, permissions and user rights, security templates and group policy, service packs, hotfixes and backups, active directory and group policy overview, wireless security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures	scanning, network protocol, policy framework, protecting data at rest, PKI, reading packets, risk management, securing server services, SIEM/Log management, steganography overview, TCP, UDP, virtual private networks, viruses and malicious code, vulnerability management overview, vulnerability scanning, web application security, auditing and forensics, network security overview, permissions and user rights, security templates and group policy, service packs, hotfixes and backups, active directory and group policy overview, wireless security, information security governance, security program development and management, information security incident management, acquisitions, IT service management/lifecycle, change management, and project management (initiating, planning executing, monitoring and controlling, closing)
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Experience with enterprise server software, database management tools, database backup and recovery procedures (including development of documentation for all recurring data management tasks), and database performance tuning methodologies	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Experience with database management tools, database backup and recovery procedures, including development of documentation for all recurring data management tasks, database configuration and performance tuning, developing physical models, utilizing data modeling tools, the design and implementation of data security models, enterprise server software, and policy development	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Experience with IT operations, and data architecture, Infrastructure
CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, conferences, webinars)	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

619

DATA ANALYST	Click to Return to Work Role List	***CATEGORY: OPERATE AND MAINTAIN*** ***SPECIALTY AREA: DATA ADMINISTRATION***
Definition: Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's or high school diploma and 4 years of experience ▪ *Example Topics:* Statistics, economics, science (if curricula contain data analysis)	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's or high school diploma and 4 years of experience ▪ *Example Topics:* Statistics, economics, science (if curricula contain data analysis)	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* Cybersecurity
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Presentation skills	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Data normalization, data warehousing, and presentation skills	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Advanced analysis, advanced data mining, advanced data science, and presentation skills
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network environments	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 3 years of relevant experience or 1 year with a master's degree; experience with query tools, analytical and quantitative reasoning, report writing, and administrative tasks	▪ *Recommended*: Yes ▪ *Examples*: 5 years of relevant experience (a master's degree may substitute for 2 years of experience); experience with data analytics, predictive modeling, multiple tool databases, responding to complex questions, and operational tasks	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 10 years of experience in data analytics systems development, software engineering, systems development, predictive modeling, and understanding data storage and retrieval techniques
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, controlled exposure to more advanced work, and detailed reassignment/rotational program)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring Entry-level coworkers under the oversight of a supervisor)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring other team members)

620

KNOWLEDGE MANAGER Click to Return to Work Role List

CATEGORY: OPERATE AND MAINTAIN
SPECIALTY AREA: KNOWLEDGE MANAGEMENT

Definition: Is responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing knowledge management fundamentals, tools, best practices, job responsibilities, and information mapping	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network operations and technology
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: Information security	▪ *Recommended*: Yes ▪ *Examples*: Information security
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

621

TECHNICAL SUPPORT SPECIALIST	Click to Return to Work Role List	***CATEGORY: OPERATE AND MAINTAIN*** ***SPECIALTY AREA: CUSTOMER SERVICE AND TECHNICAL SUPPORT***
Definition: Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (e.g., master incident management plan, when applicable).		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's (certifications addressing information systems security may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's (certifications addressing risk analysis may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Master's, Ph.D., (certifications addressing risk analysis may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information assurance technician	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: System administrator, security essentials	▪ *Recommended*: Yes ▪ *Example Topics*: Self- or instructor-led training in LAN, WAN architectures and network security, advanced network analysis
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls, honeypots, ICMP, incident handling fundamentals, intrusion detection overview, IP packets, IPS overview, IPv6, legal aspects of incident handling, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and scanning, network protocol, policy framework, protecting data at rest, PKI, reading packets, risk management, securing server services, SIEM/Log management, steganography overview, TCP, UDP, virtual private networks, viruses and malicious code,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network environments, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, focus on new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, enterprise security, risk management and incident

		vulnerability management overview, vulnerability scanning, web application security, auditing and forensics, network security overview, permissions and user rights, security templates and group policy, service packs, hotfixes and backups, active directory and group policy overview, wireless security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures	response, research and analysis, integration of computing, communications and business disciplines as well as technical integration of enterprise components
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Experience in information assurance	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Experience in information assurance and networks	▪ *Recommended*: Yes ▪ *Examples*: 7+ years of experience directly performing configurations and security implementations on LAN and WAN equipment
CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include formal training, conferences, rotations, developing publications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include formal training, conferences, rotations, developing publications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include role rotations)

622

NETWORK OPERATIONS SPECIALIST — Click to Return to Work Role List — ***CATEGORY: OPERATE AND MAINTAIN SPECIALTY AREA: NETWORK SERVICES***			
Definition: Plans, implements, and operates network services/systems, including hardware and virtual environments.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's (certifications addressing information systems security, advanced systems management may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. (certifications addressing the following topics may substitute for education: analysis, assessment, control, mitigation, and management of risk within a federal management and acquisition framework that contain personal data; identification, implementation, and integration management, acquisition and administrative risk methodologies for securing critical and sensitive information infrastructures) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Strategic satellite communications systems, operating system functionality, OSI networking model, hardware components, and client and server relationships	▪ *Recommended*: Yes ▪ *Example Topics*: Classroom or distributed learning with access to virtually emulated or physical devices, transmission systems, frequency management, support communications, replacement program system operations, strategic satellite communications systems, cyber operations, network operations and technology, business acumen and knowledge of customer/operational requirements, broad understanding of operating system functionality, OSI networking model, hardware components, client/server relationships, and the interrelationship of multiple disparate IT systems	▪ *Recommended*: Yes ▪ *Example Topics*: Classroom or distributed learning with access to virtually emulated or physical devices, self or instructor-led training in the areas of LAN, WAN architectures and network security, transmission systems, frequency management, support communications, replacement program system operations, strategic satellite communications systems, cyber operations, network operations and technology, business acumen and knowledge of customer/operational requirements, broad understanding of operating system functionality, OSI networking model, hardware components, client/server relationships, and the interrelationship of multiple disparate IT systems

CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing managing, maintaining, troubleshooting, installing, configuring basic network infrastructure; vendor certifications	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Vendor certifications; Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security
EXPERIENTIAL LEARNING	▪ *Recommended*: yes ▪ *Examples*: 0–3 years of experience in information security	▪ *Recommended*: Yes ▪ *Examples*: 4–9 years of experience in information security and/or automated digital network systems (ADNS)	▪ *Recommended*: Yes ▪ *Examples*: 7–10+ years of experience, experience directly performing configurations and security implementation on LAN and WAN equipment
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include shadowing)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include virtual learning—workshops, training, webinars)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include virtual learning—workshops, training, webinars; role rotations)

623

SYSTEM ADMINISTRATOR — Click to Return to Work Role List — ***CATEGORY: OPERATE AND MAINTAIN*** ***SPECIALTY AREA: SYSTEMS ADMINISTRATION***			
Definition: Installs, configures, troubleshoots, and maintains hardware and software and administers system accounts.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's (certifications addressing information systems security may substitute education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's (certifications addressing the following may substitute education: analyzing, assessing, controlling, determining, mitigating and managing risk within a management and acquisition framework that contains personal data; identifying, implementing and integrating management, acquisition and administrative risk methodologies for securing critical and sensitive information infrastructures) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's, master's, Ph.D. (certifications addressing the following may substitute education: analyzing, assessing, controlling, determining, mitigating and managing risk within a management and acquisition framework that contains personal data; identifying, implementing, and integrating management, acquisition, and administrative risk methodologies for securing critical and sensitive information infrastructures) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information assurance, operational support systems, and security fundamentals	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Systems administration, security fundamentals	▪ *Recommended*: Yes ▪ *Example Topics*: Self- or instructor-led training in the areas of LAN, WAN architectures, and network security, advanced network analysis, and network security vulnerability
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, business continuity and disaster recovery, cloud computing security, incident management, IT governance, risk management, securing communications,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls, honeypots, ICMP, incident handling fundamentals, intrusion detection overview, IP packets, IPS overview, IPv6, legal aspects of incident handling, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and scanning, network protocol, policy framework,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security

	authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure	protecting data at rest, PKI, reading packets, risk management, securing server services, SIEM/Log management, steganography overview, TCP, UDP, virtual private networks, viruses and malicious code, vulnerability management overview, vulnerability scanning, web application security, auditing and forensics, network security overview, permissions and user rights, security templates and group policy, service packs, hotfixes and backups, active directory and group policy overview, wireless security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures	
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Information assurance	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Information assurance, area network, wireless reach back system, enterprise messaging system, combined enterprise regional information exchange system, global command and control system, networks	▪ *Recommended*: Yes ▪ *Examples*: 7+ years of experience directly performing configurations and security implementations on LAN and WAN equipment, information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include role rotations)

SYSTEMS SECURITY ANALYST	Click to Return to Work Role List	***CATEGORY: OPERATE AND MAINTAIN SPECIALTY AREA: SYSTEMS ANALYSIS***
Definition: Is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: No (not an Entry-level Work Role)	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's (certifications addressing information systems security, advanced systems management, may substitute education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's, master's, Ph.D. (certifications addressing information systems security and advanced systems management may substitute education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information systems security, network security vulnerability, advanced network analysis, and software products	▪ *Recommended*: Yes ▪ *Example Topics*: Self- or instructor-led training in the areas of LAN, WAN architectures, and network security
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines as well as technical integration of enterprise components, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, malicious code countermeasures, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing),	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network environments, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, focus on new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls, honeypots, ICMP, incident handling fundamentals, intrusion detection overview, IP packets, IPS overview, IPv6, legal aspects of incident handling, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and scanning, network protocol, policy framework, protecting data at rest, PKI, reading packets, risk management, securing server services, SIEM/Log management, steganography overview, TCP, UDP, virtual private networks, viruses and malicious code, vulnerability management overview, vulnerability scanning, web application security, auditing and forensics, network security

		benefits management, stakeholder management, and governance	overview, permissions and user rights, security templates and group policy, service packs, hotfixes and backups, active directory and group policy overview, wireless security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures, network and endpoint security technologies, network protocols for managers, project management and business situational awareness, selling and managing the mission, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, stakeholder management, and governance
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Information assurance technician level II, information assurance manager, network	▪ *Recommended*: Yes ▪ *Examples*: 7+ of experience directly performing configurations and security implementations on LAN and WAN equipment, information assurance technician level III, information assurance manager, network
CONTINUOUS LEARNING	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include formal training, conferences, rotations, developing publications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually, work role rotations

625

CYBER LEGAL ADVISOR — Click to Return to Work Role List			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: LEGAL ADVICE AND ADVOCACY***
Definition: Provides legal advice and recommendations on relevant topics related to cyber law.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: J.D. ▪ *Example Topics:* Law (with cyber-related specialization if available)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, J.D. ▪ *Example Topics:* Law (with cyber-related specialization if available), cybersecurity, information technology, software engineering, or information systems	▪ *Recommended*: Yes ▪ *Example Types*: J.D. ▪ *Example Topics:* Law (with cyber-related specialization if available)
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: No
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: No	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing U.S. government privacy laws (privacy definitions and principles, The Privacy Act and the E-Government Act, other laws and regulations affecting U.S. government privacy practice, privacy and the federal intelligence community, other federal information privacy laws and authorities affecting government practice), U.S. government privacy practices (privacy program management and organization, records management, auditing and compliance monitoring), security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Example*: Support a cyber legal mentor in a crisis	▪ *Recommended*: Yes ▪ *Examples*: Breach response planning and operations (a discussion-based exercise that focuses on existing plans, policies, mutual aid agreements, and procedures used among multiple agencies and/or teams)
CONTINUOUS LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, associations, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, associations, rotations, and becoming a cyber legal operational lead)

CYBER INSTRUCTIONAL CURRICULUM DEVELOPER	Click to Return to Work Role List	*Category: Oversee and Govern* *Specialty Area: Training, Education, and Awareness*
Definition: Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. Note: For this role, the cybersecurity worker can be a technical expert who has an ability to train (e.g., skill in teaching and being engaging) or can be a skilled trainer who can acquire technical expertise via certifications and hands-on experience.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Psychology, instructional design, telecommunications, economics, information technology, communications, journalism, information security	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Psychology, instructional design, telecommunications, economics, information technology, communications, journalism, information security	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. ▪ *Example Topics:* IT, instructional design, information security
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Talent development, human resources, technical, instructional designer, learning, graphic design	▪ *Recommended*: Yes ▪ *Example Topics*: IT, cyber, instructional design, learning, graphic design, vendor (e.g., virtual learning environment and course management system, rapid responsive authoring tools used for creating e-learning content, and online teaching and training software trainings), 508 compliance, learning management systems	▪ *Recommended*: Yes ▪ *Example Topics*: Instructional design, workforce development, learning styles, IT
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing IT fundamentals, instructional design, training delivery, performance improvement, evaluating learning impact, managing learning programs, coaching, integrated talent management, change management, knowledge management, learning technologies, global mindset, foundational instructional design theories, application(s) for developing learning experiences for digital platforms (including project planning, content expertise, communication, writing, and technology), understanding of pertinent technology, programs, and methods (including interactive media, video, editing, digital design, and digital narrative), knowledge in focused topic areas (such as website development, web programming, and content management systems site development), e-learning design, practical knowledge, conducting a needs assessment for learning programs that aligns organizational	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, systems security engineering, C&A/ RMF, technical management, U.S. government information assurance-related policies and issuances, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing,

	objectives and the learning opportunity (aligns organizational objectives and the learning opportunity, address target populations' specific needs, identify constraints and/or problems affecting design success, basic outcomes of the learning solution linked to business problems or opportunities), designing learning solutions that reflect adult learning theories, and best address the needs of the learners and the organization through formal classroom training, blended learning, online learning, and informal approaches, use a collaborative approach with stakeholders (such as internal clients and SMEs) throughout a learning design project (plan and design the solution, select and/or create effective learning materials, establishing sign-off and approval processes for each step of the design process), creating complete learning solutions (measurable learning objectives, instructional content that reflects the diversity of the learners, a variety of learning methods and emerging technologies to reach learning outcome), identifying appropriate evaluation techniques and apply them to measure the impact of the learning solution, gamification, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines as well as technical integration of enterprise components, reducing production costs, application vulnerabilities and delivery delays, and secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition, change management and incident handling for managers, common attacks and malware, managing access control, managing defense in depth and security policy, managing disaster recovery and contingency planning, managing employees and total cost of ownership, managing operational security, managing physical security and facility safety, managing privacy and web security, managing risk and ethics, managing security awareness and protecting intellectual property, managing the network infrastructure, managing quality and growth of the security organization, managing the use of cryptography, managing vulnerabilities, managing wireless security, network and	security operations, software development security, access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology-related BCP and DRP, physical security considerations, analyzing course materials and learner information, assuring preparation of the instruction site, establishing and maintaining instructor credibility, managing the learning environment, demonstrating effective communication skills, demonstrating effective presentation skills, demonstrating effective questioning skills and techniques, responding appropriately to learner's needs for clarification and feedback, providing positive reinforcement and motivational incentives, using instructional methods appropriately, using media effectively, evaluating learner performance, evaluating delivery of instruction, reporting evaluation information, instructional design, training delivery, performance improvement, evaluating learning impact, managing learning programs, coaching, integrated talent management, change management, knowledge management, learning technologies, global mindset, evaluative concepts

		endpoint security technologies, network protocols for managers, project management and business situational awareness, selling and managing the mission, analyzing course materials and learner information, assuring preparation of the instruction site, establishing and maintaining instructor credibility, managing the learning environment, demonstrating effective communication skills, demonstrating effective presentation skills, demonstrating effective questioning skills and techniques, responding appropriately to learner's needs for clarification and feedback, providing positive reinforcement and motivational incentives, using instructional methods appropriately, using media effectively, evaluating learner performance, evaluating delivery of instruction, reporting evaluation information	
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes (Navy data does not recommend) ▪ *Examples*: 2–3 years of hands-on experience, internship, instructional designer frameworks, 508 training, evaluative concepts, adult learning styles, learning cycles, cyber or tech curriculum development experience prior	▪ *Recommended*: Yes ▪ *Examples*: 5–7+ years of hands-on experience including internships, instructional designer frameworks, 508 compliance training, evaluative concepts, exposure to different types of audiences and learning styles, technical cyber curriculum development, managerial experience, training delivery strategy, technical and user-specific content
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include attending conferences, in cybersecurity/IT cybersecurity preferred to gain technical background, curriculum-specific learning, mentoring, participation and award group collaborative environment, professional membership	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring others, receiving mentoring, cybersecurity and instructional design workshops, applying gamification, staying up-to-date on new technology and generational learning, business proposal writing, identifying and designing remediation plans)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring others, speaking at events [e.g., panels, conference presentations], championing projects, leading teams, gaining exposure to enterprise-wide cybersecurity training needs and solutions [e.g., rotations, details])

626

CYBER INSTRUCTOR	Click to Return to Work Role List	***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: TRAINING, EDUCATION, AND AWARENESS***
Definition: Develops and conducts training or education of personnel within cyber domain.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's ▪ *Example Topics:* Communications, IT, cybersecurity, education, journalism, engineering, computer science	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D.
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Adult learning styles, tactical learning styles, communications, presentation skills, conflict management, vendor training (e.g., a virtual learning environment and course management system), in-person training, distance training, online, blended, instruction	▪ *Recommended*: Yes ▪ *Example Topics*: Evaluation, adult learning styles, tactical learning styles, communications training, presentation skills, soft skills training, conflict management, vender training (e.g., a virtual learning environment and course management system), learning evaluation, instruction	▪ *Recommended*: Yes ▪ *Example Topics*: Learning evaluation, assessment, statics, train-the-trainer, instruction
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, analyzing course materials and learner information, assuring preparation of the instruction site, establishing and maintaining instructor credibility, managing the learning environment, demonstrating effective communication skills, demonstrating effective presentation skills,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing evaluative concepts, instructional design, training delivery, performance improvement, evaluating learning impact, managing learning programs, coaching, integrated talent management, change management, knowledge management, learning technologies, wireless networks, incident handing, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines as well as technical integration of enterprise components, reducing production costs, application vulnerabilities and delivery delays, as well as secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition, change management and incident handling for managers, common attacks and malware, managing access control, managing defense in depth and security policy, managing disaster recovery and contingency planning,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security

	demonstrating effective questioning skills and techniques, responding appropriately to learner's needs for clarification and feedback, providing positive reinforcement and motivational incentives, using instructional methods appropriately, using media effectively, evaluating learner performance, evaluating delivery of instruction, reporting evaluation information	managing employees and total cost of ownership, managing operational security, managing physical/facility security, managing privacy and web security, managing risk and ethics, managing security awareness and protecting intellectual property, managing the network infrastructure, managing quality and growth of the security organization, managing the use of cryptography, managing vulnerabilities, managing wireless security, network and endpoint security technologies, network protocols for managers, project management and business situational awareness, selling and managing the mission, analyzing course materials and learner information, assuring preparation of the instruction site, establishing and maintaining instructor credibility, managing the learning environment, demonstrating effective communication skills, demonstrating effective presentation skills, demonstrating effective questioning skills and techniques, responding appropriately to learners' needs for clarification and feedback, providing positive reinforcement and motivational incentives, using instructional methods appropriately, using media effectively, evaluating learner performance, evaluating delivery of instruction, reporting evaluation information	
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Example Topics*: Experience teaching and speaking in front of a group at any level; toastmasters, internship, mentoring, job shadowing	▪ *Recommended*: Yes ▪ *Examples*: Technical hands-on experience, can be a technical SME with training experience; mentoring	▪ *Recommended*: Yes ▪ *Examples*: Technical experience, teaching, mentoring, job shadowing, being shadowed, speaking at conferences, thought leadership
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include learning and development conferences, experience with gamification and cutting-edge techniques, making a business case, cybersecurity conferences, emerging technology exposure, receiving mentoring, ongoing collaboration in a team context, professional memberships)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include conferences, rotational team assignments involving technology, job shadowing, being shadowed by junior staff)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include assessments)

627

INFORMATION SYSTEMS SECURITY MANAGER Click to Return to Work Role List Definition: Is responsible for the cybersecurity of a program, organization, system, or enclave.			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: CYBERSECURITY MANAGEMENT***
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Information security, computer science, electrical systems, cybersecurity	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing advanced systems management may substitute education) ▪ *Example Topics:* Information security, computer science, electrical systems, cybersecurity	▪ *Recommended*: Yes ▪ *Example Types:* Master's, Ph.D., (certifications addressing advanced systems management, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, identity theft], strategic planning, finance, and vendor management may substitute education) ▪ *Example Topics:* Information security
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Leadership	▪ *Recommended*: Yes ▪ *Example Topics*: Leadership, technical, information system security management	▪ *Recommended*: Yes ▪ *Example Topics*: Leadership, technical cyber training
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Certifications addressing new attack vectors (emphasis on cloud computing technology, emphasis on mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, change management and incident handling for managers, common attacks and malware, managing access control, managing defense in depth and security policy, managing disaster recovery and contingency planning, managing employees and total cost of ownership, managing operational security, managing physical security and facility safety, managing privacy and web security, managing risk and ethics, managing security awareness and protecting intellectual property, managing the network infrastructure, managing quality and growth of the security organization, managing the use of cryptography,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, information, security program development and management, information security incident management

	managing vulnerabilities, managing wireless security, network and endpoint security technologies, network protocols for managers, project management and business situational awareness, selling and managing the mission, information security governance, information risk management, security program development and management, information security incident management, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, malicious code countermeasures		
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Example Types*: 2–3 years of experience as a team/technical lead working on security/networks/ systems operations, shadowing intermediate-level managers, receiving and providing prior mentoring	▪ *Recommended*: Yes ▪ *Examples*: 1–3 years of experience as a manager of security/networks/systems operations, and directly involved with operations management, policy development, system procurement activities, leadership, shadowing master-level managers, mentorship, information assurance management	▪ *Recommended*: Yes ▪ *Examples*: 3+ years of experience leading multiple security/networks/systems operations, significant involvement with operations management, business continuity and policy compliance development, system procurement activities, shadowing, mentoring, supervised on-the-job training
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Virtual learning (webinars, workshops), participation in annual security conferences	▪ *Recommended*: Yes ▪ *Examples*: 20–40 hours annually (may include workshops, seminars, participation in annual security conferences)	▪ *Recommended*: Yes ▪ *Examples*: Mentor others, speak at events (e.g., panels, conference presentations), champion projects, lead teams, exposure to enterprise-wide cybersecurity training needs and solutions (e.g., rotations, details)

628

COMSEC MANAGER Click to Return to Work Role List			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: CYBERSECURITY MANAGEMENT***
Definition: Individual who manages the communications security ('COMSEC') resources of an organization.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: No (not an Entry-level Work Role)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing national information assurance training standards for senior systems managers may substitute education)	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing national information assurance training standards for senior systems managers or chief information security officers may substitute education)
TRAINING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Example Topics*: Leadership, information system security management	▪ *Recommended*: No
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing business continuity and disaster recovery, cloud computing security, cryptography, incident management, IT governance, risk management, securing communications, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, and stakeholder management	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security leadership, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information security program development and management, information security incident management, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, and stakeholder management
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training as an information assurance technician and/or a beginner or intermediate information professional	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training as an information assurance manager and/or a beginner or intermediate information professional
CONTINUOUS LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

629

CYBER WORKFORCE DEVELOPER AND MANAGER Click to Return to Work Role List		***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: STRATEGIC PLANNING AND POLICY***
Definition: Develops cyber workforce plans, strategies, and guidance to support cyber workforce manpower, personnel, training, and education requirements and to address changes to cyber policy, doctrine, material, force structure, and education and training requirements.		
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D.
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Workforce planning/HC	▪ *Recommended*: Yes ▪ *Example Topics*: Workforce planning, cybersecurity, legislative	▪ *Recommended*: Yes ▪ *Example Topics*: Technical cybersecurity/IT, instructional design, HC, learning styles, organizational design, change management, communications
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial *Example Topics*: Certifications addressing talent management, strategic workforce planning, business strategy, differentiated segments, environmental scan, current state, futuring, gap analysis, action planning, monitoring and reporting, getting started, conclusion, business and economic development intelligence, career development principles, collaboration and problem solving, customer service methodology, diversity, labor market information and intelligence, principles of communication, program implementation principles and strategies, workforce development structure, policies and programs, business management and strategy, workforce planning and employment, human resource development, compensation and benefits, employee and labor relations, risk management, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, building financial acumen, improving financial literacy, acting on meaningful analytics, the ROI of engagement, collaboration, and retention (ECR), building trust and	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing the linkage between business strategy and talent acquisition strategy, creating a partnership with hiring managers, talent acquisition, sourcing strategy, talent pipelines, connection between the employer value proposition and talent acquisition strategy, data-driven decisions (sourcing channel effectiveness, projecting candidate availability in the talent pipeline, tying metrics to business strategy and applied talent acquisition analytics), change strategy, leadership engagement, stakeholder analysis, communications, HC and workforce impact analysis, learning and training, process and infrastructure, project management, performance management, change execution, point of contact for staff and stakeholders, deliver HR services, and perform operational HR functions, compensation and benefits, employee and labor relations, risk management, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, building financial acumen, improving financial literacy, collaboration and retention,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security

	transparency, execution and change management, and influencing skills	building trust and transparency, execution and change management, and influencing skills	
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Example Types*: Experience/apprenticeships involving cyber HR and HC, internal rotations supporting cyber teams	▪ *Recommended*: Yes ▪ *Examples*: Experience/apprenticeships involving cyber HR and HC, internal rotations supporting cyber teams; prior information security experience	▪ *Recommended*: Yes ▪ *Examples*: Experience/apprenticeships involving cyber HR and HC, internal rotations supporting cyber teams
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Exposure to workforce policy, legislation impacting the cyber workforce, interagency advisory groups/councils, industry conferences and workshops	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include policy, legislation, interagency advisory groups/councils, industry conferences and workshops, business process reengineering, organizational design, change management, communications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include policy, legislation, interagency advisory groups/councils, industry conferences and workshops, business process reengineering)

630

CYBER POLICY AND STRATEGY PLANNER Click to Return to Work Role List		***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: STRATEGIC PLANNING AND POLICY***
Definition: Develops cyberspace plans, strategy, and policy to support and align with organizational cyberspace missions and initiatives.		
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, M.B.A., J.D. ▪ *Example Topics:* IT security management, IT management, information security, political science, business management, communications, public administration with cybersecurity experience	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, M.B.A., J.D. ▪ *Example Topics:* IT security management, IT management, information security, political science, business management, communications, public administration with cybersecurity experience	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* IT security management, IT management, information security, political science, business management, communications, public administration with cybersecurity experience
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Examples Types*: Certifications addressing analysis, assessment, control, mitigation and management of risk within a federal management and acquisition framework containing personal data; identifying, implementing and integrating management, acquisition and administrative risk methodologies for securing critical and sensitive information infrastructures, strategic planning (how to plan the plan, historical analysis, horizon analysis, visioning, environmental scans [SWOT, PEST, porters etc.], mission, vision, and value statements), planning to ensure institutional effectiveness, security policy development (policy establishes bounds for behavior, policy empowers users to do the right thing, should and shall, policy, policy versus procedure, policy needs assessment processes, organizational assumptions, beliefs and values (ABVs), relationship of mission to policy, organizational culture, comprehensive security policy assessment (using the principles of psychology to implement policy, applying the SMART method to policy, how policy protects people, organizations and information,	▪ *Recommended*: Yes ▪ *Example Topics* : Certifications addressing information privacy technology, privacy program governance (organization level, develop the privacy program framework, implement the privacy policy framework, metrics) privacy operation lifecycle (assess your organization, protect, sustain, respond), program management, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, understand basic cybersecurity concepts and definitions, apply cybersecurity architecture principles, identify components of a cybersecurity architecture, define network security architecture concepts including (topology, protocols, components, principles), understand malware analysis concepts and methodology, recognize the methodologies and techniques for detecting host-and-network-based intrusions via intrusion detection technologies, identify computer network defense and vulnerability assessment tools, including open source tools and their capabilities, understand system	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics* : Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, authentication, authorization, and accountability, cryptography foundations, information security and risk management principles, network foundations, information security governance, security program development and management, incident

	case study, the process to handle a new risk, behavior-related polices, acceptable use, ethics, warning banners, policy development process, policy review and assessment process, wrap-up), leadership and management competencies (leadership building blocks, coaching and training, change management, team development, motivating, developing the vision, leadership development, building competencies, importance of communication, self-direction, brainstorming, relationship building, teamwork concepts, leader qualities, leadership benefits), access control theory, Mitnick-Shimomura attack, network addressing, network fundamentals, network mapping and scanning, network protocol, vulnerability management overview, vulnerability scanning, web application security, windows automation, auditing and forensics, hotfixes and backups, active directory and group policy overview, wireless security, info privacy technology, privacy program governance (organization level, develop the privacy program framework, implement the privacy policy framework, metrics) privacy operation lifecycle (assess your organization, protect, sustain, respond), program management, disciplined, data-driven approach and methodology for eliminating defects	hardening, apply penetration testing principles, tools, and techniques, define network systems management principles, models, methods, and tools, understand remote access technology and systems administration concepts, distinguish system and application security threats and vulnerabilities, recognize system lifecycle management principles, including software security and usability, local specialized system requirements for safety, performance, and reliability, types of incidents (categories, responses, and timelines for responses), disaster recovery and business continuity planning, incident response and handling methodologies, security event correlation tools, how different file types can be used for atypical behavior, investigative implications of hardware, operating systems, and network technologies, as well as basic concepts, practices, tools, tactics, techniques, and procedures for processing digital forensic data, network traffic analysis methods recognize new and emerging information technology and information security technologies including (the current threat landscape, mobile devices, cloud computing and storage), project management (initiating, planning executing, monitoring and controlling, closing), business continuity and disaster recovery, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, network security, security policy and awareness, systems and application security, information security governance, and Balance Score Card Indicator (BSI)	management, BSI (Balance Score Card Indicator)
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes ▪ *Examples*: Prior Information security experience	▪ *Recommended*: Yes ▪ *Examples*: Prior Information security experience
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Involvement with policy, legislation, government/agency-wide policy groups (CNNS, NIST)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include policy lifecycle, communications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (leading change, leading people, business acumen, building coalitions)

EXECUTIVE CYBER LEADERSHIP	Click to Return to Work Role List	*Category: Oversee and Govern* *Specialty Area: Executive Cyber Leadership*
Definition: Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations (to be used for GO/FO/SES only).		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Business, public administration, applied science, computer information systems, applied software, IT-related field	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing information systems security, advanced systems management, systems certification, systems administration, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, identity theft], strategic planning, finance, and vendor management may substitute education) ▪ *Example Topics:* Computer science, computer information systems, business administration, information assurance, informatics	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. (certifications addressing information systems security, advanced systems management, systems administration, system certification, and risk analysis may substitute education) ▪ *Example Topics:* Computer science, computer information systems, business administration, information assurance, informatics
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Risk management, budgeting, acquisition and contracting, vendor training	▪ *Recommended*: Yes ▪ *Example Topics*: Operational training (e.g., scaled scope penetration test, rule sets between firewall and intrusion detection system)—integration and operation, network security vulnerability	▪ *Recommended*: Yes ▪ *Example Topics*: Executive core qualifications (leading change, leading people, business acumen, building coalitions), managerial and operational workforce needs, conveying risk to stakeholders, technical, organizational behavior and change, risk management training, executive training, information system security manager
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, information security governance, security program development and management, incident management, cybersecurity leadership, system	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, information, incident management

	security, network infrastructure, access control, cryptography, assessments and audits, organizational security, managing, maintaining, troubleshooting, installing, network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, information systems security, system certification, risk analysis		
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: 4–7 years of experience in a significant security role, operational management experience in general IT disciplines (e.g., network technician, service desk support, desktop support, entry level software development, tier 1 security operations center work/triage), experience in physical security	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 7–10 years operational management experience involving penetration testing, security assessments, T2/T3 security operations, security, network operations, fundamental operations, privacy assessments, privacy testing, contracting, managing and changing business processes, aligning strategy and performance metrics to organizational mission, contracting office representative, physical security operations and training, prior rotations	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 10–15+ years high-level organizational and business strategy (e.g., staffing and planning, budget formulation, long-term risk management and risk outlay planning), IT strategic planning and understanding risk, experience with classified or highly sensitive environments (background investigations, high security), developing people (leading and organizing, leading change management)
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 20 hours annually (may include learning how to lead change, rotations, self-awareness training, contributing to information security publications, webinars, internal organization-specific leadership training, seminars)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include experience building culture, interagency joint duties, work rotations, detail(s), publishing articles, maintain credentials)	▪ *Recommended*: Yes ▪ *Examples*: 40–80 hours annually (may include continued education, attending and presenting new ideas at conferences [i.e., thought leadership])

631

PROGRAM MANAGER Click to Return to Work Role List Definition: Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: ACQUISITION AND PROGRAM/PROJECT MANAGEMENT***
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Associate's, bachelor's (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Hacking trends	▪ *Recommended*: Yes ▪ *Example Topics*: Hacking trends, contracting, business cost and financial management, applied leadership in projects and programs, and network security vulnerability	▪ *Recommended*: Yes ▪ *Example Topics*: Leadership, program management, strategy, business, cost and financial management, hacking trends, online training, and publications
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications that address requirements development and management processing, systems engineering, testing and evaluation, lifecycle logistics, contracting, business, cost, financial management, leadership, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management,	▪ *Recommended*: Yes ▪ *Example Topics* : Certifications that address project management (initiating, planning executing, monitoring and controlling, and closing), requirements development and management processing, systems engineering, testing and evaluation, lifecycle logistics, contracting, business, cost, financial management, leadership, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, stakeholder management, governance, system security, network	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address strategic program management, program lifecycle (initiating, planning, executing, controlling, and closing), benefits management, stakeholder management, governance, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security

	stakeholder management, governance, and a data-driven approach and methodology for eliminating defects	infrastructure, access control, cryptography, assessments and audits, and organizational security	
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Example Types*: 3+ years of program management experience with a budget of $10 million to $50 million, project management, mentoring, soft skills, 6-month rotations	▪ *Recommended*: Yes ▪ *Examples*: 5+ years of program management experience with a budget of $50 million to $100 million, handling day-to-day responsibilities, information assurance	▪ *Recommended*: Yes ▪ *Examples*: 7+ years of program management experience with a budget of $100 million+, overseeing all assignments involving the program, managing large and complex projects, coach others, presenting at conferences, mentoring other managers
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 20–60 hours annually (may include maintaining certifications, attending symposium/conferences, self-directed study, and taking higher education coursework)	▪ *Recommended*: Yes ▪ *Examples*: 40–80 hours annually (may include conferences, maintaining certification, on-the-job training for next level/increasing responsibilities, developmental assignments, shadowing, rotations, seminars, conferences, brown bags, and presentations)	▪ *Recommended*: Yes ▪ *Examples*: 40–120 hours annually (may include holding elected/appointed positions [e.g., committee leadership roles or attending and/or presenting at educational conferences or meetings], mentoring, and maintaining certifications)

632

IT PROJECT MANAGER Click to Return to Work Role List Definition: Directly manages it projects to provide a unique service or product.			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: ACQUISITION AND PROGRAM/PROJECT MANAGEMENT***
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: No degree, associate's, bachelor's, master's ▪ *Example Topics:* Business, cybersecurity, math, engineering and technology, information assurance, and project management	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute education) ▪ *Example Topics:* Engineering and technology, information assurance, project management	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, five-step IT alignment process to create strategic business value for your company, building a business case beyond ROI, principles of leadership and how the CIO uses them to strengthen the IT alignment process, and corporate political communications/political capital may substitute education) ▪ *Example Topics:* Project management, M.B.A. (business administration, engineering and technology, and information assurance)
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: IT, workplace-provided training, contract writing, basics of project management, leadership courses, technical training, and public speaking	▪ *Recommended*: Yes ▪ *Example Topics*: Workplace-provided training, online training, workshops, boot camps for IT project management, leadership, public speaking, network security vulnerability	▪ *Recommended*: Yes ▪ *Example Topics*: IT, project management, leadership, budget, risk management, public speaking, and information system security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, and project	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address project management (initiating, planning executing, monitoring and controlling, and closing), security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address project management (initiating, planning executing, monitoring and controlling, closing), security and risk management, asset security, security engineering, communications and network security, identity and access management,

	management (initiating, planning executing, monitoring and controlling, closing)	security operations, software development security, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	security assessment and testing, security operations, and software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 6 months–5 years of experience leading and directing projects, leading working groups, networking in other organizations and within own organization	▪ *Recommended*: Yes ▪ *Examples*: 1–7 years of developing skills in IT and project management, full-time work experience in security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security; 10 years of experience leading working groups, large complex projects, networking in other organizations and within your own organization, supervised on-the-job training with privileged information assurance	▪ *Recommended*: Yes ▪ *Examples*: 8–15+ years working in IT/PM role, successfully lead and directed large complex projects and teams, information assurance, and information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Professional memberships, forums, roundtables; online training courses, and maintaining certifications	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include professional memberships, forums, lunch and learns, roundtables, online training courses, and maintaining certifications)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, rotations, professional memberships, maintaining certifications, speaking at conferences)

633

PRODUCT SUPPORT MANAGER Click to Return to Work Role List			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: ACQUISITION AND PROGRAM/PROJECT MANAGEMENT***
Definition: Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, audit management, information security core concepts [access control, social engineering, phishing attacks, identity theft], strategic planning, finance, and vendor management may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's, master's, Ph.D. (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute for education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Network security vulnerability	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information system security
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Types*: Certifications that address any topics related to IT	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, and managing network environments, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, and monitoring of security controls	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, security program development and management, information security incident management, change management and incident handling for managers, common attacks and malware, managing access control, managing defense in depth and security policy, managing (disaster recovery and contingency planning, employees and total cost of ownership, operational security, physical security and facility safety, privacy and web security, risk and ethics, security awareness and protecting intellectual property, the network infrastructure, quality and growth of the security organization, cryptography, vulnerabilities, wireless

			security, network and endpoint security technologies), network protocols for managers, project management and business situational awareness, selling and managing the mission, enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines, technical integration of enterprise components, strategic program management, program lifecycle (initiating, planning, executing, controlling, and closing), benefits management, stakeholder management, and governance
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Example Types*: 2+ years of work experience with IT experience	▪ *Recommended*: Yes ▪ *Examples*: 2+ work years of experience in IT/ information assurance	▪ *Recommended*: Yes ▪ *Examples*: Management, training, information assurance, and information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Mentoring	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include attending conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include interagency rotational programs, and attending and speaking at conferences)

634

IT INVESTMENT/PORTFOLIO MANAGER Click to Return to Work Role List Definition: Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: ACQUISITION AND PROGRAM/PROJECT MANAGEMENT***
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Finance or IT	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's (certifications addressing advanced systems management, systems administration, system certification, risk analyst, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute education)	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Master's, Ph.D. (certifications addressing advanced systems management, systems administration, system certification, risk analyst, five-step IT alignment process to create strategic business value for your company, building a business case beyond ROI, principles of leadership and how the CIO uses them to strengthen the IT alignment process, and corporate political communications and corporate political capital may substitute education)
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Acquisition planning, market research (understanding the marketplace), defining government requirements, effective pre-award communication, proposal evaluation, contract negotiation, contract administration management, effective inspection and acceptance, contract quality assurance and evaluation, contract closeout, contract reporting, business acumen and communications skill sets, and Contracting Officer Representative Tracking (CORT) tool	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Network security vulnerability	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information system security
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, system security, access control, cryptography, assessments	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, managing network environments,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, security

	and audits, organizational security, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security	system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, strategic program management, program lifecycle (initiating, planning, executing, controlling, and closing), benefits management, stakeholder management, and governance	program development and management, information security incident management, change management and incident handling for managers, common attacks and malware, managing (access control, defense in depth and security policy, disaster recovery and contingency planning, employees and total cost of ownership, operational security, physical security and facility safety, privacy and web security, risk and ethics, security awareness and protecting intellectual property, the network infrastructure, quality and growth of the security organization, the use of cryptography, vulnerabilities, wireless security), network and endpoint security technologies, network protocols for managers, project management and business situational awareness, selling and managing the mission, enterprise security, risk management and incident response, research and analysis, integration of computing, communications, and business discipline, technical integration of enterprise components, strategic program management, program lifecycle (initiating, planning, executing, controlling, and closing), benefits management, stakeholder management, and governance
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Macros, shadowing, rotations, mentorship or apprenticeship, management succession program, and legislation	▪ *Recommended*: Yes ▪ *Examples*: Interagency rotation, mentor/mentee, information assurance	▪ *Recommended*: Yes ▪ *Examples*: 2+ years of experience Interagency rotation, knowledge sharing, mentoring, information assurance, and information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 10 hours a year	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include workshops and conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include learning and implementing best practices across enterprise, and thought leadership)

635

IT PROGRAM AUDITOR Click to Return to Work Role List			***CATEGORY: OVERSEE AND GOVERN*** ***SPECIALTY AREA: ACQUISITION AND PROGRAM/PROJECT MANAGEMENT***
Definition: Conducts evaluations of an IT program or its individual components to determine compliance with published standards.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications systems administration, risk analysis, governance, security risk management, controls, audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's (certifications addressing advanced systems management, systems administration, system certification, risk analysis, building a business case beyond ROI, principles of leadership and how the CIO uses them to strengthen the IT alignment process, and corporate political communications and corporate political capital may substitute education) ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, internal auditing, audit planning, information systems, Sarbanes-Oxley (SOX), accounting, risk assessment, project management, business process, and control objectives for information and related technologies (COBIT)	▪ *Recommended*: Yes ▪ *Example Topics*: Information system security, internal auditing, audit planning, information systems, SOX, accounting, risk assessment, project management, business process, and COBIT
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: Prior information assurance experience	▪ *Recommended*: Yes ▪ *Examples*: Prior information assurance experience
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

636

CYBER DEFENSE ANALYST Click to Return to Work Role List ***CATEGORY: PROTECT AND DEFEND***
SPECIALTY AREA: CYBER DEFENSE ANALYSIS

Definition: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: System administrator, basic cyber analyst/operator, interactive ON-NET Operator, intermediate cyber, hunt methodologies	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability technician, advanced network analyst, basic cyber analyst/operator, network traffic analysis, information security, information systems, network security, information assurance, trouble shooting, security operations, cryptography	▪ *Recommended*: Yes ▪ *Example Topics*: Hunt methodologies, information security, information systems, network security, information assurance, trouble shooting, security operations, cryptography
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing incident handling (identification, overview, and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attacks, incident handing (containment, eradication, recovery, and lessons learned), network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing incident handling (identification, overview, and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attaches, incident handing (containment, eradication, recovery, and lessons learned), network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Introductory information assurance, networks, sensor operations, network/data analysis,	▪ *Recommended*: Yes ▪ *Examples*: Information assurance, networks, radio communications, network/data analysis, packet capture	▪ *Recommended*: Yes ▪ *Examples*: Network/data analysis, packet capture analysis, malware detection, custom intrusion signature development, advanced information assurance

	packet capture analysis, hunts methodologies, intelligence analysis	analysis, malware detection, custom intrusion signature development concepts	
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include attending security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include attending security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include attending security conferences)

637

CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST Click to Return to Work Role List

CATEGORY: PROTECT AND DEFEND
SPECIALTY AREA: CYBER DEFENSE INFRASTRUCTURE SUPPORT

Definition: Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: System administrator, basic cyber analyst/operator training, security essentials, intermediate cyber, hunt methodologies	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, advanced network analysis, basic cyber analysis/operations, network traffic analysis, Intermediate cyber, hunt methodologies	▪ *Recommended*: Yes ▪ *Example Topics*: Industry-standard training (focused in one of the certifications areas listed in the credential/certifications section)
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, security program development and management, information security incident management, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Network infrastructure, firewalls, IDS/IPS, application proxies, systems administration, network storage, enterprise authentication, backups and data retention, information assurance	▪ *Recommended*: Yes ▪ *Examples*: Network infrastructure, firewalls, IDS/IPS, application proxies, systems administration, network storage, enterprise authentication, backups and data retention, information assurance	▪ *Recommended*: Yes ▪ *Examples*: Network infrastructure, firewalls, IDS/IPS, application proxies, systems administration, network storage, enterprise authentication, backups and data retention
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)

638

CYBER DEFENSE INCIDENT RESPONDER	Click to Return to Work Role List	***CATEGORY: PROTECT AND DEFEND*** ***SPECIALTY AREA: INCIDENT RESPONSE***
Definition: Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's, bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, master's, Ph.D. *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: System administrator, basic cyber analysis and operations	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, advanced network analysis, basic cyber analysis/operations, network traffic analysis, cyber operator, computer forensics invest and response, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography	▪ *Recommended*: Yes ▪ *Example Topics*: Intermediate cyber, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, Wireshark fundamentals	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing incident handling (identification, overview and preparation) buffer overflow, client attacks, covering tacks (networks, systems), denial of service attaches, network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques, and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, bots, and bot-nets	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, filesystem structure and analysis, artifact analysis

EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Malware analysis, digital forensics, data/network analysis, information assurance technician, incident handling	▪ *Recommended*: Yes ▪ *Examples*: Malware analysis, digital forensics, data/network analysis, penetration testing, information assurance, leading incident handling	▪ *Recommended*: Yes ▪ *Examples*: Malware analysis, digital forensics, data/network analysis, penetration testing, information assurance, trends analysis, quality control analysis, information assurance vulnerability management
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include participation in annual security conferences)

639

VULNERABILITY ASSESSMENT ANALYST — Click to Return to Work Role List			***CATEGORY: PROTECT AND DEFEND*** ***SPECIALTY AREA: VULNERABILITY ASSESSMENT AND MANAGEMENT***
Definition: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Systems administration, basic cyber analysis/operations, intermediate cyber core	▪ *Recommended*: Yes ▪ *Example Topics*: Network security vulnerability, advanced network analysis, basic cyber analysis/operations, network traffic analysis, intermediate cyber core, information security, troubleshooting, information systems, quality assurance and control, SQL, network security	▪ *Recommended*: Yes ▪ *Example Topics*: Information system security management, information security, troubleshooting, information systems, quality assurance and control, SQL, network security
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure	▪ *Recommended*: Yes ▪ *Example Topics:* Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Prior experience in information assurance, incident handling, vulnerability management and vulnerability analysis, and assistance programs	▪ *Recommended*: Yes ▪ *Examples*: Prior experience in information assurance, incident handling, information assurance vulnerability management and analysis, and assistance programs	▪ *Recommended*: Yes ▪ *Examples*: Prior experience in advanced information assurance and handling incidents of greater organizational impact
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, conferences, webinars, or rotations)

640
641
642

WARNING ANALYST	Click to Return to Work Role List	***CATEGORY: ANALYZE*** ***SPECIALTY AREA: THREAT ANALYSIS***
Definition: Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's, Master's, PhD
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Cyber operations fundamentals, operational intelligence analysis	▪ *Recommended*: No ▪ *Example Topics*: Cyber operations fundamentals, operational intelligence analysis, and reporting	▪ *Recommended*: Yes ▪ *Example Topics*: Policies that enforce cyber and cyber-physical systems, synergistic cyber security (ranging from the effective use of hardware and the application of security in system architectures to effective user interfaces and clear documentation), developing and deploying procedures for securing information assets on IT systems in the face of cyber-attacks, network security threats and vulnerabilities and analyze protocols creating protected distributed systems, cyber operations fundamentals, operational intelligence analysis, and reporting
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Examples*: Certifications addressing advanced IDS concepts, application protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment, IDS rules, IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, filters, UDP and ICMP, focus on new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, information systems audit process, IT governance and management, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets	▪ *Recommended*: Yes ▪ *Examples*: Certifications addressing advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment, IDS rules, IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, focus on new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, information systems audit process, IT governance and management, information systems acquisition, development, implementation, operations,	▪ *Recommended*: Yes ▪ *Examples*: Certifications addressing new attack vectors (emphasis on cloud computing technology, emphasis on mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, information, security program development and management, information security incident management, risk identification, assessment and evaluation, risk response, risk monitoring, information systems control design and implementation, and control monitoring and maintenance

		maintenance, and service management, and protection of information assets	
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Intelligence analysis	▪ *Recommended*: Yes ▪ *Examples*: Supervised on the job training JQR (CND Intelligence Analysis and Assessments) JQR (CND Intelligence Analysis Open Source Research)	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

643

ALL-SOURCE ANALYST

Click to Return to Work Role List

CATEGORY: ANALYZE
SPECIALTY AREA: ALL-SOURCE ANALYSIS

Definition: Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Bachelor's ▪ *Example Topics:* Computer science, engineering, math	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, PhD
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Database queries, vendor trainings transmission control protocol / internet protocol (TCP / IP), IP addressing, MAC addresses, PEN testing, computer forensics, privacy, standards, policy training, offered trainings	▪ *Recommended*: Yes ▪ *Example Topics*: Data and privacy laws (e.g., NIST controls and standards, policy), information security, information systems, network security, information assurance, Unix, trouble shooting, security operations, cryptography, transmission control protocol / internet protocol (TCP / IP)	▪ *Recommended*: Yes ▪ *Example Topics*: Intelligence skills, data flow architecture, firewalls, data and privacy laws (e.g. NIST controls and standards, policy), programing languages, vendor trainings, information security, information systems, network security, information assurance, Unix, trouble shooting, security operations, cryptography, transmission control protocol / internet protocol (TCP / IP)
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms, and tablet computers), new vulnerabilities, existing threats to operating environments, auditing, information systems audit process, IT governance and management, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets, pen testing, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, managing, maintaining,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing project management (initiating, planning executing, monitoring and controlling, closing), focus on new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT governance and management, information systems acquisition, development, implementation, operations, maintenance, and service management, and protection of information assets, information security governance,

	troubleshooting, installing, configuring basic network infrastructure, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support		information risk management, security program development and management, incident management, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, U.S. government privacy laws (privacy definitions and principles, The Privacy Act and the E-Government Act, other laws and regulations affecting U.S. government privacy practice, privacy and the federal government intelligence community, other federal information privacy laws and authorities affecting government practice), U.S. government privacy practices (privacy program management and organization, records management, auditing and compliance monitoring)
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Database, writing queries, tool specific training and experience, programming	▪ *Recommended*: Yes ▪ *Examples*: Interdepartmental rotations and external rotations, receiving mentoring, viewing and analyzing data	▪ *Recommended*: N/A (see prior levels)
CONTINUOUS LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Conferences	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Mentoring

644

645

CYBER INTEL PLANNER	Click to Return to Work Role List	***CATEGORY: COLLECT AND OPERATE*** ***SPECIALTY AREA: CYBER OPERATIONAL PLANNING***
Definition: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, PhD
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Cyber analysis, advanced cyber warfare, basic cyber analysis/operations, information warfare	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced cyber warfare, network attacks, cyber operations	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced cyber warfare, network attacks, cyber operations
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security	▪ *Recommended*: Yes ▪ *Examples*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

CYBER OPS PLANNER	Click to Return to Work Role List	***CATEGORY: COLLECT AND OPERATE*** ***SPECIALTY AREA: CYBER OPERATIONAL PLANNING***
Definition: Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Joint cyber analysis, joint advanced cyber warfare, cyber network operations	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced cyber warfare, network attack, cyber operations, information security, troubleshooting, information systems, business process, risk management, SQL, Unix	▪ *Recommended*: Yes ▪ *Example Topics*: Advanced cyber warfare, network attacks, cyber operations, information security, troubleshooting, information systems, business process, risk management, SQL, Unix
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms, and tablet computers), new vulnerabilities, existing threats to operating environments, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

PARTNER INTEGRATION PLANNER Click to Return to Work Role List ***CATEGORY: COLLECT AND OPERATE***
SPECIALTY AREA: CYBER OPERATIONAL PLANNING

Definition: Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, Bachelor's	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's, Bachelor's, Master's, PhD
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Communication skills, understanding organizational culture, cyber operations, advanced cyber warfare	▪ *Recommended*: Yes ▪ *Example Topics*: Communication skills, understanding organizational culture, negotiation skills, department structures, advanced cyber warfare, network attack, cyber operations	▪ *Recommended*: Yes ▪ *Example Topics*: Communication skills, understanding organizational culture, negotiation skills, department structures, advanced cyber warfare, network attack, cyber operations
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Conferences	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Presenting at conferences, receiving mentoring from an experienced manager
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 – 80 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 – 120 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

650

CYBER CRIME INVESTIGATOR Click to Return to Work Role List			***CATEGORY: INVESTIGATE*** ***SPECIALTY AREA: CYBER INVESTIGATION***
Definition: Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.			
	Entry	**Intermediate**	**Advanced**
EDUCATION	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, computer forensics, Linux, Unix, TCP/IP, malware analysis, Python, network security, cryptography	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Information security, computer forensics, Linux, Unix, TCP/IP, malware analysis, Python, network security, cryptography
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, protection of information assets, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, information security governance, information security program development and management, information security incident management	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, protection of information assets, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, information security governance, information security program development and management, information security incident management
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

651

FORENSICS ANALYST	Click to Return to Work Role List	***CATEGORY: INVESTIGATE*** ***SPECIALTY AREA: DIGITAL FORENSICS***
Definition: Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, including digital media and logs associated with cyber intrusion incidents.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types*: Associate's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D.
TRAINING	▪ *Recommended*: Yes ▪ *Example Topics*: Basic cybersecurity analysis/operations, systems administration	▪ *Recommended*: Yes ▪ *Example Topics*: Basic cybersecurity analysis/operations, network security vulnerability technical skills	▪ *Recommended*: Yes ▪ *Example Topics*: Basic cybersecurity analysis/operations, network security vulnerability technical skills
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, incident handling (identification, overview and preparation) buffer overflow, client attacks, denial of service attacks, incident handing (containment, eradication, recovery, and lessons learned), network attacks, password attacks, reconnaissance, scanning (discovery and mapping techniques and defense), session hijacking and cache poisoning, techniques for maintaining access, web applications attacks, worms, and bots	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, analysis of file and program activity, acquisition, preparation and preservation of digital evidence, analysis of user communications, fundamental digital forensics, hose and application event log analysis, browser forensics, browser artifacts analysis, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, wireshark fundamentals	▪ *Recommended*: Yes ▪ *Example Topics*: Certification addressing analysis of malicious document files, analysis of protected executables, analysis of web-based malware, common Windows malware characteristics in assembly, in-depth analysis of malicious browser scripts, in-depth analysis of malicious executables, malware analysis using memory forensics, malware code and behavioral analysis fundamentals
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Learning addressing sensor operations, information assurance, networks, intelligence analysis	▪ *Recommended*: Yes ▪ *Examples*: Learning addressing information assurance, networks, threats	▪ *Recommended*: Yes ▪ *Examples*: Learning addressing information assurance, malware
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A

652

CYBER DEFENSE FORENSICS ANALYST	Click to Return to Work Role List	***CATEGORY: INVESTIGATE*** ***SPECIALTY AREA: DIGITAL FORENSICS***
Definition: Analyzes digital evidence and investigates computer security incidents to derive information in support of system/network vulnerability mitigation.		

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types*: Associate's	▪ *Recommended*: Yes ▪ *Example Types*: Bachelor's	▪ *Recommended*: Yes ▪ *Example Types*: Master's, Ph.D.
TRAINING	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Basic cybersecurity analysis/operations, systems administration, information security	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Basic cybersecurity analysis/operations, systems administration, information security, vendor, troubleshooting, business processes, information systems, SQL, Linux, risk management, Java	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Basic cybersecurity analysis/operations, systems administration, information security, vendor, troubleshooting, business process, information systems, SQL, Linux, risk management, Java
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, new attack vectors (emphasis on cloud computing technology, mobile platforms, and tablet computers), new vulnerabilities, existing threats to operating environments, incident handling (identification, overview, and preparation), buffer overflow, client attacks, denial of service attacks, incident handing (containment, eradication, recovery, and lessons learned), network attacks, password attacks, reconnaissance, scanning (discovery and mapping, techniques, and defense), session hijacking and cache poisoning, techniques for maintaining access, web	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing identification of malicious system and user activity, incident response in an enterprise environment, incident response process and framework, timeline artifact analysis, timeline collection, timeline processing, volatile data collection, analysis of profiling of systems and devices, analysis of file and program activity, acquisition, preparation, and preservation of digital evidence, analysis of user communications, advanced IDS concepts, applications protocols, concepts of TCP/IP and the link layer, DNS, fragmentation, IDS fundamentals and initial deployment (e.g., snort, bro), IDS rules (e.g., snort, bro), IPv6, network architecture and event correlation, network traffic analysis and forensics, packet engineering, silk and other traffic analysis tools, TCP, Tcpdump filters, UDP and ICMP, wireshark fundamentals, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing analysis of malicious document files, analyzing protected executables, analyzing web-based malware, common windows malware characteristics in assembly, in-depth analysis of malicious browser scripts, in-depth analysis of malicious executables, malware analysis using memory forensics, malware code and behavioral analysis fundamentals, Windows assembly code concepts for reverse-engineering, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information systems audit process, IT government and management, information systems acquisition, development, implementation, operations, maintenance, and service management, protection of information

	applications attacks, worms, bots, and bot-nets	maintenance, and service management, protection of information assets, information security governance, information security program development and management, information security incident management, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, U.S. government privacy laws (privacy definitions and principles, the Privacy Act and the E-Government Act, other laws and regulations affecting U.S. government privacy practice, privacy, and the federal intelligence community, other federal information privacy laws and authorities affecting government practice), U.S. government privacy practices (privacy program management and organization, records management, auditing and compliance monitoring)	assets, information security governance, information security program development and management, information security incident management, system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, U.S. government privacy laws (privacy definitions and principles, the Privacy Act and the E-Government Act, other laws and regulations affecting U.S. government privacy practice, privacy, and the federal intelligence community, other federal information privacy laws and authorities affecting government practice), U.S. government privacy practices (privacy program management and organization, records management, auditing, and compliance monitoring)
EXPERIENTIAL LEARNING	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Learning addressing sensor operations, information assurance, intelligence analysis	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Learning addressing information assurance, networks, threats	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: Learning addressing advanced information assurance, malware
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A

Appendix B - References

[1] NIST Special Publication (SP) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, August 2017, https://doi.org/10.6028/NIST.SP.800-181

[2] Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017) , https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[3] CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market. [Website], http://cyberseek.org/

[4] Classification & Qualifications GENERAL SCHEDULE QUALIFICATION STANDARDS [Website], https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/#url=List-by-Occupational-Series

[5] Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals [Website], https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf

[6] Federal Virtual Training Environment (FedVTE) [Website], https://fedvte.usalearning.gov/