NICE Cybersecurity Workforce Framework (NCWF)

National Initiative for Cybersecurity Education (NICE)

Bill Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte
NICE Cybersecurity Workforce Framework (NCWF)

National Initiative for Cybersecurity Education (NICE)

Bill Newhouse
Applied Cybersecurity Division
Information Technology Laboratory

Stephanie Keith
Cyber Workforce Strategy & Policy Division
Office of the Deputy DoD Chief Information Officer

Benjamin Scribner
Cyber Education and Awareness Branch
DHS National Protection and Programs Directorate

Greg Witte
G2, Inc.
Annapolis Junction, MD

November 2016
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-181
CODEN: NSPUE2

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 http://csrc.nist.gov/publications.

Public comment period: November 2, 2016, through January 6, 2017

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002
Email: ncwf@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).
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. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication describes the NICE Cybersecurity Workforce Framework (NCWF), the product of many years of collaboration regarding workforce training and education. NCWF provides a fundamental reference resource for describing and sharing information about cybersecurity work roles, the discrete tasks performed by staff within those roles, and the knowledge, skills, and abilities (KSAs) needed to complete the tasks successfully. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NCWF improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NCWF is a resource from which organizations or sectors can develop additional publications or tools focused on defining or providing guidance on aspects of workforce development, planning, training, and education.

Keywords

Ability; cybersecurity; cyberspace; education; knowledge; role; skill; task; training; work role.
Acknowledgements

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. We appreciate the leadership and work of Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). In particular, we also wish to thank Lynne Clarke, Ryan Farr, Jodi Guss, Lori Pfannenstein, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matt Smith, Bluma Sussman, Baris Yakin, Onika Williams, and Montana Williams for their individual contributions to this publication.

The first NCWF was posted for public comment in September of 2012 and published in April 2013 as NCWF version 1.0 [1]. The authors wish to recognize Dr. Jane Homeyer, Anne Quigley, Rex Min, Maya Yankelevich, and Peggy Maxson for leading its development, and we wish to recognize Roy Burgess for his leadership in the development of NCWF version 2.0 [2].

Finally, the authors also respectfully acknowledge the seminal work in computer security that dates back to the 1960s. The vision, insights, and dedicated efforts of those early pioneers in computer security serve as the philosophical and technical foundation for the tasks, knowledge, skills, and abilities noted in this publication to address the critically important problem of cybersecurity workforce.

Note to Reviewers

With the continuing frequency, intensity, and adverse consequences of cybersecurity attacks, disruptions, hazards, and threats to federal, state, and local governments, the military, businesses, industry, and critical infrastructure, the need for a workforce prepared to deploy, provide, maintain, and develop the requisite cybersecurity has never been more important to the economic and national security interests of the United States. - Bill Newhouse, Deputy Director, NICE

Trademark Information

All trademarks or registered trademarks belong to their respective organizations.
Executive Summary

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire, prepared to protect our nation from existing and emerging cybersecurity challenges. Despite increasing awareness and global focus on cybersecurity, many managers report a shortage of skilled cybersecurity workers and need assistance with hiring qualified staff to fill critical security gaps. To address these needs, this publication describes the NICE Cybersecurity Workforce Framework (NCWF).

As the threats to cybersecurity and the protections implemented grow and evolve, a cybersecurity workforce must be prepared to adapt, design, develop, implement, maintain, measure, and understand all aspects of cybersecurity. A cybersecurity workforce includes not only technically focused staff but those who apply knowledge of cybersecurity and its inherent challenges when preparing their organization to successfully implement its mission. A knowledgeable and skilled cybersecurity workforce can implement and maintain protections and take actions to meet our nation’s needs.

This publication serves as a fundamental reference to support a workforce capable of meeting an organization’s cybersecurity needs. It describes how the NCWF provides organizations with a common, consistent lexicon to categorize and describe cybersecurity work. The document defines the NCWF components, namely Categories, Specialty Areas, and Work Roles. Finally, it describes a superset of cybersecurity Tasks for each work role and the Knowledge, Skills, and Abilities (KSAs) demonstrated by a person whose cybersecurity position includes each work role. Based upon these components, the common lexicon provided by the NCWF enables consistent organization and communication about cybersecurity work.

The NCWF can be viewed as a cybersecurity workforce dictionary, and consumers of the NCWF can reference it for different workforce development, education, and/or training purposes. For instance, it provides a starting point and helps set standards for developing academic pathways, career pathways, position descriptions, and training content. The NCWF helps to ensure our nation is able to educate, recruit, train, develop, and retain a highly qualified cybersecurity workforce. It serves several key audiences within the cybersecurity community including:

- **Employers**, to help assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions;
- **Current and future employees**, to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity
jobs and positions. The NCWF also enables staffing specialists and guidance counselors to use the NCWF as a resource to support these employees or job seekers;

- **Training and certification providers** who desire to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs;

- **Education providers** who may use the NCWF as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and Tasks described; and

- **Technology providers** who can identify cybersecurity Work Roles and specific Tasks and KSAs associated with services and hardware/software products they supply.

As a mechanism to organize information technology (IT), cybersecurity, and cyber-related work, the NCWF helps organizations to organize roles and responsibilities through the following components:

- **Categories** – A high-level grouping of common cybersecurity functions;

- **Specialty Areas** – Distinct areas of cybersecurity work;

- **Work Roles** – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks;

- **Tasks** – Specific work activities that could be assigned to a professional working in one of the NCWF’s Work Roles; and

- **Knowledge, Skills, and Abilities (KSAs)** – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

The NCWF components work together to describe the range of cybersecurity work, from a high level to the very granular. Each Category contains Specialty Areas, each of which contains one or more Work Roles. Each Work Role is composed of numerous Tasks and KSAs. Providing this range of detail helps organizations to systematically build their cybersecurity workforce, which, in turn, enables improved performance, cost-effective workforce management, and continuous readiness.

While some of the NCWF is based on federal government programs, any organization with cybersecurity workforce needs will benefit from the standards described and can customize the NCWF as needed.

Using the NCWF as described above will help strengthen an organization’s cybersecurity workforce. Investment in the existing workforce, such as through initiatives focused on training and retaining existing talent, will help the organization to prepare for and realize its risk management objectives. The common language provided by the NCWF also helps bridge workforce needs to external frameworks, such as the Cybersecurity Framework (CSF) [3], the U.S. Department of Labor Competency Models [4], the U.S. Department of Education Employability Skills Framework [5], and the National Security Agency (NSA)/Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units [6].
The NCWF builds upon decades of industry research into how to effectively manage the risks to valuable organizational electronic and physical information. Cybersecurity tactics are ever-changing, always identifying new ways to gain information advantage through technology. As we evolve, the ways we perform cybersecurity functions continue to evolve, as must the components of the NCWF. As part of an ongoing collaborative approach, NICE will periodically consider recommendations received and will update the NCWF publication(s). Additionally, new reference materials or tools will be developed to cross-reference elements of the NCWF. To the extent possible, digital reference materials will be posted to the NICE website as an aid to applying and utilizing NCWF and associated materials.
# Table of Contents

Executive Summary ..................................................................................................... iv  

1 Introduction ............................................................................................................ 1  
  1.1 NCWF Background .......................................................................................... 2  
  1.2 Purpose and Applicability ............................................................................... 3  
  1.3 Audience/NCWF Consumers .......................................................................... 3  
     1.3.1 Employers ............................................................................................ 3  
     1.3.2 Current and Future Cybersecurity Workers .......................................... 5  
     1.3.3 Educators/Trainers ............................................................................... 5  
     1.3.4 Technology Providers ......................................................................... 5  
  1.4 Organization of this Special Publication .......................................................... 5  

2 NCWF Components and Relationships ................................................................ 7  
  2.1 Components of the NCWF .............................................................................. 7  
     2.1.1 Categories ............................................................................................ 7  
     2.1.2 Specialty Areas .................................................................................... 7  
     2.1.3 Work Roles ........................................................................................... 7  
     2.1.4 Tasks .................................................................................................... 7  
     2.1.5 Knowledge, Skills, and Abilities ............................................................ 7  
  2.2 NCWF Component Relationships ................................................................... 8  

3 Applying the NCWF ................................................................................................ 9  
  3.1 Identification of Cybersecurity Workforce Needs ............................................ 9  
  3.2 Education and Training of Cybersecurity Workforce Members ..................... 10  
  3.3 Recruitment and Hiring of Highly Skilled Cybersecurity Talent .................... 10  
  3.4 Retention and Development of Highly Skilled Cybersecurity Talent ............. 11  
  3.5 Cybersecurity Framework (CSF) .................................................................. 12  
     3.5.1 Example Integration of CSF with NCWF ............................................ 14  

4 Future Revision Process ..................................................................................... 17  
  4.1 Additional Concepts for Future Consideration .............................................. 17  

List of Appendices

Appendix A— Listing of NCWF Elements ................................................................. 19  
  A.1 NCWF Workforce Categories ....................................................................... 19  
  A.2 NCWF Specialty Areas ............................................................................... 20
A.3 NCWF Work Roles

A.4 NCWF Work Role Tasks

A.5 NCWF Knowledge Descriptions

A.6 NCWF Skills Descriptions

A.7 NCWF Ability Descriptions

Appendix B—Work Role Detail Listing

Appendix C—Acronyms

Appendix D—References

List of Tables

Table 1 - Crosswalk of NCWF Workforce Categories to CSF Functions
Table 2 - NCWF Workforce Categories
Table 3 - NCWF Specialty Areas
Table 4 - NCWF Work Roles
Table 5 - NCWF Work Role Tasks
Table 6 - NCWF Knowledge Descriptions
Table 7 - NCWF Skills Descriptions
Table 8 - NCWF Ability Descriptions
1 Introduction

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire, prepared to protect our nation from existing and emerging cybersecurity challenges.

There are national activities that focus on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure, enterprise, and operational technology systems and networks. As the threats to cybersecurity and the protections implemented grow and evolve, a cybersecurity workforce must be prepared to adapt, design, develop, implement, maintain, measure, and understand all aspects of cybersecurity. A cybersecurity workforce includes not only technically focused staff but those who apply knowledge of cybersecurity and its inherent challenges when preparing their organization to successfully implement its mission. A knowledgeable and skilled cybersecurity workforce can implement and maintain the protections and take actions to meet our nation’s needs.

Today’s systems and networks are complex assemblages of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations with the capability to process, store, and transmit information in a timely, more secure manner to support various missions and business functions. The degree to which organizations have come to depend upon these systems and networks to conduct routine, important, and critical missions and business functions means that the protection of the underlying systems and environments of operation is paramount to the success of the organization.

The selection of appropriate security and privacy controls for information systems continues to be an important task that can have significant implications on the operations and assets of an organization as well as the welfare of individuals. Finding qualified individuals with the Knowledge, Skills, And Abilities (KSAs) who can select, maintain, assess, implement, and upgrade the appropriate security and privacy controls is a challenge being addressed by more and more organizations who now understand that cybersecurity risks need to be addressed by a capable and ready cybersecurity workforce.

Understanding how to develop and maintain a workforce that allows an organization to focus on the cybersecurity risks to its operations and assets, to individuals, to other organizations, and to the nation is vital. A prepared cybersecurity workforce is also essential in a globally interconnected digital information and communications infrastructure that underpins almost
every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security.

1.1 NCWF Background

The concept for the NCWF began before the establishment of NICE and grew out of the recognition that the cybersecurity workforce (federal and private industry) could not be measured, and that the roles needed to support our nation’s cybersecurity were undefined. To combat this challenge, the Federal Chief Information Officers (CIO) Council was tasked in 2008 to provide a standard framework to understand the cybersecurity roles within the federal government.

In 2008, the Federal CIO Council produced a research report that referenced where other information technology professional development efforts were also under way, and specific roles were identified as needed by agencies to conduct cybersecurity work.

In 2011, thirteen roles were identified and published by the Federal CIO Council. This content was created with input from focus groups with subject-matter experts from numerous federal agencies.

Building on this work, the first version of the NCWF was posted for public comment in September 2011. The comments were incorporated into a version that became the basis of cybersecurity functional codes by the Office of Personnel Management (OPM) in 2013. Use of these codes enabled federal agencies to identify the cybersecurity workforce, determine baseline capabilities, examine hiring trends, identify skill gaps, and more effectively recruit, hire, develop, and retain a valuable cybersecurity workforce.

A government-wide review of that first version of the NCWF provided an opportunity for other organizations to comment and recommend edits. The Department of Homeland Security (DHS) analyzed this input and validated final recommendations via focus groups with subject-matter experts from around the country and across private industry, academia, and government.

A key focus of DHS’ focus groups was to gather equal input across industry sectors to ensure that the NCWF is applicable across the nation and not just to government agencies. The resulting second version of the NCWF was drafted, validated, and published in 2014.

Since 2014, the Department of Defense (DoD) further refined the NCWF and added the Work Roles – which are provided for the first time in this publication – to add more specificity and to help organizations better associate cybersecurity positions with the NCWF. DoD developed the Work Roles with input from private industry and government, and DHS refined them to ensure private sector and civilian government applicability.
1.2 Purpose and Applicability

The purpose of this publication is to provide a fundamental reference resource to support a workforce capable of meeting an organization’s cybersecurity needs by:

- Providing organizations with a common, consistent lexicon that categorizes and describes cybersecurity work;
- Organizing cybersecurity work into seven high-level Categories and over 50 Work Roles within those seven Categories;
- Offering a superset of Tasks for each Work Role; and
- Offering a superset list of Knowledge, Skills, and Abilities (KSAs) for each work role.

Using the NCWF as a reference resource will improve the communication about cybersecurity needed to identify, recruit, and develop talent. The NCWF will allow employers to use more focused, consistent language in professional development programs, in their use of industry certifications, and in their selection of relevant training opportunities for their workforce. The NCWF facilitates the use of a more consistent, comparable, and repeatable approach to select and specify cybersecurity roles for positions within organizations. It also provides a common lexicon that academic institutions can use to develop cybersecurity curricula that better prepares students for current and anticipated cybersecurity workforce needs.

The application of the NCWF as a resource is meant to offer the ability to describe all cybersecurity work. An applicability goal of the NCWF is that any cybersecurity job or position can be described by identifying the relevant components identified within the NCWF. Context of the mission or business processes being supported by that job or position will drive which components are selected from within the NCWF. This document does not seek to provide a definition of cybersecurity, since the use of that term varies depending upon an organization’s mission or business context.

The NCWF is a resource from which organizations or sectors can develop additional publications or tools focused on defining or providing guidance on aspects of workforce development, planning, training, and education.

1.3 Audience/NCWF Consumers

The NCWF can be viewed as a cybersecurity workforce dictionary, and consumers of the NCWF will reference it for different workforce development, education, or training purposes. The NCWF is an essential resource that will help to ensure that our nation can educate, recruit, train, develop, and retain a highly qualified cybersecurity workforce.

1.3.1 Employers

Use of the common lexicon within the NCWF enables employers to establish standards for inventorying and developing their cybersecurity workforce. The NCWF can be used by employers and organizational leadership to:
• Inventory and track their cybersecurity workforce to gain a greater understanding of the strengths and gaps in Knowledge, Skills, and Abilities and Tasks performed;
• Identify training and qualification requirements to develop critical Knowledge, Skills, and Abilities to perform cybersecurity Tasks;
• Improve position descriptions and job vacancy announcements by using specific Work Roles from the NCWF and selecting relevant KSAs and Tasks; and
• Identify the most relevant Work Roles and develop career paths to guide staff in gaining the requisite skills for those roles.

Figure 1 illustrates how the NCWF helps to build a strong cybersecurity workforce.

As shown, several key inputs improve the benefits and value of the NCWF for a capable and ready cybersecurity workforce:

• A common lexicon supports consistent use of terminology by educators, employers, and employees.
• Criticality Analysis helps to identify those Tasks and KSAs that form a baseline set (i.e., that are key to multiple Work Roles or to specific role-based training). The analysis also helps identify those Tasks and KSAs that are critical for successful performance with a given Work Role.
• Proficiency Analysis supports understanding of the expectation of the level to which a person in a Work Role exhibits the KSAs described. For example, someone in a given Work Role may exhibit varied understanding and ability as that worker progresses from entry-level to expert. Proficiency considerations are an important workforce consideration and are included in the additional concepts for future consideration in the NCWF, as described in Section 4.1.
1.3.2 Current and Future Cybersecurity Workers

The NCWF supports those in the cybersecurity field and those who might wish to enter the cybersecurity field, to explore Tasks within cybersecurity Categories and Work Roles. It also assists those who support these workers, such as staffing specialists and guidance counselors, to help job seekers and students understand which cybersecurity Work Roles and which associated Knowledge, Skills, and Abilities are being valued by employers for in-demand cybersecurity jobs and positions.

These workers are further supported when vacancy announcements and open position descriptions use the common lexicon of the NCWF, providing clear and consistent descriptions of the cybersecurity tasks and training that are likely to be needed for those positions.

When training providers and industry certification providers use the common lexicon of the NCWF, those in the cybersecurity field, or those who might wish to enter the cybersecurity field, can find training and/or certification providers that can help them learn the tasks necessary to secure a cybersecurity job or to progress into new positions. Use of the common lexicon helps students and professionals to obtain KSAs that are typically demonstrated by a person whose cybersecurity position includes a given Work Role. This understanding helps them seek out academic programs that include learning outcomes and knowledge units that map to the KSAs and Tasks that are valued by employers.

1.3.3 Educators/Trainers

The NCWF provides a reference for educators to develop curriculum, training programs, courses, seminars, and exercises or challenges that cover the KSAs and Tasks described in the NCWF.

Staffing specialists and guidance counselors can use the NCWF as a resource for career exploration.

1.3.4 Technology Providers

The NCWF allows a technology provider to identify the cybersecurity Work Roles and the Tasks and KSAs associated with hardware and software products and services they provide.

1.4 Organization of this Special Publication

The remainder of this special publication is organized as follows:

- Chapter Two defines the components of the NCWF: (i) Categories; (ii) Specialty Areas; (iii) Work Roles; (iv) associated supersets of Tasks; and (v) Knowledge, Skills, and Abilities for each Work Role.
- Chapter Three shows the application of the NCWF through cross-walk illustrations with applicable external models.
- Chapter Four describes the process by which revisions to the NCWF will be periodically addressed.
- Appendix A describes the NCWF list of Categories, Specialty Areas, Work Roles, Tasks, and KSAs.
- Appendix B provides a detailed listing of each Work Role, including the associated Tasks and KSAs.
- Additional appendices describe applicable acronyms and references.
2 NCWF Components and Relationships

2.1 Components of the NCWF

The NCWF organizes information technology (IT), cybersecurity, and cyber-related work. This section introduces and defines the core components of the NCWF in support of those areas.

2.1.1 Categories

Categories provide the overarching organizational structure of the NCWF. There are seven Categories and all are composed of Specialty Areas and Work Roles. This organizing structure is based on extensive job analyses that groups together work and workers that share common major functions, regardless of job titles or other occupational terms.

2.1.2 Specialty Areas

Categories contain groupings of cybersecurity work, which are called Specialty Areas. There were 31 Specialty Areas called out in NCWF version 1.0 [1] and 32 in NCWF version 2.0 [2]. Each specialty area represents an area of concentrated work, or function, within cybersecurity. Those previous versions of the NCWF provided the typical Tasks and Knowledge, Skills and Abilities (KSAs) within each specialty area. Specialty Areas in a given Category are typically more similar to one another than to Specialty Areas in other Categories. In this publication, Tasks and KSAs are now connected with the Work Roles defined in Appendix A.

2.1.3 Work Roles

Work Roles are the most detailed groupings of IT, cybersecurity, or cyber-related work. These roles include lists of knowledge, skills, and abilities that a person must have to perform a set of functions or tasks.

For members of the cybersecurity workforce, work being performed is described by selecting one or more Work Roles from the NCWF relevant to that job or position, in support of mission or business processes.

To aid in the organization and communication about cybersecurity responsibilities, Work Roles are grouped into specific classes of categories and specialty areas, as described below.

2.1.4 Tasks

Every Work Role requires an individual to perform certain duties, or Tasks. Tasks are examples of the type of work that could be assigned to a professional working in one of the NCWF’s Work Roles.

2.1.5 Knowledge, Skills, and Abilities

Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform a job and are generally demonstrated through relevant experience, education, or training. The NCWF
associates KSAs with Work Roles to clearly define the qualifying experience or capabilities needed to successfully perform the tasks or functions associated with a given Role.

### 2.2 NCWF Component Relationships

Various NCWF components work together to describe the information technology (IT), cybersecurity, and cyber-related work. As illustrated in Figure 2, each Category is supported by Specialty Areas, each of which is supported by one or more Work Roles. Each Work Role, in turn, is composed of numerous discrete Tasks and associated KSAs. Notably, KSAs numbered K0001 through K0006 are core to all cybersecurity activities and apply to every Work Role.

Grouping components in this manner helps to organize the Work Roles and related Tasks and KSAs, simplifies communicating about cybersecurity topics, and helps with alignment to external frameworks. Specific associations of Work Roles to Tasks, Knowledge, Skills, and Abilities are described in Appendix B.

![Figure 2 - Relationships among NCWF Components](image)
3 Applying the NCWF

Application of the various components, as described in Section 2, enables the organization to achieve a broad array of benefits. Using the NCWF to understand organizational needs and assess the extent to which those needs are met, helps the organization to plan, implement, and monitor a successful cybersecurity program. The following topics illustrate how to apply the NCWF to achieve these business purposes, ensuring effective performance, cost-effective workforce management, and continuous cybersecurity readiness. While several of the examples are based upon a strategy that is specific to federal government programs, any organization with cybersecurity workforce needs will benefit from the principles described. The following topics are helpful to all those involved in cybersecurity workforce development.

3.1 Identification of Cybersecurity Workforce Needs

With technology becoming a critical element of nearly every part of society, cybersecurity is a rapidly changing and expanding field. This expansion requires a cadre of skilled workers to help organizations perform cybersecurity functions. As organizations identify what is needed to manage risk adequately, both now and in the future, leaders need to consider the workforce capabilities and capacity needed.

The DHS Cybersecurity Workforce Development Toolkit (CWDT) – which provides tools and guidance to help organizations understand and build their cybersecurity workforce – describes the first step in preparing to build your cybersecurity workforce as having a shared vision for organizing your cybersecurity workforce against cybersecurity work. Having a common understanding supports leaders in responding to changing environments – giving you data to better adjust resources, see patterns of work, and highlight areas of potential risk. This understanding is especially important in the ever-changing environment of cybersecurity. The CWDT includes a Cybersecurity Workforce Planning Capability Maturity Model (CMM), a self-assessment tool to help organizations evaluate the maturity of their cybersecurity workforce planning capability.

Once the organization has determined cybersecurity requirements (such as through a cybersecurity audit or an internal self-assessment), the NCWF helps specify the Work Roles and Tasks that will help fulfill those. While general terms, such as “cyber professionals,” have historically been used to measure needs, the specificity provided by NCWF provides a better approach to describe the dozens of discrete job functions needed. By defining the required and available competencies of resources, and by identifying gaps between required and available skills, the organization can identify critical needs. NCWF helps an organization to answer the following questions, drawn from the Baldrige Cybersecurity Excellence Builder Tool, regarding maintenance of an effective and supportive workforce environment to achieve its cybersecurity goals:

- How do you assess your workforce capability and capacity needs related to cybersecurity?
- How do you organize and manage your cybersecurity workforce to establish roles and responsibilities?
How do you prepare your workforce for changing cybersecurity capability and capacity needs?

The cybersecurity landscape is always evolving, so the NCWF helps to provide continuous monitoring of these needs as part of a proactive risk management approach.

### 3.2 Education and Training of Cybersecurity Workforce Members

Access to information security education and training has grown significantly in recent years, partly due to efforts by the federal government to improve and expand formal cybersecurity education programs. Despite this success, many organizations continue to find that such programs are not adequately preparing students to support the needs described by the Work Roles. The NCWF, through its consistent lexicon, helps educators to prepare students with the specific Knowledge, Skills, and Abilities that should be demonstrated by a person whose cybersecurity position includes those Work Roles.

Academic institutions are a critical part of preparing and educating the cybersecurity workforce. Collaboration among public and private entities, such as through the NICE program, enable such institutions to determine common knowledge and abilities that are needed. In turn, developing and delivering curricula that are harmonized with the NCWF lexicon allows institutions to better prepare students for filling employers’ cybersecurity positions. As the pipeline of students finding desired jobs in cybersecurity increases, more students will be attracted to academic cybersecurity programs as a reliable pathway to a career. An example of such success is the NSA/DHS National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program Office, which developed a mapping document [6] that demonstrates a relationship between the CAE-CD Knowledge Units and the NCWF.

### 3.3 Recruitment and Hiring of Highly Skilled Cybersecurity Talent

As relevant cybersecurity assessments (e.g., information security audits) inform the organization about risk management priorities, and in response to the workforce assessment described in Section 3.1, application of NCWF will help organizations to accomplish better strategic workforce planning and hiring. NCWF definitions may be used to create or revise position descriptions that consistently portray the Work Roles, and the lexicon helps candidates to accurately seek out specific positions for which they are interested and qualified. Through the use of NCWF Task definitions to describe job duties and responsibilities, and the use of NCWF KSAs to describe the position’s needed skills and qualifications, candidates and hiring managers will gain a consistent understanding of expectations. Application of these criteria also helps to develop evaluation criteria for vetting and approving candidates.

The DHS CMSI PushbuttonPD™ Tool [11] allows managers, supervisors, and HR specialists to rapidly draft a federal employee Position Description (PD) without the need for extensive training or prior knowledge of position classification. It is designed to present language from multiple, mission-critical authoritative sources and standards for duties, tasks, and KSAs, rapidly capture the hiring official’s requirements, and present them in a robust hiring package that can be easily integrated into existing agency HR processes.
Application of the NCWF is not restricted to external hiring. Because it supports specific training recommendations and performance measurement capability, the framework assists organizations with retraining existing staff to take on cybersecurity Work Roles. NCWF may also support organizations’ ability to temporarily or permanently obtain external staff augmentation to fill those gaps that were identified in Section 3.1, and/or may be able to obtain external resources that can support education and training to ensure that internal candidates end up with the necessary knowledge and skills.

3.4 Retention and Development of Highly Skilled Cybersecurity Talent

A critical aspect of a skilled cybersecurity workforce involves the retention and development of the skilled talent already onboard. A current employee has existing relationships, institutional knowledge, and organizational experience that is hard to replace. Refilling a position after an employee leaves often brings new advertising and hiring costs, expenses for training, diminished productivity, and reduced morale. The DHS CWDT [9] offers profiles as a guide to focuses on retaining staff at every level whether entry level, mid-career or seasoned cybersecurity professionals. The following list illustrates some of the ways that NCWF supports retention and development of cybersecurity talent:

- Since some personnel recognize that cybersecurity is an exciting and technical field, the broad range of Work Roles and Specialty Areas provides a range of cybersecurity functions to which they might aspire and work to attain.
- While some organizations have been able to attract cybersecurity talent, the ability to retain such talent will depend, in part, on the ability to offer a progressively challenging and evolving set of Work Roles, such as those enumerated by the NCWF.
- The detailed understanding of the Tasks and KSAs helps existing staff to understand the specific steps needed to develop their capabilities, promoting readiness for a particular desired position. The organization might even rotate staff into such positions to develop skills in a particular set of KSAs.
- Understanding of the Tasks and KSAs helps organizations to identify group training opportunities that will help prepare numerous staff members to perform duties in particular Categories, Specialty Areas, and Work Roles.
- KSAs help organizations to understand which technical abilities will help a person in a position that includes specific cybersecurity Work Roles. Building upon the value of knowledge-based certifications, organizations may be able to use training and examinations that are based on cybersecurity skills and abilities, such as those that evaluate KSA proficiency in a realistic environment.
- Considering the gaps identified in Section 3.1, the organization can use existing personnel to fill critical cybersecurity staffing needs, leveraging the ability to review resumes of existing staff to identify those with desirable KSAs.
- Organizations can identify personnel that are diligent in improving KSAs in relevant areas, rewarding those who perform well and developing improvement plans for those needing work in particular areas of ability.
The NCWF is helpful for existing employees who desire to move into a cybersecurity Work Role from another position (e.g., a reliable employee in a non-cybersecurity work role that is being phased out, or a worker in a position that’s less challenging than desired.) Through identification of a challenging career path, such an employee may be invigorated by the new opportunity, armed with an understanding of what KSAs will help prepare them for the new role.

Using the NCWF as described above will help strengthen the organization’s cybersecurity workforce. Investment in the existing workforce, such as through initiatives focused on training and retaining existing talent, will help the organization to prepare for and realize its risk management objectives.

3.5 Cybersecurity Framework (CSF)

In 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity [3], commonly referred to as the Cybersecurity Framework (CSF). Developed in response to Executive Order (EO) 13636 [12], the CSF was created to provide a performance-based and cost-effective approach to help organizations to identify, assess, and manage cybersecurity risk. It was built through a series of public workshops that were convened by NIST to better understand what standards and methodologies are helpful for achieving effective risk management, and how voluntary existing good practices might be implemented to improve cybersecurity.

CSF is composed of three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Each component reinforces the connection between business drivers and cybersecurity activities. The most relevant part of CSF to NCWF is the Framework Core. The Core’s elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These functions - Identify, Protect, Detect, Respond, and Recover - are described in further detail below.

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help to support achievement of the outcomes in each Category.

- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

A companion document, the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* [13], discusses key areas of CSF development and alignment, including industry collaboration. Its plans are based on feedback received from stakeholders throughout the development process, including elements that impact cybersecurity workforce organization and communication. The
roadmap points to the need for a skilled cybersecurity workforce to meet the unique cybersecurity needs of critical infrastructure. It recognizes that, as the cybersecurity threat and technology environments evolve, the workforce must continue to adapt to design, develop, implement, maintain, and continuously improve the necessary cybersecurity practices.

The Core Functions each contribute to a high-level understanding of the cybersecurity needs of the organization:

- **Identify (ID)** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect (PR)** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect (DE)** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS)** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover (RC)** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

In many ways, these Functions correlate to the NCWF Categories. Table 1 describes the relationships among the CSF Functions and NCWF Categories.
Table 1 - Crosswalk of NCWF Workforce Categories to CSF Functions

<table>
<thead>
<tr>
<th>NCWF Category</th>
<th>Category Description</th>
<th>Related CSF Function(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision (SP)</td>
<td>Conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for some aspect of the systems' development.</td>
<td>Identify (ID), Protect (PR)</td>
</tr>
<tr>
<td>Operate and Maintain (OM)</td>
<td>Providing the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.</td>
<td>Protect (PR), Detect (DE)</td>
</tr>
<tr>
<td>Oversee and Govern (OV)</td>
<td>Specialty Areas responsible for providing leadership, management, direction, or development and advocacy so that the organization may effectively conduct cybersecurity work.</td>
<td>Identify (ID), Protect (PR), Detect (DE), Recover (RC)</td>
</tr>
<tr>
<td>Protect and Defend (PR)</td>
<td>Specialty Areas responsible for identifying, analyzing, and mitigating threats to internal information technology (IT) systems or networks.</td>
<td>Protect (PR), Detect (DE), Respond (RS)</td>
</tr>
<tr>
<td>Analyze (AN)</td>
<td>Specialty Areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.</td>
<td>Identify (ID), Detect (DE), Respond (RS)</td>
</tr>
<tr>
<td>Collect and Operate (CO)</td>
<td>Specialty Areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.</td>
<td>Detect (DE), Protect (PR), Respond (RS)</td>
</tr>
<tr>
<td>Investigate (IN)</td>
<td>Specialty Areas responsible for investigating cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.</td>
<td>Detect (DE), Respond (RS), Recover (RC)</td>
</tr>
</tbody>
</table>

3.5.1 Example Integration of CSF with NCWF

While the CSF and the NCWF were developed separately, each complements the other by describing a hierarchical approach to achieving cybersecurity goals. Consider the following example:

CSF’s Detect function includes a category of Security Continuous Monitoring (DE.CM). The category includes a subcategory, DE.CM-1, pointing to an outcome of, “The network is monitored to detect potential cybersecurity events.” While CSF describes this outcome, and provides several informative references regarding the security controls to achieve it, CSF does not provide any informative guidance regarding whom should be responsible for attaining the outcome, or what KSAs would apply.
Reviewing the NCWF, we identify the Cybersecurity Defense Incident Responder (PR-IR-001) role in the Protect and Defend (PR) category, Incident Response (IR) specialty area. We can review the description of this role to ensure that it aligns with the CSF DE.CM-1 outcome:

- Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches to maximize survival of life, preservation of property, and information security. Investigates and analyzes relevant response activities and evaluates the effectiveness of and improvements to existing practices.

- Investigates, analyzes, and responds to cybersecurity incidents within the network environment or enclave.

We learn from Appendix A of this document that the person whose position includes this Work Role might be expected to perform many of the following Tasks, which align with the desired CSF outcome:

- **T0041** - Coordinate and provide expert technical support to enterprise-wide cybersecurity defense technicians to resolve cybersecurity defense incidents.
- **T0047** - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
- **T0161** - Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
- **T0163** - Perform cybersecurity defense incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and make recommendations that enable expeditious remediation.
- **T0170** - Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
- **T0175** - Perform real-time cybersecurity defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
- **T0214** - Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
- **T0233** - Track and document cybersecurity defense incidents from initial detection through final resolution.
- **T0246** - Write and publish cybersecurity defense techniques, guidance, and reports on incident findings to appropriate constituencies.
- **T0262** - Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
T0278 - Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cybersecurity defense incidents within the enterprise.

T0279 - Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.

T0312 - Coordinate with intelligence analysts to correlate threat assessment data.

T0333 - Perform cybersecurity defense trend analysis and reporting.

T0395 - Write and publish after-action reviews.

T0503 - Monitor external data sources (e.g., cybersecurity defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain the currency of cybersecurity defense threat condition and determine which security issues may have an impact on the enterprise.

T0510 - Coordinate incident response functions.

Furthermore, from Appendix B, we can learn the broad range of KSAs that might be needed by a person whose cybersecurity position includes this Work Role.

Armed with this information, an organization seeking to achieve the outcome described by CSF DE.CM-1 may determine whether one or more existing staff have the necessary skills to complete the tasks described. If one or more KSAs are lacking, the employee desiring to fill that Work Role will know specifically what areas need improvement and can seek academic classes or industry training to gain the necessary knowledge. If no such staff are found, the employer has specific Task descriptions and KSA requirements that may be advertised in a job posting, or that may be used for contractor staff to augment existing personnel.
4 Future Revision Process

The NCWF builds upon decades of industry research into how to effectively manage the risks to valuable organizational electronic and physical information. Through the years, the industry that has been referred to as computer security, information security, and now cybersecurity has been supported by dedicated workers supporting an evolving set of Work Roles, Tasks, and KSAs. Cybersecurity tactics are ever-changing, always identifying new ways to gain information advantage through technology. As we evolve the ways we perform cybersecurity functions, so must the components of the NCWF continue to evolve.

NCWF users are encouraged to provide feedback and comments through the Workforce Framework page at the NICE project website [14]. As part of an ongoing collaborative approach, NICE will periodically consider the current set of recommendations for expansion, update/correction, withdrawal, or integration of NCWF elements. The program will work to achieve consensus on these recommended changes, drawing on public and private sector input including that of federal cybersecurity workforce and education leadership, and the NCWF publication will be updated accordingly. This approach provides an ongoing set of NCWF elements that are stable, flexible, and technically sound for use as a reference for workforce training and educational needs.

Additionally, new reference materials will be developed to cross-reference elements of the NCWF. To the extent possible, digital reference materials will be posted to the NICE website as an aid to applying and utilizing NCWF and associated materials.

4.1 Additional Concepts for Future Consideration

Several work-related elements have been raised at various discussions and, while not currently integrated into the NCWF, are areas that are likely to be the subject of further research and guidance. The areas of further investigation are:

- **System Security Engineering (SSE)** – Many elements of systems security engineering (a specialty engineering discipline of systems engineering) contribute to a fully integrated, system-level perspective of cybersecurity. Additional research will be conducted to ensure that the Tasks and KSAs described fully support the SSE lifecycle described in Draft NIST Special Publication (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [15]. SP 800-160 describes how SSE “helps to ensure that the appropriate security principles, concepts, methods, and practices are applied during the system life cycle to achieve stakeholder objectives for the protection of assets across all forms of adversity characterized as disruptions, hazards, and threats; to reduce security vulnerability and therefore, reduce susceptibility to adversity; and to provide a sufficient base of evidence that supports claims that the desired level of trustworthiness has been achieved — that is, a level of trustworthiness that the agreed-upon asset protection needs of stakeholders can be adequately satisfied on a continuous basis despite such adversity.”
• **Relationship of Job Title to Work Role** - Job titles are a description of an employee’s job or position in the organization. Job titles vary from organization to organization. Rather than looking to job titles as a means to determine that a position is in the cybersecurity field, it may be beneficial to look at Tasks as a means to identify the cybersecurity Work Roles that are being performed. For the federal government, development of a dedicated cybersecurity job series may enable easier translation between the NCWF and job titles. It would also make it easier to inventory cybersecurity positions and target workforce development (e.g., hiring and incentives, training, retention programs).

• **Competency** – Extensive work has been done to consider competency models which support NCWF participants in many ways. The Department of Labor’s Employment and Training Administration [8] defines a competency as “the capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position.” In addition to the enumeration of technical KSAs, competency models also consider behavioral indicators and describe nontechnical considerations such as Personal Effectiveness, Academic, and Workplace Competencies. Additional information about these considerations is available from the Department of Labor’s CareerOneStop Site.[4]

• **Proficiency Levels and Career Paths** – Beginner, Intermediate, and Senior/Expert proficiency levels can be described by exploring Experience & Credentials, Competencies Skills / and KSAs, and Training & Development Activities. The DHS CWDT includes a section known as ADVANCE, Develop Your People, that includes templates to create custom cybersecurity career paths; links to training, certifications and professional events; and ideas for retaining staff at every level. Individual sectors, associations, and organizations may wish to create their own publications on proficiency levels and career paths.
## Appendix A—Listing of NCWF Elements

### A.1 NCWF Workforce Categories

Table 2 provides a description of each Category described by the NCWF. Each includes an identifier (e.g., SP) that helps to quickly reference the Category and to support the creation of NCWF Work Role identifiers (see Table 4 - NCWF Work Roles).

<table>
<thead>
<tr>
<th>Categories</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision (SP)</td>
<td>Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.</td>
</tr>
<tr>
<td>Operate and Maintain (OM)</td>
<td>Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.</td>
</tr>
<tr>
<td>Oversee and Govern (OV)</td>
<td>Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.</td>
</tr>
<tr>
<td>Protect and Defend (PR)</td>
<td>Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.</td>
</tr>
<tr>
<td>Analyze (AN)</td>
<td>Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.</td>
</tr>
<tr>
<td>Collect and Operate (CO)</td>
<td>Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.</td>
</tr>
<tr>
<td>Investigate (IN)</td>
<td>Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.</td>
</tr>
</tbody>
</table>

Note to Reviewers: The content listed in Appendix A and Appendix B is drawn from multiple sources. Feedback regarding the descriptions of each NCWF component, including Tasks and KSAs, is welcome. The authors also solicit input regarding additional Tasks that might be performed by workers in a particular Work Role, and associated KSAs.
A.2 NCWF Specialty Areas

Table 3 provides a description of each of the NCWF Specialty Areas. As with the NCWF Categories, each Specialty Area includes an identifier (e.g., RM) that helps to quickly reference the area and further supports the creation of NCWF Work Role identifiers (see Table 4 - NCWF Work Roles).

<table>
<thead>
<tr>
<th>Categories</th>
<th>Specialty Areas</th>
<th>Specialty Area Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision (SP)</td>
<td>Risk Management (RM)</td>
<td>Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.</td>
</tr>
<tr>
<td></td>
<td>Software Development (DEV)</td>
<td>Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.</td>
</tr>
<tr>
<td></td>
<td>Systems Architecture (ARC)</td>
<td>Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.</td>
</tr>
<tr>
<td></td>
<td>Technology R&amp;D (RD)</td>
<td>Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.</td>
</tr>
<tr>
<td></td>
<td>Systems Requirements Planning (RP)</td>
<td>Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.</td>
</tr>
<tr>
<td></td>
<td>Test and Evaluation (TE)</td>
<td>Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.</td>
</tr>
<tr>
<td></td>
<td>Systems Development (SYS)</td>
<td>Works on the development phases of the systems development life cycle.</td>
</tr>
<tr>
<td>Operate and Maintain (OM)</td>
<td>Data Administration (DA)</td>
<td>Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management (KM)</td>
<td>Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.</td>
</tr>
<tr>
<td>Categories</td>
<td>Specialty Areas</td>
<td>Specialty Area Descriptions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Customer Service and Technical Support (TS)</td>
<td>Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).</td>
<td></td>
</tr>
<tr>
<td>Network Services (NET)</td>
<td>Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.</td>
<td></td>
</tr>
<tr>
<td>Systems Administration (SA)</td>
<td>Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also, manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.</td>
<td></td>
</tr>
<tr>
<td>Systems Analysis (AN)</td>
<td>Conducts the integration/testing, operations, and maintenance of systems security.</td>
<td></td>
</tr>
<tr>
<td>Oversee and Govern (OV)</td>
<td>Legal Advice and Advocacy (LG)</td>
<td>Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.</td>
</tr>
<tr>
<td></td>
<td>Training, Education, and Awareness (ED)</td>
<td>Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity Management (MG)</td>
<td>Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.</td>
</tr>
<tr>
<td></td>
<td>Strategic Planning and Policy (PL)</td>
<td>Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.</td>
</tr>
<tr>
<td></td>
<td>Executive Cybersecurity Leadership (EX)</td>
<td>Supervises, manages, and/or leads work and workers performing cybersecurity work</td>
</tr>
<tr>
<td></td>
<td>Acquisition and Program/Project Management (PM)</td>
<td>Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that</td>
</tr>
<tr>
<td>Categories</td>
<td>Specialty Areas</td>
<td>Specialty Area Descriptions</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Protect and Defend (PR)</td>
<td>Cybersecurity Defense Analysis (DA)</td>
<td>Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity Defense Infrastructure Support (INF)</td>
<td>Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.</td>
</tr>
<tr>
<td></td>
<td>Incident Response (IR)</td>
<td>Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Assessment and Management (VA)</td>
<td>Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.</td>
</tr>
<tr>
<td>Analyze (AN)</td>
<td>Threat Analysis (TA)</td>
<td>Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.</td>
</tr>
<tr>
<td></td>
<td>Exploitation Analysis (XA)</td>
<td>Analyzes collected information to identify vulnerabilities and potential for exploitation.</td>
</tr>
<tr>
<td></td>
<td>All-Source Analysis (AN)</td>
<td>Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.</td>
</tr>
<tr>
<td></td>
<td>Targets (TD)</td>
<td>Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.</td>
</tr>
<tr>
<td></td>
<td>Language Analysis (LA)</td>
<td>Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.</td>
</tr>
<tr>
<td>Collect and Operate (CO)</td>
<td>Collection Operations (CL)</td>
<td>Executes collection using appropriate strategies and within the priorities established through the collection management process.</td>
</tr>
</tbody>
</table>
| | Cyber Operational Planning (PL) | Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting...
<table>
<thead>
<tr>
<th>Categories</th>
<th>Specialty Areas</th>
<th>Specialty Area Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cyber Operations (OP)</td>
<td>Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.</td>
</tr>
<tr>
<td>Investigate (IN)</td>
<td>Cyber Investigation (CI)</td>
<td>Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.</td>
</tr>
<tr>
<td></td>
<td>Digital Forensics (FO)</td>
<td>Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.</td>
</tr>
</tbody>
</table>
A.3 NCWF Work Roles

Table 4 provides a description of each of the Work Roles described by the NCWF. Each Work Role is identified by the Category and Specialty Area, followed by a sequential number (e.g., SP-RM-001 is the first Work Role in the SP Category, RM Specialty Area). Some of the Work Role Descriptions originate with external documents (e.g., Committee on National Security Systems Instruction [CNSSI] 4009) and include that information in the description column. As described in Section 4, the NCWF will be periodically refreshed, with some Work Roles becoming deprecated, added, or modified to address changes to the cybersecurity workforce landscape.

### Table 4 - NCWF Work Roles

<table>
<thead>
<tr>
<th>Category/Major Specialty Area</th>
<th>Work Role</th>
<th>NCWF ID</th>
<th>Work Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision (SP)</td>
<td>Authorizing Official/Designating Representative</td>
<td>SP-RM-001</td>
<td>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 (CNSSI 4009).</td>
</tr>
<tr>
<td>Risk Management (RM)</td>
<td>Security Control Assessor</td>
<td>SP-RM-002</td>
<td>Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).</td>
</tr>
<tr>
<td>Software Development (DEV)</td>
<td>Software Developer</td>
<td>SP-DEV-001</td>
<td>Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.</td>
</tr>
<tr>
<td></td>
<td>Secure Software Assessor</td>
<td>SP-DEV-002</td>
<td>Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.</td>
</tr>
<tr>
<td>Systems Architecture (ARC)</td>
<td>Enterprise Architect</td>
<td>SP-ARC-001</td>
<td>Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.</td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------</td>
<td>------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Architect</td>
<td>SP-ARC-002</td>
</tr>
<tr>
<td>Technology R&amp;D (RD)</td>
<td></td>
<td>Research &amp; Development Specialist</td>
<td>SP-RD-001</td>
</tr>
<tr>
<td>Systems Requirements Planning (RP)</td>
<td></td>
<td>Systems Requirements Planner</td>
<td>SP-RP-001</td>
</tr>
<tr>
<td>Test and Evaluation (TE)</td>
<td></td>
<td>System Testing and Evaluation Specialist</td>
<td>SP-TE-001</td>
</tr>
<tr>
<td>Systems Development (SYS)</td>
<td></td>
<td>Information Systems Security Developer</td>
<td>SP-SYS-001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systems Developer</td>
<td>SP-SYS-002</td>
</tr>
<tr>
<td>Operate and Maintain (OM)</td>
<td>Data Administration (DA)</td>
<td>Database Administrator</td>
<td>OM-DA-001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Analyst</td>
<td>OM-DA-002</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management (KM)</td>
<td>Knowledge Manager</td>
<td>OM-KM-001</td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------</td>
<td>------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Customer Service and Technical Support (TS)</td>
<td>Technical Support Specialist</td>
<td>OM-TS-001</td>
<td>Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).</td>
</tr>
<tr>
<td>Network Services (NET)</td>
<td>Network Operations Specialist</td>
<td>OM-NET-001</td>
<td>Plans, implements, and operates network services/systems, to include hardware and virtual environments.</td>
</tr>
<tr>
<td>Systems Administration (SA)</td>
<td>System Administrator</td>
<td>OM-SA-001</td>
<td>Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.</td>
</tr>
<tr>
<td>Systems Analysis (AN)</td>
<td>Systems Security Analyst</td>
<td>OM-AN-001</td>
<td>Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.</td>
</tr>
<tr>
<td>Legal Advice and Advocacy (LG)</td>
<td>Cyber Legal Advisor</td>
<td>OV-LG-001</td>
<td>Provides legal advice and recommendations on relevant topics related to cyber law.</td>
</tr>
<tr>
<td>Privacy Compliance Manager</td>
<td></td>
<td>OV-LG-002</td>
<td>Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.</td>
</tr>
<tr>
<td>Training, Education, and Awareness (ED)</td>
<td>Cyber Instructional Curriculum Developer</td>
<td>OV-ED-001</td>
<td>Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.</td>
</tr>
<tr>
<td>Cyber Instructor</td>
<td></td>
<td>OV-ED-002</td>
<td>Develops and conducts training or education of personnel within cyber domain.</td>
</tr>
<tr>
<td>Cybersecurity Management (MG)</td>
<td>Information Systems Security Manager</td>
<td>OV-MG-001</td>
<td>Responsible for the cybersecurity of a program, organization, system, or enclave.</td>
</tr>
<tr>
<td>COMSEC Manager</td>
<td></td>
<td>OV-MG-002</td>
<td>Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).</td>
</tr>
<tr>
<td>Strategic Planning and Policy (PL)</td>
<td>Cyber Workforce Developer and Manager</td>
<td>OV-PL-001</td>
<td>Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.</td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cyber Policy and Strategy Planner</td>
<td></td>
<td>OV-PL-002</td>
<td></td>
</tr>
<tr>
<td>Executive Cyber Leadership (EX)</td>
<td>Executive Cyber Leadership</td>
<td>OV-EX-001</td>
<td></td>
</tr>
<tr>
<td>Acquisition and Program/Project Management (PM)</td>
<td>Program Manager</td>
<td>OV-PM-001</td>
<td></td>
</tr>
<tr>
<td>IT Project Manager</td>
<td></td>
<td>OV-PM-002</td>
<td></td>
</tr>
<tr>
<td>IT Investment/Portfolio Manager</td>
<td></td>
<td>OV-PM-003</td>
<td></td>
</tr>
<tr>
<td>IT Program Auditor</td>
<td></td>
<td>OV-PM-004</td>
<td></td>
</tr>
<tr>
<td>Protect and Defend (PR)</td>
<td>Cyber Defense Analysis (DA)</td>
<td>Cyber Defense Analyst</td>
<td>PR-DA-001</td>
</tr>
<tr>
<td>Cyber Defense Infrastructure Support (INF)</td>
<td>Cyber Defense Infrastructure Support Specialist</td>
<td>PR-INF-001</td>
<td></td>
</tr>
<tr>
<td>Incident Response (IR)</td>
<td>Cyber Defense Incident Responder</td>
<td>PR-IR-001</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment and Management (VA)</td>
<td>Vulnerability Assessment Analyst</td>
<td>PR-VA-001</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------</td>
<td>----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Analyze (AN)</td>
<td>Threat Analysis (TA)</td>
<td>Warning Analyst</td>
<td>AN-TA-001</td>
</tr>
<tr>
<td>Exploitation Analysis (XA)</td>
<td>Exploitation Analyst</td>
<td>AN-XA-001</td>
<td>Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.</td>
</tr>
<tr>
<td>All-Source Analysis (AN)</td>
<td>All-Source Analyst</td>
<td>AN-AN-001</td>
<td>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.</td>
</tr>
<tr>
<td>Mission Assessment Specialist</td>
<td>AN-AN-002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Targets (TD)</td>
<td>Target Developer</td>
<td>AN-TD-001</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target Network Analyst</td>
<td>AN-TD-002</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Language Analysis (LA)</td>
<td>Multi-Disciplined Language Analyst</td>
<td>AN-LA-001</td>
<td>Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.</td>
</tr>
<tr>
<td>Collect and Operate (CO)</td>
<td>Collection Operations (CL)</td>
<td>All Source-Collection Manager</td>
<td>CO-CL-001</td>
</tr>
<tr>
<td></td>
<td>All Source-Collection Requirements Manager</td>
<td>CO-CL-002</td>
<td>Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.</td>
</tr>
<tr>
<td>Cyber Operational Planning (PL)</td>
<td>Cyber Intel Planner</td>
<td>CO-PL-001</td>
<td>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 in cyberspace.</td>
</tr>
<tr>
<td>Category</td>
<td>Specialty Area</td>
<td>Work Role</td>
<td>NCWF ID</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------</td>
<td>------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Cyber Ops Planner</td>
<td>CO-PL-002</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Partner Integration Planner</td>
<td>CO-PL-003</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Cyber Operations (OP)</td>
<td>CO-OP-001</td>
<td>Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.</td>
<td></td>
</tr>
<tr>
<td>Cyber Crime Investigator</td>
<td>IN-CI-001</td>
<td>Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.</td>
<td></td>
</tr>
<tr>
<td>Digital Forensics (FO)</td>
<td>IN-FO-001</td>
<td>Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.</td>
<td></td>
</tr>
<tr>
<td>Cyber Defense Forensics Analyst</td>
<td>IN-FO-002</td>
<td>Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.</td>
<td></td>
</tr>
</tbody>
</table>
### A.4 NCWF Work Role Tasks

Table 5 provides a listing of the various Tasks associated with NCWF Work Roles. Because the Tasks have evolved over many years and are expected to continue to do so, they are not sorted in a particular order and will simply continue to grow sequentially.

**Table 5 - NCWF Work Role Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0001</td>
<td>Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.</td>
</tr>
<tr>
<td>T0002</td>
<td>Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.</td>
</tr>
<tr>
<td>T0003</td>
<td>Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.</td>
</tr>
<tr>
<td>T0004</td>
<td>Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.</td>
</tr>
<tr>
<td>T0005</td>
<td>Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.</td>
</tr>
<tr>
<td>T0006</td>
<td>Advocate organization's official position in legal and legislative proceedings.</td>
</tr>
<tr>
<td>T0007</td>
<td>Analyze and define data requirements and specifications.</td>
</tr>
<tr>
<td>T0008</td>
<td>Analyze and plan for anticipated changes in data capacity requirements.</td>
</tr>
<tr>
<td>T0009</td>
<td>Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.</td>
</tr>
<tr>
<td>T0010</td>
<td>Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.</td>
</tr>
<tr>
<td>T0011</td>
<td>Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.</td>
</tr>
<tr>
<td>T0012</td>
<td>Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support.</td>
</tr>
<tr>
<td>T0013</td>
<td>Apply coding and testing standards, apply security testing tools including &quot;fuzzing&quot; static-analysis code scanning tools, and conduct code reviews.</td>
</tr>
<tr>
<td>T0014</td>
<td>Apply secure code documentation.</td>
</tr>
<tr>
<td>T0015</td>
<td>Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.</td>
</tr>
<tr>
<td>T0016</td>
<td>Apply security policies to meet security objectives of the system.</td>
</tr>
<tr>
<td>T0017</td>
<td>Apply service oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.</td>
</tr>
<tr>
<td>T0018</td>
<td>Assess the effectiveness of cybersecurity measures utilized by system(s).</td>
</tr>
<tr>
<td>T0019</td>
<td>Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.</td>
</tr>
<tr>
<td>T0020</td>
<td>Develop content for cyber defense tools.</td>
</tr>
<tr>
<td>T0021</td>
<td>Build, test, and modify product prototypes using working models or theoretical models.</td>
</tr>
<tr>
<td>T0022</td>
<td>Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.</td>
</tr>
<tr>
<td>T0023</td>
<td>Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.</td>
</tr>
<tr>
<td>T0024</td>
<td>Collect and maintain data needed to meet system cybersecurity reporting.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0025</td>
<td>Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.</td>
</tr>
<tr>
<td>T0026</td>
<td>Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.</td>
</tr>
<tr>
<td>T0027</td>
<td>Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion.</td>
</tr>
<tr>
<td>T0028</td>
<td>Conduct and/or support authorized penetration testing on enterprise network assets.</td>
</tr>
<tr>
<td>T0029</td>
<td>Conduct functional and connectivity testing to ensure continuing operability.</td>
</tr>
<tr>
<td>T0030</td>
<td>Conduct interactive training exercises to create an effective learning environment.</td>
</tr>
<tr>
<td>T0031</td>
<td>Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.</td>
</tr>
<tr>
<td>T0032</td>
<td>Conduct Privacy Impact Assessments (PIA) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).</td>
</tr>
<tr>
<td>T0033</td>
<td>Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.</td>
</tr>
<tr>
<td>T0034</td>
<td>Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.</td>
</tr>
<tr>
<td>T0035</td>
<td>Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).</td>
</tr>
<tr>
<td>T0036</td>
<td>Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.</td>
</tr>
<tr>
<td>T0037</td>
<td>Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.</td>
</tr>
<tr>
<td>T0038</td>
<td>Develop threat model based on customer interviews and requirements.</td>
</tr>
<tr>
<td>T0039</td>
<td>Consult with customers to evaluate functional requirements.</td>
</tr>
<tr>
<td>T0040</td>
<td>Consult with engineering staff to evaluate interface between hardware and software.</td>
</tr>
<tr>
<td>T0041</td>
<td>Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.</td>
</tr>
<tr>
<td>T0042</td>
<td>Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications.</td>
</tr>
<tr>
<td>T0043</td>
<td>Coordinate with enterprise-wide cyber defense staff to validate network alerts.</td>
</tr>
<tr>
<td>T0044</td>
<td>Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.</td>
</tr>
<tr>
<td>T0045</td>
<td>Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.</td>
</tr>
<tr>
<td>T0046</td>
<td>Correct errors by making appropriate changes and rechecking the program to ensure desired results are produced.</td>
</tr>
<tr>
<td>T0047</td>
<td>Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.</td>
</tr>
<tr>
<td>T0048</td>
<td>Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats.</td>
</tr>
<tr>
<td>T0049</td>
<td>Decrypt seized data using technical means.</td>
</tr>
<tr>
<td>T0050</td>
<td>Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0051</td>
<td>Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.</td>
</tr>
<tr>
<td>T0052</td>
<td>Define project scope and objectives based on customer requirements.</td>
</tr>
<tr>
<td>T0053</td>
<td>Design and develop cybersecurity or cybersecurity-enabled products.</td>
</tr>
<tr>
<td>T0054</td>
<td>Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.</td>
</tr>
<tr>
<td>T0055</td>
<td>Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.</td>
</tr>
<tr>
<td>T0056</td>
<td>Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.</td>
</tr>
<tr>
<td>T0057</td>
<td>Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.</td>
</tr>
<tr>
<td>T0058</td>
<td>Determine level of assurance of developed capabilities based on test results.</td>
</tr>
<tr>
<td>T0059</td>
<td>Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet.</td>
</tr>
<tr>
<td>T0060</td>
<td>Develop an understanding of the needs and requirements of information end-users.</td>
</tr>
<tr>
<td>T0061</td>
<td>Develop and direct system testing and validation procedures and documentation.</td>
</tr>
<tr>
<td>T0062</td>
<td>Develop and document requirements, capabilities, and constraints for design procedures and processes.</td>
</tr>
<tr>
<td>T0063</td>
<td>Develop and document systems administration standard operating procedures.</td>
</tr>
<tr>
<td>T0064</td>
<td>Review and validate data mining and data warehousing programs, processes, and requirements.</td>
</tr>
<tr>
<td>T0065</td>
<td>Develop and implement network backup and recovery procedures.</td>
</tr>
<tr>
<td>T0066</td>
<td>Develop and maintain strategic plans.</td>
</tr>
<tr>
<td>T0067</td>
<td>Develop architectures or system components consistent with technical specifications.</td>
</tr>
<tr>
<td>T0068</td>
<td>Develop data standards, policies, and procedures.</td>
</tr>
<tr>
<td>T0069</td>
<td>Develop detailed security design documentation for component and interface specifications to support system design and development.</td>
</tr>
<tr>
<td>T0070</td>
<td>Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.</td>
</tr>
<tr>
<td>T0071</td>
<td>Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).</td>
</tr>
<tr>
<td>T0072</td>
<td>Develop methods to monitor and measure risk, compliance, and assurance efforts.</td>
</tr>
<tr>
<td>T0073</td>
<td>Develop new or identify existing awareness and training materials that are appropriate for intended audiences.</td>
</tr>
<tr>
<td>T0074</td>
<td>Develop policy, programs, and guidelines for implementation.</td>
</tr>
<tr>
<td>T0075</td>
<td>Provide technical summary of findings in accordance with established reporting procedures.</td>
</tr>
<tr>
<td>T0076</td>
<td>Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.</td>
</tr>
<tr>
<td>T0077</td>
<td>Develop secure code and error handling.</td>
</tr>
<tr>
<td>T0078</td>
<td>Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0079</td>
<td>Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.</td>
</tr>
<tr>
<td>T0080</td>
<td>Develop test plans to address specifications and requirements.</td>
</tr>
<tr>
<td>T0081</td>
<td>Diagnose network connectivity problem.</td>
</tr>
<tr>
<td>T0082</td>
<td>Document and address organization’s information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition lifecycle.</td>
</tr>
<tr>
<td>T0083</td>
<td>Draft statements of preliminary or residual security risks for system operation.</td>
</tr>
<tr>
<td>T0084</td>
<td>Employ secure configuration management processes.</td>
</tr>
<tr>
<td>T0085</td>
<td>Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.</td>
</tr>
<tr>
<td>T0086</td>
<td>Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.</td>
</tr>
<tr>
<td>T0087</td>
<td>Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.</td>
</tr>
<tr>
<td>T0088</td>
<td>Ensure security improvement actions are evaluated, validated, and implemented as required.</td>
</tr>
<tr>
<td>T0089</td>
<td>Ensure acquired or developed system(s) and architecture(s) are consistent with organization’s cybersecurity architecture guidelines.</td>
</tr>
<tr>
<td>T0090</td>
<td>Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.</td>
</tr>
<tr>
<td>T0091</td>
<td>Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).</td>
</tr>
<tr>
<td>T0092</td>
<td>Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.</td>
</tr>
<tr>
<td>T0093</td>
<td>Establish and maintain communication channels with stakeholders.</td>
</tr>
<tr>
<td>T0094</td>
<td>Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.</td>
</tr>
<tr>
<td>T0095</td>
<td>Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals).</td>
</tr>
<tr>
<td>T0096</td>
<td>Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.</td>
</tr>
<tr>
<td>T0097</td>
<td>Establish the effectiveness and comprehensiveness of existing training programs.</td>
</tr>
<tr>
<td>T0098</td>
<td>Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.</td>
</tr>
<tr>
<td>T0099</td>
<td>Examine recovered data for information of relevance to the issue at hand.</td>
</tr>
<tr>
<td>T0100</td>
<td>Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.</td>
</tr>
<tr>
<td>T0101</td>
<td>Identify alternative information security strategies to address organizational security objective.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0107</td>
<td>Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).</td>
</tr>
<tr>
<td>T0108</td>
<td>Identify and prioritize critical business functions in collaboration with organizational stakeholders.</td>
</tr>
<tr>
<td>T0109</td>
<td>Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.</td>
</tr>
<tr>
<td>T0110</td>
<td>Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.</td>
</tr>
<tr>
<td>T0111</td>
<td>Identify basic common coding flaws at a high level.</td>
</tr>
<tr>
<td>T0112</td>
<td>Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.</td>
</tr>
<tr>
<td>T0113</td>
<td>Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.</td>
</tr>
<tr>
<td>T0114</td>
<td>Identify elements of proof of the crime.</td>
</tr>
<tr>
<td>T0115</td>
<td>Identify information technology (IT) security program implications of new technologies or technology upgrades.</td>
</tr>
<tr>
<td>T0116</td>
<td>Identify organizational policy stakeholders.</td>
</tr>
<tr>
<td>T0117</td>
<td>Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.</td>
</tr>
<tr>
<td>T0118</td>
<td>Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.</td>
</tr>
<tr>
<td>T0119</td>
<td>Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.</td>
</tr>
<tr>
<td>T0120</td>
<td>Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.</td>
</tr>
<tr>
<td>T0121</td>
<td>Implement new system design procedures, test procedures, and quality standards.</td>
</tr>
<tr>
<td>T0122</td>
<td>Implement security designs for new or existing system(s).</td>
</tr>
<tr>
<td>T0123</td>
<td>Implement specific cybersecurity countermeasures for systems and/or applications.</td>
</tr>
<tr>
<td>T0124</td>
<td>Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).</td>
</tr>
<tr>
<td>T0125</td>
<td>Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).</td>
</tr>
<tr>
<td>T0126</td>
<td>Install or replace network hubs, routers, and switches.</td>
</tr>
<tr>
<td>T0127</td>
<td>Integrate and align information security and/or cybersecurity policies to ensure system analysis meets security requirements.</td>
</tr>
<tr>
<td>T0128</td>
<td>Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.</td>
</tr>
<tr>
<td>T0129</td>
<td>Integrate new systems into existing network architecture.</td>
</tr>
<tr>
<td>T0130</td>
<td>Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.</td>
</tr>
<tr>
<td>T0131</td>
<td>Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.</td>
</tr>
<tr>
<td>T0132</td>
<td>Interpret and/or approve security requirements relative to the capabilities of new information technologies.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0133</td>
<td>Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program.</td>
</tr>
<tr>
<td>T0134</td>
<td>Lead and align information technology (IT) security priorities with the security strategy.</td>
</tr>
<tr>
<td>T0135</td>
<td>Lead and oversee information security budget, staffing, and contracting.</td>
</tr>
<tr>
<td>T0136</td>
<td>Maintain baseline system security according to organizational policies.</td>
</tr>
<tr>
<td>T0137</td>
<td>Maintain database management systems software.</td>
</tr>
<tr>
<td>T0138</td>
<td>Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.</td>
</tr>
<tr>
<td>T0139</td>
<td>Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.</td>
</tr>
<tr>
<td>T0140</td>
<td>Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.</td>
</tr>
<tr>
<td>T0141</td>
<td>Maintain information systems assurance and accreditation materials.</td>
</tr>
<tr>
<td>T0142</td>
<td>Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.</td>
</tr>
<tr>
<td>T0143</td>
<td>Make recommendations based on test results.</td>
</tr>
<tr>
<td>T0144</td>
<td>Manage accounts, network rights, and access to systems and equipment.</td>
</tr>
<tr>
<td>T0145</td>
<td>Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).</td>
</tr>
<tr>
<td>T0146</td>
<td>Manage the compilation, cataloging, caching, distribution, and retrieval of data.</td>
</tr>
<tr>
<td>T0147</td>
<td>Manage the monitoring of information security data sources to maintain organizational situational awareness.</td>
</tr>
<tr>
<td>T0148</td>
<td>Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.</td>
</tr>
<tr>
<td>T0149</td>
<td>Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.</td>
</tr>
<tr>
<td>T0150</td>
<td>Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.</td>
</tr>
<tr>
<td>T0151</td>
<td>Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure they provide the intended level of protection.</td>
</tr>
<tr>
<td>T0152</td>
<td>Monitor and maintain databases to ensure optimal performance.</td>
</tr>
<tr>
<td>T0153</td>
<td>Monitor network capacity and performance.</td>
</tr>
<tr>
<td>T0154</td>
<td>Monitor and report the usage of knowledge management assets and resources.</td>
</tr>
<tr>
<td>T0155</td>
<td>Document and escalate incidents (including event’s history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.</td>
</tr>
<tr>
<td>T0156</td>
<td>Oversee and make recommendations regarding configuration management.</td>
</tr>
<tr>
<td>T0157</td>
<td>Oversee the information security training and awareness program.</td>
</tr>
<tr>
<td>T0158</td>
<td>Participate in an information security risk assessment during the Security Assessment and Authorization process.</td>
</tr>
<tr>
<td>T0159</td>
<td>Participate in the development or modification of the computer environment cybersecurity program plans and requirements.</td>
</tr>
<tr>
<td>T0160</td>
<td>Patch network vulnerabilities to ensure information is safeguarded against outside parties.</td>
</tr>
<tr>
<td>T0161</td>
<td>Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.</td>
</tr>
<tr>
<td>T0162</td>
<td>Perform backup and recovery of databases to ensure data integrity.</td>
</tr>
<tr>
<td>T0163</td>
<td>Perform cyber defense incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0164</td>
<td>Perform cyber defense trend analysis and reporting.</td>
</tr>
<tr>
<td>T0165</td>
<td>Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.</td>
</tr>
<tr>
<td>T0166</td>
<td>Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.</td>
</tr>
<tr>
<td>T0167</td>
<td>Perform file signature analysis.</td>
</tr>
<tr>
<td>T0168</td>
<td>Perform hash comparison against established database.</td>
</tr>
<tr>
<td>T0169</td>
<td>Perform cybersecurity testing of developed applications and/or systems.</td>
</tr>
<tr>
<td>T0170</td>
<td>Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.</td>
</tr>
<tr>
<td>T0171</td>
<td>Perform integrated quality assurance testing for security functionality and resiliency attack.</td>
</tr>
<tr>
<td>T0172</td>
<td>Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).</td>
</tr>
<tr>
<td>T0173</td>
<td>Perform timeline analysis.</td>
</tr>
<tr>
<td>T0174</td>
<td>Perform needs analysis to determine opportunities for new and improved business process solutions.</td>
</tr>
<tr>
<td>T0175</td>
<td>Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).</td>
</tr>
<tr>
<td>T0176</td>
<td>Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.</td>
</tr>
<tr>
<td>T0177</td>
<td>Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.</td>
</tr>
<tr>
<td>T0178</td>
<td>Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.</td>
</tr>
<tr>
<td>T0179</td>
<td>Perform static media analysis.</td>
</tr>
<tr>
<td>T0180</td>
<td>Perform system administration on specialized cyber defense applications and systems (e.g., anti-virus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup and restoration.</td>
</tr>
<tr>
<td>T0181</td>
<td>Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.</td>
</tr>
<tr>
<td>T0182</td>
<td>Perform tier 1, 2, and 3 malware analysis.</td>
</tr>
<tr>
<td>T0183</td>
<td>Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.</td>
</tr>
<tr>
<td>T0184</td>
<td>Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.</td>
</tr>
<tr>
<td>T0185</td>
<td>Plan and manage the delivery of knowledge management projects.</td>
</tr>
<tr>
<td>T0186</td>
<td>Plan, execute, and verify data redundancy and system recovery procedures.</td>
</tr>
<tr>
<td>T0187</td>
<td>Plan and recommend modifications or adjustments based on exercise results or system environment.</td>
</tr>
<tr>
<td>T0188</td>
<td>Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.</td>
</tr>
<tr>
<td>T0189</td>
<td>Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.</td>
</tr>
<tr>
<td>T0190</td>
<td>Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).</td>
</tr>
<tr>
<td>T0191</td>
<td>Prepare use cases to justify the need for specific information technology (IT) solutions.</td>
</tr>
<tr>
<td>T0192</td>
<td>Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.</td>
</tr>
<tr>
<td>T0193</td>
<td>Process crime scenes.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0194</td>
<td>Properly document all systems security implementation, operations and maintenance activities and update as necessary.</td>
</tr>
<tr>
<td>T0195</td>
<td>Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.</td>
</tr>
<tr>
<td>T0196</td>
<td>Provide advice on project costs, design concepts, or design changes.</td>
</tr>
<tr>
<td>T0197</td>
<td>Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances.</td>
</tr>
<tr>
<td>T0198</td>
<td>Provide daily summary reports of network events and activity relevant to cyber defense practices.</td>
</tr>
<tr>
<td>T0200</td>
<td>Provide feedback on network requirements, including network architecture and infrastructure.</td>
</tr>
<tr>
<td>T0201</td>
<td>Provide guidelines for implementing developed systems to customers or installation teams.</td>
</tr>
<tr>
<td>T0202</td>
<td>Provide cybersecurity guidance to leadership.</td>
</tr>
<tr>
<td>T0203</td>
<td>Provide input on security requirements to be included in statements of work and other appropriate procurement documents.</td>
</tr>
<tr>
<td>T0204</td>
<td>Provide input to implementation plans and standard operating procedures.</td>
</tr>
<tr>
<td>T0205</td>
<td>Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).</td>
</tr>
<tr>
<td>T0206</td>
<td>Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.</td>
</tr>
<tr>
<td>T0207</td>
<td>Provide ongoing optimization and problem solving support.</td>
</tr>
<tr>
<td>T0208</td>
<td>Provide recommendations for possible improvements and upgrades.</td>
</tr>
<tr>
<td>T0209</td>
<td>Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.</td>
</tr>
<tr>
<td>T0210</td>
<td>Provide recommendations on new database technologies and architectures.</td>
</tr>
<tr>
<td>T0211</td>
<td>Provide system related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.</td>
</tr>
<tr>
<td>T0212</td>
<td>Provide technical assistance on digital evidence matters to appropriate personnel.</td>
</tr>
<tr>
<td>T0213</td>
<td>Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.</td>
</tr>
<tr>
<td>T0214</td>
<td>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.</td>
</tr>
<tr>
<td>T0215</td>
<td>Recognize a possible security violation and take appropriate action to report the incident, as required.</td>
</tr>
<tr>
<td>T0216</td>
<td>Recognize and accurately report forensic artifacts indicative of a particular operating system.</td>
</tr>
<tr>
<td>T0217</td>
<td>Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.</td>
</tr>
<tr>
<td>T0218</td>
<td>Recommend new or revised security, resilience, and dependability measures based on the results of reviews.</td>
</tr>
<tr>
<td>T0219</td>
<td>Recommend resource allocations required to securely operate and maintain an organization’s cybersecurity requirements.</td>
</tr>
<tr>
<td>T0220</td>
<td>Resolve conflicts in laws, regulations, policies, standards, or procedures.</td>
</tr>
<tr>
<td>T0221</td>
<td>Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.</td>
</tr>
<tr>
<td>T0222</td>
<td>Review existing and proposed policies with stakeholders.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0223</td>
<td>Review or conduct audits of information technology (IT) programs and projects.</td>
</tr>
<tr>
<td>T0224</td>
<td>Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).</td>
</tr>
<tr>
<td>T0225</td>
<td>Secure the electronic device or information source.</td>
</tr>
<tr>
<td>T0226</td>
<td>Serve on agency and interagency policy boards.</td>
</tr>
<tr>
<td>T0227</td>
<td>Recommend policy and coordinate review and approval.</td>
</tr>
<tr>
<td>T0228</td>
<td>Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.</td>
</tr>
<tr>
<td>T0229</td>
<td>Support the design and execution of exercise scenarios.</td>
</tr>
<tr>
<td>T0230</td>
<td>Provide support to security/certification test and evaluation activities.</td>
</tr>
<tr>
<td>T0231</td>
<td>Test and maintain network infrastructure including software and hardware devices.</td>
</tr>
<tr>
<td>T0232</td>
<td>Track and document cyber defense incidents from initial detection through final resolution.</td>
</tr>
<tr>
<td>T0233</td>
<td>Track audit findings and recommendations to ensure appropriate mitigation actions are taken.</td>
</tr>
<tr>
<td>T0234</td>
<td>Translate functional requirements into technical solutions.</td>
</tr>
<tr>
<td>T0235</td>
<td>Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.</td>
</tr>
<tr>
<td>T0236</td>
<td>Troubleshoot system hardware and software.</td>
</tr>
<tr>
<td>T0237</td>
<td>Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).</td>
</tr>
<tr>
<td>T0238</td>
<td>Use federal and organization-specific published documents to manage operations of their computing environment system(s).</td>
</tr>
<tr>
<td>T0239</td>
<td>Capture and analyze network traffic associated with malicious activities using network monitoring tools.</td>
</tr>
<tr>
<td>T0240</td>
<td>Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.</td>
</tr>
<tr>
<td>T0241</td>
<td>Utilize models and simulations to analyze or predict system performance under different operating conditions.</td>
</tr>
<tr>
<td>T0242</td>
<td>Verify and update security documentation reflecting the application/system security design features.</td>
</tr>
<tr>
<td>T0243</td>
<td>Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.</td>
</tr>
<tr>
<td>T0244</td>
<td>Verify that the software application/network/system accreditation and assurance documentation is current.</td>
</tr>
<tr>
<td>T0245</td>
<td>Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.</td>
</tr>
<tr>
<td>T0246</td>
<td>Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.</td>
</tr>
<tr>
<td>T0247</td>
<td>Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.</td>
</tr>
<tr>
<td>T0248</td>
<td>Research current technology to understand capabilities of required system or network.</td>
</tr>
<tr>
<td>T0249</td>
<td>Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.</td>
</tr>
<tr>
<td>T0250</td>
<td>Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).</td>
</tr>
<tr>
<td>T0251</td>
<td>Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).</td>
</tr>
<tr>
<td>T0252</td>
<td>Conduct cursory binary analysis.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0254</td>
<td>Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.</td>
</tr>
<tr>
<td>T0255</td>
<td>Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.</td>
</tr>
<tr>
<td>T0256</td>
<td>Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.</td>
</tr>
<tr>
<td>T0257</td>
<td>Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.</td>
</tr>
<tr>
<td>T0258</td>
<td>Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.</td>
</tr>
<tr>
<td>T0259</td>
<td>Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>T0260</td>
<td>Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.</td>
</tr>
<tr>
<td>T0261</td>
<td>Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.</td>
</tr>
<tr>
<td>T0262</td>
<td>Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).</td>
</tr>
<tr>
<td>T0263</td>
<td>Identify security requirements specific to an information technology (IT) system in all phases of the System Life Cycle.</td>
</tr>
<tr>
<td>T0264</td>
<td>Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.</td>
</tr>
<tr>
<td>T0265</td>
<td>Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.</td>
</tr>
<tr>
<td>T0266</td>
<td>Perform penetration testing as required for new or updated applications.</td>
</tr>
<tr>
<td>T0267</td>
<td>Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.</td>
</tr>
<tr>
<td>T0268</td>
<td>Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.</td>
</tr>
<tr>
<td>T0269</td>
<td>Design and develop key management functions (as related to cybersecurity).</td>
</tr>
<tr>
<td>T0270</td>
<td>Analyze user needs and requirements to plan and conduct system security development.</td>
</tr>
<tr>
<td>T0271</td>
<td>Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).</td>
</tr>
<tr>
<td>T0272</td>
<td>Ensure security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.</td>
</tr>
<tr>
<td>T0273</td>
<td>Develop and document supply chain risks for critical system elements, as appropriate.</td>
</tr>
<tr>
<td>T0274</td>
<td>Create auditable evidence of security measures.</td>
</tr>
<tr>
<td>T0275</td>
<td>Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs).</td>
</tr>
<tr>
<td>T0276</td>
<td>Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.</td>
</tr>
<tr>
<td>T0277</td>
<td>Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0278</td>
<td>Collect intrusion artifacts (e.g., source code, malware, trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.</td>
</tr>
<tr>
<td>T0279</td>
<td>Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.</td>
</tr>
<tr>
<td>T0280</td>
<td>Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.</td>
</tr>
<tr>
<td>T0281</td>
<td>Forecast ongoing service demands and ensure security assumptions are reviewed as necessary.</td>
</tr>
<tr>
<td>T0282</td>
<td>Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.</td>
</tr>
<tr>
<td>T0283</td>
<td>Collaborate with stakeholders to identify and/or develop appropriate solutions technology.</td>
</tr>
<tr>
<td>T0284</td>
<td>Design and develop new tools/technologies as related to cybersecurity.</td>
</tr>
<tr>
<td>T0285</td>
<td>Perform virus scanning on digital media.</td>
</tr>
<tr>
<td>T0286</td>
<td>Perform file system forensic analysis.</td>
</tr>
<tr>
<td>T0287</td>
<td>Perform static analysis to mount an &quot;image&quot; of a drive (without necessarily having the original drive).</td>
</tr>
<tr>
<td>T0288</td>
<td>Perform static malware analysis.</td>
</tr>
<tr>
<td>T0289</td>
<td>Utilize deployable forensics tool kit to support operations as necessary.</td>
</tr>
<tr>
<td>T0290</td>
<td>Determine tactics, techniques, and procedures (TTPs) for intrusion sets.</td>
</tr>
<tr>
<td>T0291</td>
<td>Examine network topologies to understand data flows through the network.</td>
</tr>
<tr>
<td>T0292</td>
<td>Recommend computing environment vulnerability corrections.</td>
</tr>
<tr>
<td>T0293</td>
<td>Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).</td>
</tr>
<tr>
<td>T0294</td>
<td>Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).</td>
</tr>
<tr>
<td>T0295</td>
<td>Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.</td>
</tr>
<tr>
<td>T0296</td>
<td>Isolate and remove malware.</td>
</tr>
<tr>
<td>T0297</td>
<td>Identify applications and operating systems of a network device based on network traffic.</td>
</tr>
<tr>
<td>T0298</td>
<td>Reconstruct a malicious attack or activity based off network traffic.</td>
</tr>
<tr>
<td>T0299</td>
<td>Identify network mapping and operating system (OS) fingerprinting activities.</td>
</tr>
<tr>
<td>T0300</td>
<td>Develop and document User Experience (UX) requirements including information architecture and user interface requirements.</td>
</tr>
<tr>
<td>T0301</td>
<td>Develop and implement cybersecurity independent audit processes for application software/networks/systems and oversee ongoing independent audits to ensure that operational and Research and Design (R&amp;D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by Systems Administrators and other cybersecurity staff when performing their day-to-day activities.</td>
</tr>
<tr>
<td>T0302</td>
<td>Develop contract language to ensure supply chain, system, network, and operational security are met.</td>
</tr>
<tr>
<td>T0303</td>
<td>Identify and leverage the enterprise-wide version control system while designing and developing secure applications.</td>
</tr>
<tr>
<td>T0304</td>
<td>Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.</td>
</tr>
<tr>
<td>T0305</td>
<td>Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.</td>
</tr>
<tr>
<td>T0306</td>
<td>Supports incident management, service level management, change management, release management, continuity management, and availability management for databases and data management systems.</td>
</tr>
<tr>
<td>T0307</td>
<td>Analyze candidate architectures, allocate security services, and select security mechanisms.</td>
</tr>
<tr>
<td>T0308</td>
<td>Analyze incident data for emerging trends.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td>T0309</td>
<td>Assess the effectiveness of security controls.</td>
</tr>
<tr>
<td>T0310</td>
<td>Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the NE or enclave.</td>
</tr>
<tr>
<td>T0311</td>
<td>Consult with customers about software system design and maintenance.</td>
</tr>
<tr>
<td>T0312</td>
<td>Coordinate with intelligence analysts to correlate threat assessment data.</td>
</tr>
<tr>
<td>T0313</td>
<td>Design and document quality standards.</td>
</tr>
<tr>
<td>T0314</td>
<td>Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.</td>
</tr>
<tr>
<td>T0315</td>
<td>Develop and deliver technical training to educate others or meet customer needs.</td>
</tr>
<tr>
<td>T0316</td>
<td>Develop or assist in the development of computer based training modules or classes.</td>
</tr>
<tr>
<td>T0317</td>
<td>Develop or assist in the development of course assignments.</td>
</tr>
<tr>
<td>T0318</td>
<td>Develop or assist in the development of course evaluations.</td>
</tr>
<tr>
<td>T0319</td>
<td>Develop or assist in the development of grading and proficiency standards.</td>
</tr>
<tr>
<td>T0320</td>
<td>Assist in the development of individual/collective development, training, and/or remediation plans.</td>
</tr>
<tr>
<td>T0321</td>
<td>Develop or assist in the development of learning objectives and goals.</td>
</tr>
<tr>
<td>T0322</td>
<td>Develop or assist in the development of on-the-job training materials or programs.</td>
</tr>
<tr>
<td>T0323</td>
<td>Develop or assist in the development of written tests for measuring and assessing learner proficiency.</td>
</tr>
<tr>
<td>T0324</td>
<td>Direct software programming and development of documentation.</td>
</tr>
<tr>
<td>T0325</td>
<td>Document a system's purpose and preliminary system security concept of operations.</td>
</tr>
<tr>
<td>T0326</td>
<td>Employ configuration management processes.</td>
</tr>
<tr>
<td>T0327</td>
<td>Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.</td>
</tr>
<tr>
<td>T0328</td>
<td>Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.</td>
</tr>
<tr>
<td>T0329</td>
<td>Follow software and systems engineering life cycle standards and processes.</td>
</tr>
<tr>
<td>T0330</td>
<td>Maintain assured message delivery systems.</td>
</tr>
<tr>
<td>T0331</td>
<td>Maintain incident tracking and solution database.</td>
</tr>
<tr>
<td>T0332</td>
<td>Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.</td>
</tr>
<tr>
<td>T0333</td>
<td>Perform cyber defense trend analysis and reporting.</td>
</tr>
<tr>
<td>T0334</td>
<td>Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).</td>
</tr>
<tr>
<td>T0335</td>
<td>Build, install, configure, and test dedicated cyber defense hardware.</td>
</tr>
<tr>
<td>T0336</td>
<td>Withdrawn: Integrated with T0228</td>
</tr>
<tr>
<td>T0337</td>
<td>Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.</td>
</tr>
<tr>
<td>T0338</td>
<td>Write detailed functional specifications that document the architecture development process.</td>
</tr>
<tr>
<td>T0339</td>
<td>Leads efforts to promote the organization's use of knowledge management and information sharing.</td>
</tr>
<tr>
<td>T0340</td>
<td>Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0341</td>
<td>Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.</td>
</tr>
<tr>
<td>T0342</td>
<td>Analyze data sources to provide actionable recommendations.</td>
</tr>
<tr>
<td>T0343</td>
<td>Analyze the crisis situation to ensure public, personal, and resource protection.</td>
</tr>
<tr>
<td>T0344</td>
<td>Assess all the configuration management (change configuration/release management) processes.</td>
</tr>
<tr>
<td>T0345</td>
<td>Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.</td>
</tr>
<tr>
<td>T0346</td>
<td>Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.</td>
</tr>
<tr>
<td>T0347</td>
<td>Assess the validity of source data and subsequent findings.</td>
</tr>
<tr>
<td>T0348</td>
<td>Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.</td>
</tr>
<tr>
<td>T0349</td>
<td>Collect metrics and trending data.</td>
</tr>
<tr>
<td>T0351</td>
<td>Conduct a market analysis to identify, assess, and recommend commercial, GOTS, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.</td>
</tr>
<tr>
<td>T0352</td>
<td>Conduct hypothesis testing using statistical processes.</td>
</tr>
<tr>
<td>T0353</td>
<td>Conduct learning needs assessments and identify requirements.</td>
</tr>
<tr>
<td>T0354</td>
<td>Confer with systems analysts, engineers, programmers and others to design application.</td>
</tr>
<tr>
<td>T0355</td>
<td>Coordinate and manage the overall service provided to a customer end-to-end.</td>
</tr>
<tr>
<td>T0356</td>
<td>Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.</td>
</tr>
<tr>
<td>T0357</td>
<td>Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.</td>
</tr>
<tr>
<td>T0358</td>
<td>Create interactive learning exercises to create an effective learning environment.</td>
</tr>
<tr>
<td>T0359</td>
<td>Design and develop system administration and management functionality for privileged access users.</td>
</tr>
<tr>
<td>T0360</td>
<td>Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.</td>
</tr>
<tr>
<td>T0361</td>
<td>Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.</td>
</tr>
<tr>
<td>T0362</td>
<td>Develop and facilitate data-gathering methods.</td>
</tr>
<tr>
<td>T0363</td>
<td>Develop and implement standardized position descriptions based on established cyber work roles.</td>
</tr>
<tr>
<td>T0364</td>
<td>Develop and review recruiting, hiring, and retention procedures in accordance with current Human Resource (HR) policies.</td>
</tr>
<tr>
<td>T0365</td>
<td>Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.</td>
</tr>
<tr>
<td>T0366</td>
<td>Develop or assist in the development of training policies and protocols for cyber training.</td>
</tr>
<tr>
<td>T0367</td>
<td>Develop strategic insights from large data sets.</td>
</tr>
<tr>
<td>T0368</td>
<td>Develop the goals and objectives for cyber curriculum.</td>
</tr>
<tr>
<td>T0369</td>
<td>Ensure cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.</td>
</tr>
</tbody>
</table>

43
<table>
<thead>
<tr>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0370</td>
<td>Ensure that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.</td>
</tr>
<tr>
<td>T0371</td>
<td>Establish acceptable limits for the software application, network, or system.</td>
</tr>
<tr>
<td>T0372</td>
<td>Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.</td>
</tr>
<tr>
<td>T0373</td>
<td>Establish and oversee waiver processes for cyber career field entry and training qualification requirements.</td>
</tr>
<tr>
<td>T0374</td>
<td>Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.</td>
</tr>
<tr>
<td>T0375</td>
<td>Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.</td>
</tr>
<tr>
<td>T0376</td>
<td>Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.</td>
</tr>
<tr>
<td>T0377</td>
<td>Gather feedback on customer satisfaction and internal service performance to foster continual improvement.</td>
</tr>
<tr>
<td>T0378</td>
<td>Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).</td>
</tr>
<tr>
<td>T0379</td>
<td>Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).</td>
</tr>
<tr>
<td>T0380</td>
<td>Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.</td>
</tr>
<tr>
<td>T0381</td>
<td>Present technical information to technical and non-technical audiences.</td>
</tr>
<tr>
<td>T0382</td>
<td>Present data in creative formats.</td>
</tr>
<tr>
<td>T0383</td>
<td>Program custom algorithms.</td>
</tr>
<tr>
<td>T0384</td>
<td>Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.</td>
</tr>
<tr>
<td>T0385</td>
<td>Provide actionable recommendations to critical stakeholders based on data analysis and findings.</td>
</tr>
<tr>
<td>T0386</td>
<td>Provide criminal investigative support to trial counsel during the judicial process.</td>
</tr>
<tr>
<td>T0387</td>
<td>Review and apply cyber career field qualification standards.</td>
</tr>
<tr>
<td>T0388</td>
<td>Review and apply organizational policies related to or having an effect on the cyber workforce.</td>
</tr>
<tr>
<td>T0389</td>
<td>Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.</td>
</tr>
<tr>
<td>T0390</td>
<td>Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.</td>
</tr>
<tr>
<td>T0391</td>
<td>Support integration of qualified cyber workforce personnel into information systems lifecycle development processes.</td>
</tr>
<tr>
<td>T0392</td>
<td>Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.</td>
</tr>
<tr>
<td>T0393</td>
<td>Validate specifications and requirements for testability.</td>
</tr>
<tr>
<td>T0394</td>
<td>Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.</td>
</tr>
<tr>
<td>T0395</td>
<td>Write and publish after action reviews.</td>
</tr>
<tr>
<td>T0396</td>
<td>Process image with appropriate tools depending on analyst’s goals.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0397</td>
<td>Perform Windows registry analysis.</td>
</tr>
<tr>
<td>T0398</td>
<td>Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.</td>
</tr>
<tr>
<td>T0399</td>
<td>Enter media information into tracking database (e.g. Product Tracker Tool) for digital media that has been acquired.</td>
</tr>
<tr>
<td>T0400</td>
<td>Correlate incident data and perform cyber defense reporting.</td>
</tr>
<tr>
<td>T0401</td>
<td>Maintain deployable cyber defense toolkit (e.g. specialized cyber defense software/hardware) to support IRT mission.</td>
</tr>
<tr>
<td>T0402</td>
<td>Effectively allocate storage capacity in the design of data management systems.</td>
</tr>
<tr>
<td>T0403</td>
<td>Read, interpret, write, modify, and execute simple scripts (e.g., PERL, VBS) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).</td>
</tr>
<tr>
<td>T0404</td>
<td>Utilize different programming languages to write code, open files, read files, and write output to different files.</td>
</tr>
<tr>
<td>T0405</td>
<td>Utilize opens source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).</td>
</tr>
<tr>
<td>T0406</td>
<td>Ensure design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.</td>
</tr>
<tr>
<td>T0407</td>
<td>Participate in the acquisition process as necessary.</td>
</tr>
<tr>
<td>T0408</td>
<td>Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.</td>
</tr>
<tr>
<td>T0409</td>
<td>Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.</td>
</tr>
<tr>
<td>T0410</td>
<td>Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.</td>
</tr>
<tr>
<td>T0411</td>
<td>Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.</td>
</tr>
<tr>
<td>T0412</td>
<td>Conduct import/export reviews for acquiring systems and software.</td>
</tr>
<tr>
<td>T0413</td>
<td>Develop data management capabilities (e.g., cloud based, centralized cryptographic key management) to include support to the mobile workforce.</td>
</tr>
<tr>
<td>T0414</td>
<td>Develop supply chain, system, network, performance, and cyber security requirements.</td>
</tr>
<tr>
<td>T0415</td>
<td>Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.</td>
</tr>
<tr>
<td>T0416</td>
<td>Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.</td>
</tr>
<tr>
<td>T0417</td>
<td>Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Anti-Virus solution) when appropriate.</td>
</tr>
<tr>
<td>T0418</td>
<td>Install, update, and troubleshoot systems/servers.</td>
</tr>
<tr>
<td>T0419</td>
<td>Acquire and maintain a working knowledge of constitutional issues relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.</td>
</tr>
<tr>
<td>T0420</td>
<td>Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).</td>
</tr>
<tr>
<td>T0421</td>
<td>Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).</td>
</tr>
<tr>
<td>T0422</td>
<td>Implement data management standards, requirements, and specifications.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0423</td>
<td>Analyze computer-generated threats for counter intelligence or criminal activity.</td>
</tr>
<tr>
<td>T0424</td>
<td>Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.</td>
</tr>
<tr>
<td>T0425</td>
<td>Analyze organizational cyber policy.</td>
</tr>
<tr>
<td>T0426</td>
<td>Analyze the results of software, hardware, or interoperability testing.</td>
</tr>
<tr>
<td>T0427</td>
<td>Analyze user needs and requirements to plan architecture.</td>
</tr>
<tr>
<td>T0428</td>
<td>Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.</td>
</tr>
<tr>
<td>T0429</td>
<td>Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.</td>
</tr>
<tr>
<td>T0430</td>
<td>Gather and preserve evidence used on the prosecution of computer crimes.</td>
</tr>
<tr>
<td>T0431</td>
<td>Check system hardware availability, functionality, integrity, and efficiency.</td>
</tr>
<tr>
<td>T0432</td>
<td>Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.</td>
</tr>
<tr>
<td>T0433</td>
<td>Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.</td>
</tr>
<tr>
<td>T0434</td>
<td>Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.</td>
</tr>
<tr>
<td>T0435</td>
<td>Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.</td>
</tr>
<tr>
<td>T0436</td>
<td>Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.</td>
</tr>
<tr>
<td>T0437</td>
<td>Correlates training and learning to business or mission requirements.</td>
</tr>
<tr>
<td>T0438</td>
<td>Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).</td>
</tr>
<tr>
<td>T0439</td>
<td>Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.</td>
</tr>
<tr>
<td>T0440</td>
<td>Captures and integrates essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.</td>
</tr>
<tr>
<td>T0441</td>
<td>Define and integrate current and future mission environments.</td>
</tr>
<tr>
<td>T0442</td>
<td>Create training courses tailored to the audience and physical environment.</td>
</tr>
<tr>
<td>T0443</td>
<td>Deliver training courses tailored to the audience and physical/virtual environments.</td>
</tr>
<tr>
<td>T0444</td>
<td>Apply concepts, procedures, software, equipment, and/or technology applications to students.</td>
</tr>
<tr>
<td>T0445</td>
<td>Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.</td>
</tr>
<tr>
<td>T0446</td>
<td>Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.</td>
</tr>
<tr>
<td>T0447</td>
<td>Design hardware, operating systems, and software applications to adequately address requirements.</td>
</tr>
<tr>
<td>T0448</td>
<td>Develop enterprise architecture or system components required to meet user needs.</td>
</tr>
<tr>
<td>T0449</td>
<td>Design to security requirements to ensure requirements are met for all systems and/or applications.</td>
</tr>
<tr>
<td>T0450</td>
<td>Design training curriculum and course content based on requirements.</td>
</tr>
<tr>
<td>T0451</td>
<td>Participate in development of training curriculum and course content.</td>
</tr>
<tr>
<td>T0452</td>
<td>Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital.</td>
</tr>
<tr>
<td>T0453</td>
<td>Determine and develop leads and identify sources of information in order to identify and/or prosecute the responsible parties to an intrusion or other crimes.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0454</td>
<td>Define baseline security requirements in accordance with applicable guidelines.</td>
</tr>
<tr>
<td>T0455</td>
<td>Develop software system testing and validation procedures, programming, and documentation.</td>
</tr>
<tr>
<td>T0456</td>
<td>Develop secure software testing and validation procedures.</td>
</tr>
<tr>
<td>T0457</td>
<td>Develop system testing and validation procedures, programming, and documentation.</td>
</tr>
<tr>
<td>T0458</td>
<td>Comply with organization systems administration standard operating procedures.</td>
</tr>
<tr>
<td>T0459</td>
<td>Implement data mining and data warehousing applications.</td>
</tr>
<tr>
<td>T0460</td>
<td>Develop and implement data mining and data warehousing programs.</td>
</tr>
<tr>
<td>T0461</td>
<td>Implement and enforce local network usage policies and procedures.</td>
</tr>
<tr>
<td>T0462</td>
<td>Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.</td>
</tr>
<tr>
<td>T0463</td>
<td>Develop cost estimates for new or modified system(s).</td>
</tr>
<tr>
<td>T0464</td>
<td>Develop detailed design documentation for component and interface specifications to support system design and development.</td>
</tr>
<tr>
<td>T0465</td>
<td>Develop guidelines for implementation.</td>
</tr>
<tr>
<td>T0466</td>
<td>Develop mitigation strategies to address cost, schedule, performance, and security risks.</td>
</tr>
<tr>
<td>T0467</td>
<td>Ensure training meets the goals and objectives for cybersecurity training, education, or awareness.</td>
</tr>
<tr>
<td>T0468</td>
<td>Diagnose and resolve customer reported system incidents, problems, and events.</td>
</tr>
<tr>
<td>T0469</td>
<td>Analyze and report organizational security posture trends.</td>
</tr>
<tr>
<td>T0470</td>
<td>Analyze and report system security posture trends.</td>
</tr>
<tr>
<td>T0471</td>
<td>Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).</td>
</tr>
<tr>
<td>T0472</td>
<td>Draft, staff, and publish cyber policy.</td>
</tr>
<tr>
<td>T0473</td>
<td>Document and update as necessary all definition and architecture activities.</td>
</tr>
<tr>
<td>T0474</td>
<td>Provide legal analysis and decisions to inspector generals, privacy officers, oversight and compliance personnel with regard to compliance with cybersecurity policies and relevant legal and regulatory requirements.</td>
</tr>
<tr>
<td>T0475</td>
<td>Assess adequate access controls based on principles of least privilege and need-to-know.</td>
</tr>
<tr>
<td>T0476</td>
<td>Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.</td>
</tr>
<tr>
<td>T0477</td>
<td>Ensure the execution of disaster recovery and continuity of operations.</td>
</tr>
<tr>
<td>T0478</td>
<td>Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.</td>
</tr>
<tr>
<td>T0479</td>
<td>Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.</td>
</tr>
<tr>
<td>T0480</td>
<td>Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.</td>
</tr>
<tr>
<td>T0481</td>
<td>Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).</td>
</tr>
<tr>
<td>T0482</td>
<td>Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.</td>
</tr>
<tr>
<td>T0483</td>
<td>Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).</td>
</tr>
<tr>
<td>T0484</td>
<td>Document the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.</td>
</tr>
<tr>
<td>T0485</td>
<td>Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0486</td>
<td>Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&amp;A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.</td>
</tr>
<tr>
<td>T0487</td>
<td>Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.</td>
</tr>
<tr>
<td>T0488</td>
<td>Implement designs for new or existing system(s).</td>
</tr>
<tr>
<td>T0489</td>
<td>Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.</td>
</tr>
<tr>
<td>T0490</td>
<td>Install and configure database management systems and software.</td>
</tr>
<tr>
<td>T0491</td>
<td>Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.</td>
</tr>
<tr>
<td>T0492</td>
<td>Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.</td>
</tr>
<tr>
<td>T0493</td>
<td>Lead and oversee budget, staffing, and contracting.</td>
</tr>
<tr>
<td>T0494</td>
<td>Administer accounts, network rights, and access to systems and equipment.</td>
</tr>
<tr>
<td>T0495</td>
<td>Manage Accreditation Packages (e.g., ISO/IEC 15026-2).</td>
</tr>
<tr>
<td>T0496</td>
<td>Perform the management/inventory of information technology (IT) resources.</td>
</tr>
<tr>
<td>T0497</td>
<td>Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.</td>
</tr>
<tr>
<td>T0498</td>
<td>Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.</td>
</tr>
<tr>
<td>T0499</td>
<td>Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.</td>
</tr>
<tr>
<td>T0500</td>
<td>Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.</td>
</tr>
<tr>
<td>T0501</td>
<td>Monitor and maintain system/server configuration.</td>
</tr>
<tr>
<td>T0502</td>
<td>Monitor and report client-level computer system performance.</td>
</tr>
<tr>
<td>T0503</td>
<td>Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.</td>
</tr>
<tr>
<td>T0504</td>
<td>Assess and monitor cybersecurity related to system implementation and testing practices.</td>
</tr>
<tr>
<td>T0505</td>
<td>Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.</td>
</tr>
<tr>
<td>T0506</td>
<td>Seek consensus on proposed policy changes from stakeholders.</td>
</tr>
<tr>
<td>T0507</td>
<td>Oversee installation, implementation, configuration, and support of system components.</td>
</tr>
<tr>
<td>T0508</td>
<td>Verify minimum security requirements are in place for all applications.</td>
</tr>
<tr>
<td>T0509</td>
<td>Perform an information security risk assessment.</td>
</tr>
<tr>
<td>T0510</td>
<td>Coordinate incident response functions.</td>
</tr>
<tr>
<td>T0511</td>
<td>Perform developmental testing on systems under development.</td>
</tr>
<tr>
<td>T0512</td>
<td>Perform interoperability testing on systems exchanging electronic information with other systems.</td>
</tr>
<tr>
<td>T0513</td>
<td>Perform operational testing.</td>
</tr>
<tr>
<td>T0514</td>
<td>Diagnose faulty system/server hardware.</td>
</tr>
<tr>
<td>T0515</td>
<td>Perform repairs on faulty system/server hardware.</td>
</tr>
<tr>
<td>T0516</td>
<td>Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.</td>
</tr>
<tr>
<td>T0517</td>
<td>Integrate results regarding the identification of gaps in security architecture.</td>
</tr>
<tr>
<td>T0518</td>
<td>Perform security reviews and identify security gaps in architecture.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0519</td>
<td>Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment.</td>
</tr>
<tr>
<td>T0520</td>
<td>Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).</td>
</tr>
<tr>
<td>T0521</td>
<td>Plan implementation strategy to ensure enterprise components can be integrated and aligned.</td>
</tr>
<tr>
<td>T0522</td>
<td>Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).</td>
</tr>
<tr>
<td>T0523</td>
<td>Prepare reports to document the investigation following legal standards and requirements.</td>
</tr>
<tr>
<td>T0524</td>
<td>Promote knowledge sharing between information owners/users through an organization’s operational processes and systems.</td>
</tr>
<tr>
<td>T0525</td>
<td>Provide enterprise cybersecurity and supply chain risk management guidance.</td>
</tr>
<tr>
<td>T0526</td>
<td>Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.</td>
</tr>
<tr>
<td>T0527</td>
<td>Provide input to implementation plans and standard operating procedures as they relate to information systems security.</td>
</tr>
<tr>
<td>T0528</td>
<td>Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials.</td>
</tr>
<tr>
<td>T0529</td>
<td>Provide policy guidance to cyber management, staff, and users.</td>
</tr>
<tr>
<td>T0530</td>
<td>Develop a trend analysis and impact report.</td>
</tr>
<tr>
<td>T0531</td>
<td>Troubleshoot hardware/software interface and interoperability problems.</td>
</tr>
<tr>
<td>T0532</td>
<td>Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.</td>
</tr>
<tr>
<td>T0533</td>
<td>Review, conduct, or participate in audits of cyber programs and projects.</td>
</tr>
<tr>
<td>T0534</td>
<td>Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).</td>
</tr>
<tr>
<td>T0535</td>
<td>Recommend revisions to curriculum end course content based on feedback from previous training sessions.</td>
</tr>
<tr>
<td>T0536</td>
<td>Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).</td>
</tr>
<tr>
<td>T0537</td>
<td>Support the CIO in the formulation of cyber-related policies.</td>
</tr>
<tr>
<td>T0538</td>
<td>Provide support to test and evaluation activities.</td>
</tr>
<tr>
<td>T0539</td>
<td>Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.</td>
</tr>
<tr>
<td>T0540</td>
<td>Record and manage test data.</td>
</tr>
<tr>
<td>T0541</td>
<td>Trace system requirements to design components and perform gap analysis.</td>
</tr>
<tr>
<td>T0542</td>
<td>Translate proposed capabilities into technical requirements.</td>
</tr>
<tr>
<td>T0543</td>
<td>Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis.</td>
</tr>
<tr>
<td>T0544</td>
<td>Verify stability, interoperability, portability, and/or scalability of system architecture.</td>
</tr>
<tr>
<td>T0545</td>
<td>Work with stakeholders to resolve computer security incidents and vulnerability compliance.</td>
</tr>
<tr>
<td>T0546</td>
<td>Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.</td>
</tr>
<tr>
<td>T0547</td>
<td>Research and evaluate available technologies and standards to meet customer requirements.</td>
</tr>
<tr>
<td>T0548</td>
<td>Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.</td>
</tr>
<tr>
<td>T0549</td>
<td>Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0550</td>
<td>Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).</td>
</tr>
<tr>
<td>T0551</td>
<td>Draft and publish supply chain security and risk management documents.</td>
</tr>
<tr>
<td>T0552</td>
<td>Review and approve a supply chain security/risk management policy.</td>
</tr>
<tr>
<td>T0553</td>
<td>Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.</td>
</tr>
<tr>
<td>T0554</td>
<td>Determine and document software patches or the extent of releases that would leave software vulnerable.</td>
</tr>
<tr>
<td>T0555</td>
<td>Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.</td>
</tr>
<tr>
<td>T0556</td>
<td>Assess and design security management functions as related to cyberspace.</td>
</tr>
<tr>
<td>T0557</td>
<td>Integrate key management functions as related to cyberspace.</td>
</tr>
<tr>
<td>T0558</td>
<td>Analyze user needs and requirements to plan and conduct system development.</td>
</tr>
<tr>
<td>T0559</td>
<td>Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations).</td>
</tr>
<tr>
<td>T0560</td>
<td>Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).</td>
</tr>
<tr>
<td>T0561</td>
<td>Accurately characterize targets.</td>
</tr>
<tr>
<td>T0562</td>
<td>Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.</td>
</tr>
<tr>
<td>T0563</td>
<td>Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.</td>
</tr>
<tr>
<td>T0564</td>
<td>Analyze feedback to determine extent to which collection products and services are meeting requirements.</td>
</tr>
<tr>
<td>T0565</td>
<td>Analyze incoming collection requests.</td>
</tr>
<tr>
<td>T0566</td>
<td>Analyze own operational architecture, tools, and procedures for ways to improve performance.</td>
</tr>
<tr>
<td>T0567</td>
<td>Analyze target operational architecture for ways to gain access.</td>
</tr>
<tr>
<td>T0568</td>
<td>Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirements, interagency/international agreements.</td>
</tr>
<tr>
<td>T0569</td>
<td>Answer requests for information.</td>
</tr>
<tr>
<td>T0570</td>
<td>Apply and utilize authorized cyber capabilities to enable access to targeted networks.</td>
</tr>
<tr>
<td>T0571</td>
<td>Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.</td>
</tr>
<tr>
<td>T0572</td>
<td>Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.</td>
</tr>
<tr>
<td>T0573</td>
<td>Assess and apply operational environment factors and risks to collection management process.</td>
</tr>
<tr>
<td>T0574</td>
<td>Apply and obey applicable statutes, laws, regulations and policies.</td>
</tr>
<tr>
<td>T0575</td>
<td>Coordinate for intelligence support to operational planning activities.</td>
</tr>
<tr>
<td>T0576</td>
<td>Assess all-source intelligence and recommend targets to support cyber operation objectives.</td>
</tr>
<tr>
<td>T0577</td>
<td>Assess efficiency of existing information exchange and management systems.</td>
</tr>
<tr>
<td>T0578</td>
<td>Assess performance of collection assets against prescribed specifications.</td>
</tr>
<tr>
<td>T0579</td>
<td>Assess target vulnerabilities and/or operational capabilities to determine course of action.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0580</td>
<td>Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and then adjust collection strategies and collection requirements accordingly.</td>
</tr>
<tr>
<td>T0581</td>
<td>Assist and advise inter-agency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.</td>
</tr>
<tr>
<td>T0582</td>
<td>Provide expertise to course of action development.</td>
</tr>
<tr>
<td>T0583</td>
<td>Provide subject matter expertise to the development of a common operational picture.</td>
</tr>
<tr>
<td>T0584</td>
<td>Maintain a common intelligence picture.</td>
</tr>
<tr>
<td>T0585</td>
<td>Assist subject matter expertise to the development of cyber operations specific indicators.</td>
</tr>
<tr>
<td>T0586</td>
<td>Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.</td>
</tr>
<tr>
<td>T0587</td>
<td>Assist in the development and refinement of priority information requirements.</td>
</tr>
<tr>
<td>T0588</td>
<td>Provide expertise to the development of measures of effectiveness and measures of performance.</td>
</tr>
<tr>
<td>T0589</td>
<td>Assist in the identification of intelligence collection shortfalls.</td>
</tr>
<tr>
<td>T0590</td>
<td>Enable synchronization of intelligence support plans across partner organizations as required.</td>
</tr>
<tr>
<td>T0591</td>
<td>Perform analysis for target infrastructure exploitation activities.</td>
</tr>
<tr>
<td>T0592</td>
<td>Provide input to the identification of cyber-related success criteria.</td>
</tr>
<tr>
<td>T0593</td>
<td>Brief threat and/or target current situations.</td>
</tr>
<tr>
<td>T0594</td>
<td>Build and maintain electronic target folders.</td>
</tr>
<tr>
<td>T0595</td>
<td>Classify documents in accordance with classification guidelines.</td>
</tr>
<tr>
<td>T0596</td>
<td>Close requests for information once satisfied.</td>
</tr>
<tr>
<td>T0597</td>
<td>Collaborate with intelligence analysts/targeting organizations involved in related areas.</td>
</tr>
<tr>
<td>T0598</td>
<td>Collaborate with development organizations to create and deploy the tools needed to achieve objectives.</td>
</tr>
<tr>
<td>T0599</td>
<td>Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.</td>
</tr>
<tr>
<td>T0600</td>
<td>Collaborate with other internal and external partner organizations on target access and operational issues.</td>
</tr>
<tr>
<td>T0601</td>
<td>Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).</td>
</tr>
<tr>
<td>T0602</td>
<td>Collaborates with customer to define information requirements.</td>
</tr>
<tr>
<td>T0603</td>
<td>Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.</td>
</tr>
<tr>
<td>T0604</td>
<td>Compare allocated and available assets to collection demand as expressed through requirements.</td>
</tr>
<tr>
<td>T0605</td>
<td>Compile lessons learned from collection management activity's execution of organization collection objectives.</td>
</tr>
<tr>
<td>T0606</td>
<td>Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.</td>
</tr>
<tr>
<td>T0607</td>
<td>Identify and conduct analysis of target communications to identify information essential to support operations.</td>
</tr>
<tr>
<td>T0608</td>
<td>Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.</td>
</tr>
<tr>
<td>T0609</td>
<td>Conduct access enabling of wireless computer and digital networks.</td>
</tr>
<tr>
<td>T0610</td>
<td>Conduct collection and processing of wireless computer and digital networks.</td>
</tr>
<tr>
<td>T0611</td>
<td>Conduct end-of-operations assessments.</td>
</tr>
<tr>
<td>T0612</td>
<td>Conduct exploitation of wireless computer and digital networks.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0613</td>
<td>Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.</td>
</tr>
<tr>
<td>T0614</td>
<td>Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.</td>
</tr>
<tr>
<td>T0615</td>
<td>Conduct in-depth research and analysis.</td>
</tr>
<tr>
<td>T0616</td>
<td>Conduct network scouting and vulnerability analyses of systems within a network.</td>
</tr>
<tr>
<td>T0617</td>
<td>Conduct nodal analysis.</td>
</tr>
<tr>
<td>T0618</td>
<td>Conduct on-net activities to control and exfiltrate data from deployed technologies.</td>
</tr>
<tr>
<td>T0619</td>
<td>Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.</td>
</tr>
<tr>
<td>T0620</td>
<td>Conduct open source data collection via various online tools.</td>
</tr>
<tr>
<td>T0621</td>
<td>Conduct quality control in order to determine validity and relevance of information gathered about networks.</td>
</tr>
<tr>
<td>T0622</td>
<td>Develop, review and implement all levels of planning guidance in support of cyber operations.</td>
</tr>
<tr>
<td>T0623</td>
<td>Conduct survey of computer and digital networks.</td>
</tr>
<tr>
<td>T0624</td>
<td>Conduct target research and analysis.</td>
</tr>
<tr>
<td>T0625</td>
<td>Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.</td>
</tr>
<tr>
<td>T0626</td>
<td>Construct collection plans and matrixes using established guidance and procedures.</td>
</tr>
<tr>
<td>T0627</td>
<td>Contribute to crisis action planning for cyber operations.</td>
</tr>
<tr>
<td>T0628</td>
<td>Contribute to the development of the organization's decision support tools if necessary.</td>
</tr>
<tr>
<td>T0629</td>
<td>Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers.</td>
</tr>
<tr>
<td>T0630</td>
<td>Incorporate intelligence equities into the overall design of cyber operations plans.</td>
</tr>
<tr>
<td>T0631</td>
<td>Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.</td>
</tr>
<tr>
<td>T0632</td>
<td>Coordinate inclusion of collection plan in appropriate documentation.</td>
</tr>
<tr>
<td>T0633</td>
<td>Coordinate target vetting with appropriate partners.</td>
</tr>
<tr>
<td>T0634</td>
<td>Re-task or re-direct collection assets and resources.</td>
</tr>
<tr>
<td>T0635</td>
<td>Coordinate with intelligence and cyber defense partners to obtain relevant essential information.</td>
</tr>
<tr>
<td>T0636</td>
<td>Coordinate with intelligence planners to ensure collection managers receive information requirements.</td>
</tr>
<tr>
<td>T0637</td>
<td>Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.</td>
</tr>
<tr>
<td>T0638</td>
<td>Coordinate, produce and track intelligence requirements.</td>
</tr>
<tr>
<td>T0639</td>
<td>Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.</td>
</tr>
<tr>
<td>T0640</td>
<td>Uses intelligence estimates to counter potential target actions.</td>
</tr>
<tr>
<td>T0641</td>
<td>Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.</td>
</tr>
<tr>
<td>T0642</td>
<td>Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.</td>
</tr>
<tr>
<td>T0643</td>
<td>Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).</td>
</tr>
<tr>
<td>T0644</td>
<td>Detect exploits against targeted networks and hosts and react accordingly.</td>
</tr>
<tr>
<td>T0645</td>
<td>Determine course of action for addressing changes to objectives, guidance, and operational environment.</td>
</tr>
<tr>
<td>T0646</td>
<td>Determine existing collection management webpage databases, libraries and storehouses.</td>
</tr>
</tbody>
</table>

52
<table>
<thead>
<tr>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0647</td>
<td>Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.</td>
</tr>
<tr>
<td>T0648</td>
<td>Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.</td>
</tr>
<tr>
<td>T0649</td>
<td>Determine organizations and/or echelons with collection authority over all accessible collection assets.</td>
</tr>
<tr>
<td>T0650</td>
<td>Determine what technologies are used by a given target.</td>
</tr>
<tr>
<td>T0651</td>
<td>Develop a method for comparing collection reports to outstanding requirements to identify information gaps.</td>
</tr>
<tr>
<td>T0652</td>
<td>Develop all-source intelligence targeting materials.</td>
</tr>
<tr>
<td>T0653</td>
<td>Apply analytic techniques to gain more target information.</td>
</tr>
<tr>
<td>T0654</td>
<td>Develop and maintain deliberate and/or crisis plans.</td>
</tr>
<tr>
<td>T0655</td>
<td>Develop and review specific cyber operations guidance for integration into broader planning activities.</td>
</tr>
<tr>
<td>T0656</td>
<td>Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.</td>
</tr>
<tr>
<td>T0657</td>
<td>Develop coordinating instructions by collection discipline for each phase of an operation.</td>
</tr>
<tr>
<td>T0658</td>
<td>Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives.</td>
</tr>
<tr>
<td>T0659</td>
<td>Develop detailed intelligence support to cyber operations requirements.</td>
</tr>
<tr>
<td>T0660</td>
<td>Develop information requirements necessary for answering priority information requests.</td>
</tr>
<tr>
<td>T0661</td>
<td>Develop measures of effectiveness and measures of performance.</td>
</tr>
<tr>
<td>T0662</td>
<td>Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.</td>
</tr>
<tr>
<td>T0663</td>
<td>Develop munitions effectiveness assessment or operational assessment materials.</td>
</tr>
<tr>
<td>T0664</td>
<td>Develop new techniques for gaining and keeping access to target systems.</td>
</tr>
<tr>
<td>T0665</td>
<td>Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.</td>
</tr>
<tr>
<td>T0666</td>
<td>Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.</td>
</tr>
<tr>
<td>T0667</td>
<td>Develop potential courses of action.</td>
</tr>
<tr>
<td>T0668</td>
<td>Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.</td>
</tr>
<tr>
<td>T0669</td>
<td>Develop strategy and processes for partner planning, operations, and capability development.</td>
</tr>
<tr>
<td>T0670</td>
<td>Develop, implement, and recommend changes to appropriate planning procedures and policies.</td>
</tr>
<tr>
<td>T0671</td>
<td>Develop, maintain, and assess cyber cooperation security agreements with external partners.</td>
</tr>
<tr>
<td>T0672</td>
<td>Devise, document, and validate cyber operation strategy, and planning documents.</td>
</tr>
<tr>
<td>T0673</td>
<td>Disseminate reports to inform decision makers on collection issues.</td>
</tr>
<tr>
<td>T0674</td>
<td>Disseminate tasking messages and collection plans.</td>
</tr>
<tr>
<td>T0675</td>
<td>Conduct and document an assessment of the collection results using established procedures.</td>
</tr>
<tr>
<td>T0676</td>
<td>Draft cyber intelligence collection and production requirements.</td>
</tr>
<tr>
<td>T0677</td>
<td>Edit or execute simple scripts (e.g., PERL, VBS) on Windows and UNIX systems.</td>
</tr>
<tr>
<td>T0678</td>
<td>Engage customers to understand customers’ intelligence needs and wants.</td>
</tr>
<tr>
<td>T0679</td>
<td>Ensure operational planning efforts are effectively transitioned to current operations.</td>
</tr>
<tr>
<td>T0680</td>
<td>Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0681</td>
<td>Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.</td>
</tr>
<tr>
<td>T0682</td>
<td>Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.</td>
</tr>
<tr>
<td>T0683</td>
<td>Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.</td>
</tr>
<tr>
<td>T0684</td>
<td>Estimate operational effects generated through cyber activities.</td>
</tr>
<tr>
<td>T0685</td>
<td>Evaluate threat decision-making processes.</td>
</tr>
<tr>
<td>T0686</td>
<td>Identify threat vulnerabilities.</td>
</tr>
<tr>
<td>T0687</td>
<td>Identify threats to Blue Force vulnerabilities.</td>
</tr>
<tr>
<td>T0688</td>
<td>Evaluate available capabilities against desired effects in order to recommend efficient solutions.</td>
</tr>
<tr>
<td>T0689</td>
<td>Evaluate extent to which collected information and/or produced intelligence satisfy information requests.</td>
</tr>
<tr>
<td>T0690</td>
<td>Evaluate intelligence estimates to support the planning cycle.</td>
</tr>
<tr>
<td>T0691</td>
<td>Evaluate the conditions that affect employment of available cyber intelligence capabilities.</td>
</tr>
<tr>
<td>T0692</td>
<td>Generate and evaluate the effectiveness of network analysis strategies.</td>
</tr>
<tr>
<td>T0693</td>
<td>Evaluate extent to which collection operations are synchronized with operational requirements.</td>
</tr>
<tr>
<td>T0694</td>
<td>Evaluate the effectiveness of collection operations against the collection plan.</td>
</tr>
<tr>
<td>T0695</td>
<td>Examine intercept-related metadata and content with an understanding of targeting significance.</td>
</tr>
<tr>
<td>T0696</td>
<td>Exploit network devices, security devices, and/or terminals or environments using various methods or tools.</td>
</tr>
<tr>
<td>T0697</td>
<td>Facilitate access enabling by physical and/or wireless means.</td>
</tr>
<tr>
<td>T0698</td>
<td>Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.</td>
</tr>
<tr>
<td>T0699</td>
<td>Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.</td>
</tr>
<tr>
<td>T0700</td>
<td>Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.</td>
</tr>
<tr>
<td>T0701</td>
<td>Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.</td>
</tr>
<tr>
<td>T0702</td>
<td>Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.</td>
</tr>
<tr>
<td>T0703</td>
<td>Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.</td>
</tr>
<tr>
<td>T0704</td>
<td>Incorporate cyber operations and communications security support plans into organization objectives.</td>
</tr>
<tr>
<td>T0705</td>
<td>Incorporate intelligence and counterintelligence to support plan development.</td>
</tr>
<tr>
<td>T0706</td>
<td>Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)</td>
</tr>
<tr>
<td>T0707</td>
<td>Generate requests for information.</td>
</tr>
<tr>
<td>T0708</td>
<td>Identify threat tactics, and methodologies.</td>
</tr>
<tr>
<td>T0709</td>
<td>Identify all available partner intelligence capabilities and limitations supporting cyber operations.</td>
</tr>
<tr>
<td>T0710</td>
<td>Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.</td>
</tr>
<tr>
<td>T0711</td>
<td>Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0712</td>
<td>Identify and manage security cooperation priorities with external partners.</td>
</tr>
<tr>
<td>T0713</td>
<td>Identify and submit intelligence requirements for the purposes of designating priority information requirements.</td>
</tr>
<tr>
<td>T0714</td>
<td>Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.</td>
</tr>
<tr>
<td>T0715</td>
<td>Identify collection gaps and potential collection strategies against targets.</td>
</tr>
<tr>
<td>T0716</td>
<td>Identify coordination requirements and procedures with designated collection authorities.</td>
</tr>
<tr>
<td>T0717</td>
<td>Identify critical target elements.</td>
</tr>
<tr>
<td>T0718</td>
<td>Identify intelligence gaps and shortfalls.</td>
</tr>
<tr>
<td>T0719</td>
<td>Identify cyber intelligence gaps and shortfalls.</td>
</tr>
<tr>
<td>T0720</td>
<td>Identify gaps in our understanding of target technology and developing innovative collection approaches.</td>
</tr>
<tr>
<td>T0721</td>
<td>Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.</td>
</tr>
<tr>
<td>T0722</td>
<td>Identify network components and their functionality to enable analysis and target development.</td>
</tr>
<tr>
<td>T0723</td>
<td>Identify potential collection disciplines for application against priority information requirements.</td>
</tr>
<tr>
<td>T0724</td>
<td>Identify potential points of strength and vulnerability within a network.</td>
</tr>
<tr>
<td>T0725</td>
<td>Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.</td>
</tr>
<tr>
<td>T0726</td>
<td>Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.</td>
</tr>
<tr>
<td>T0727</td>
<td>Identify, locate, and track targets via geospatial analysis techniques.</td>
</tr>
<tr>
<td>T0728</td>
<td>Provide input to or develop courses of action based on threat factors.</td>
</tr>
<tr>
<td>T0729</td>
<td>Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.</td>
</tr>
<tr>
<td>T0730</td>
<td>Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.</td>
</tr>
<tr>
<td>T0731</td>
<td>Initiate requests to guide tasking and assist with collection management.</td>
</tr>
<tr>
<td>T0732</td>
<td>Integrate cyber planning/targeting efforts with other organizations.</td>
</tr>
<tr>
<td>T0733</td>
<td>Interpret environment preparations assessments to determine a course of action.</td>
</tr>
<tr>
<td>T0734</td>
<td>Issue requests for information.</td>
</tr>
<tr>
<td>T0735</td>
<td>Lead and coordinate intelligence support to operational planning.</td>
</tr>
<tr>
<td>T0736</td>
<td>Lead or enable exploitation operations in support of organization objectives and target requirements.</td>
</tr>
<tr>
<td>T0737</td>
<td>Link priority collection requirements to optimal assets and resources.</td>
</tr>
<tr>
<td>T0738</td>
<td>Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.</td>
</tr>
<tr>
<td>T0739</td>
<td>Maintain relationships with internal and external partners involved in cyber planning or related areas.</td>
</tr>
<tr>
<td>T0740</td>
<td>Maintain situational awareness and functionality of organic operational infrastructure.</td>
</tr>
<tr>
<td>T0741</td>
<td>Maintain situational awareness of cyber-related intelligence requirements and associated tasking.</td>
</tr>
<tr>
<td>T0742</td>
<td>Maintain situational awareness of partner capabilities and activities.</td>
</tr>
<tr>
<td>T0743</td>
<td>Maintain situational awareness to determine if changes to the operating environment require review of the plan.</td>
</tr>
<tr>
<td>T0744</td>
<td>Maintain target lists (i.e., RTL, JTL, CTL, etc.).</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0745</td>
<td>Make recommendations to guide collection in support of customer requirements.</td>
</tr>
<tr>
<td>T0746</td>
<td>Modify collection requirements as necessary.</td>
</tr>
<tr>
<td>T0747</td>
<td>Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.</td>
</tr>
<tr>
<td>T0748</td>
<td>Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.</td>
</tr>
<tr>
<td>T0749</td>
<td>Monitor and report on validated threat activities.</td>
</tr>
<tr>
<td>T0750</td>
<td>Monitor completion of reallocated collection efforts.</td>
</tr>
<tr>
<td>T0751</td>
<td>Monitor open source websites for hostile content directed towards organizational or partner interests.</td>
</tr>
<tr>
<td>T0752</td>
<td>Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements.</td>
</tr>
<tr>
<td>T0753</td>
<td>Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.</td>
</tr>
<tr>
<td>T0754</td>
<td>Monitor target networks to provide indications and warning of target communications changes or processing failures.</td>
</tr>
<tr>
<td>T0755</td>
<td>Monitor the operational environment for potential factors and risks to the collection operation management process.</td>
</tr>
<tr>
<td>T0756</td>
<td>Operate and maintain automated systems for gaining and maintaining access to target systems.</td>
</tr>
<tr>
<td>T0757</td>
<td>Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.</td>
</tr>
<tr>
<td>T0758</td>
<td>Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).</td>
</tr>
<tr>
<td>T0759</td>
<td>Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.</td>
</tr>
<tr>
<td>T0760</td>
<td>Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.</td>
</tr>
<tr>
<td>T0761</td>
<td>Provide SME and support to planning/developmental forums and working groups as appropriate.</td>
</tr>
<tr>
<td>T0762</td>
<td>Provide subject matter expertise in course of action development.</td>
</tr>
<tr>
<td>T0763</td>
<td>Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.</td>
</tr>
<tr>
<td>T0764</td>
<td>Provide subject matter expertise to planning efforts with internal and external cyber operations partners.</td>
</tr>
<tr>
<td>T0765</td>
<td>Provide subject matter expertise to development of exercises.</td>
</tr>
<tr>
<td>T0766</td>
<td>Propose policy which governs interactions with external coordination groups.</td>
</tr>
<tr>
<td>T0767</td>
<td>Perform content and/or metadata analysis to meet organization objectives.</td>
</tr>
<tr>
<td>T0768</td>
<td>Conduct cyber activities to degrade/remove information resident in computers and computer networks.</td>
</tr>
<tr>
<td>T0769</td>
<td>Perform targeting automation activities.</td>
</tr>
<tr>
<td>T0770</td>
<td>Develop website characterizations.</td>
</tr>
<tr>
<td>T0771</td>
<td>Provide subject matter expertise to website characterizations.</td>
</tr>
<tr>
<td>T0772</td>
<td>Prepare for and provide subject matter expertise to exercises.</td>
</tr>
<tr>
<td>T0773</td>
<td>Prioritize collection requirements for collection platforms based on platform capabilities.</td>
</tr>
<tr>
<td>T0774</td>
<td>Process exfiltrated data for analysis and/or dissemination to customers.</td>
</tr>
<tr>
<td>T0775</td>
<td>Produce network reconstructions.</td>
</tr>
<tr>
<td>T0776</td>
<td>Produce target system analysis products.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0777</td>
<td>Profile network or system administrators and their activities.</td>
</tr>
<tr>
<td>T0778</td>
<td>Profile targets and their activities.</td>
</tr>
<tr>
<td>T0779</td>
<td>Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.</td>
</tr>
<tr>
<td>T0780</td>
<td>Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.</td>
</tr>
<tr>
<td>T0781</td>
<td>Provide aim point and re-engagement recommendations.</td>
</tr>
<tr>
<td>T0782</td>
<td>Provide analyses and support for effectiveness assessment.</td>
</tr>
<tr>
<td>T0783</td>
<td>Provide current intelligence support to critical internal/external stakeholders as appropriate.</td>
</tr>
<tr>
<td>T0784</td>
<td>Provide cyber focused guidance and advice on intelligence support plan inputs.</td>
</tr>
<tr>
<td>T0785</td>
<td>Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.</td>
</tr>
<tr>
<td>T0786</td>
<td>Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.</td>
</tr>
<tr>
<td>T0787</td>
<td>Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.</td>
</tr>
<tr>
<td>T0788</td>
<td>Provide input and assist in post-action effectiveness assessments.</td>
</tr>
<tr>
<td>T0789</td>
<td>Provide input and assist in the development of plans and guidance.</td>
</tr>
<tr>
<td>T0790</td>
<td>Provide input for targeting effectiveness assessments for leadership acceptance.</td>
</tr>
<tr>
<td>T0791</td>
<td>Provide input to the administrative and logistical elements of an operational support plan.</td>
</tr>
<tr>
<td>T0792</td>
<td>Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.</td>
</tr>
<tr>
<td>T0793</td>
<td>Provide effectiveness support to designated exercises, and/or time sensitive operations.</td>
</tr>
<tr>
<td>T0794</td>
<td>Provide operations and re-engagement recommendations.</td>
</tr>
<tr>
<td>T0795</td>
<td>Provide planning support between internal and external partners.</td>
</tr>
<tr>
<td>T0796</td>
<td>Provide real-time actionable geolocation information.</td>
</tr>
<tr>
<td>T0797</td>
<td>Provide target recommendations which meet leadership objectives.</td>
</tr>
<tr>
<td>T0798</td>
<td>Provide targeting products and targeting support as designated.</td>
</tr>
<tr>
<td>T0799</td>
<td>Provide time sensitive targeting support.</td>
</tr>
<tr>
<td>T0800</td>
<td>Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.</td>
</tr>
<tr>
<td>T0801</td>
<td>Recommend refinement, adaption, termination, and execution of operational plans as appropriate.</td>
</tr>
<tr>
<td>T0802</td>
<td>Review appropriate information sources to determine validity and relevance of information gathered.</td>
</tr>
<tr>
<td>T0803</td>
<td>Reconstruct networks in diagram or report format.</td>
</tr>
<tr>
<td>T0804</td>
<td>Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.</td>
</tr>
<tr>
<td>T0805</td>
<td>Report intelligence-derived significant network events and intrusions.</td>
</tr>
<tr>
<td>T0806</td>
<td>Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.</td>
</tr>
<tr>
<td>T0807</td>
<td>Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.</td>
</tr>
<tr>
<td>T0808</td>
<td>Review and comprehend organizational leadership objectives and guidance for planning.</td>
</tr>
<tr>
<td>T0809</td>
<td>Review capabilities of allocated collection assets.</td>
</tr>
<tr>
<td>T0810</td>
<td>Review intelligence collection guidance for accuracy/applicability.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0811</td>
<td>Review list of prioritized collection requirements and essential information.</td>
</tr>
<tr>
<td>T0812</td>
<td>Review and update overarching collection plan, as required.</td>
</tr>
<tr>
<td>T0813</td>
<td>Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.</td>
</tr>
<tr>
<td>T0814</td>
<td>Revise collection matrix based on availability of optimal assets and resources.</td>
</tr>
<tr>
<td>T0815</td>
<td>Sanitize and minimize information to protect sources and methods.</td>
</tr>
<tr>
<td>T0816</td>
<td>Scope the cyber intelligence planning effort.</td>
</tr>
<tr>
<td>T0817</td>
<td>Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.</td>
</tr>
<tr>
<td>T0818</td>
<td>Serve as a liaison with external partners.</td>
</tr>
<tr>
<td>T0819</td>
<td>Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.</td>
</tr>
<tr>
<td>T0820</td>
<td>Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.</td>
</tr>
<tr>
<td>T0821</td>
<td>Specify discipline-specific collections and/or taskings that must be executed in the near term.</td>
</tr>
<tr>
<td>T0822</td>
<td>Submit information requests to collection requirement management section for processing as collection requests.</td>
</tr>
<tr>
<td>T0823</td>
<td>Submit or respond to requests for deconfliction of cyber operations.</td>
</tr>
<tr>
<td>T0824</td>
<td>Support identification and documentation of collateral effects.</td>
</tr>
<tr>
<td>T0825</td>
<td>Synchronize cyber international engagement activities and associated resource requirements as appropriate.</td>
</tr>
<tr>
<td>T0826</td>
<td>Synchronize cyber portions of security cooperation plans.</td>
</tr>
<tr>
<td>T0827</td>
<td>Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.</td>
</tr>
<tr>
<td>T0828</td>
<td>Test and evaluate locally developed tools for operational use.</td>
</tr>
<tr>
<td>T0829</td>
<td>Test internal developed tools and techniques against target tools.</td>
</tr>
<tr>
<td>T0830</td>
<td>Track status of information requests, including those processed as collection requests and production requirements, using established procedures.</td>
</tr>
<tr>
<td>T0831</td>
<td>Translate collection requests into applicable discipline-specific collection requirements.</td>
</tr>
<tr>
<td>T0832</td>
<td>Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.</td>
</tr>
<tr>
<td>T0833</td>
<td>Validate requests for information according to established criteria.</td>
</tr>
<tr>
<td>T0834</td>
<td>Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.</td>
</tr>
<tr>
<td>T0835</td>
<td>Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.</td>
</tr>
<tr>
<td>T0836</td>
<td>Document lessons learned that convey the results of events and/or exercises.</td>
</tr>
<tr>
<td>T0837</td>
<td>Advise managers and operators on language and cultural issues that impact organization objectives.</td>
</tr>
<tr>
<td>T0838</td>
<td>Analyze and process information using language and/or cultural expertise.</td>
</tr>
<tr>
<td>T0839</td>
<td>Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.</td>
</tr>
<tr>
<td>T0840</td>
<td>Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.</td>
</tr>
<tr>
<td>T0841</td>
<td>Conduct all-source target research to include the use of open source materials in the target language.</td>
</tr>
<tr>
<td>T0842</td>
<td>Conduct analysis of target communications to identify essential information in support of organization objectives.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0843</td>
<td>Perform quality review and provide feedback on transcribed or translated materials.</td>
</tr>
<tr>
<td>T0844</td>
<td>Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.</td>
</tr>
<tr>
<td>T0845</td>
<td>Identify cyber threat tactics and methodologies.</td>
</tr>
<tr>
<td>T0846</td>
<td>Identify target communications within the global network.</td>
</tr>
<tr>
<td>T0847</td>
<td>Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.</td>
</tr>
<tr>
<td>T0848</td>
<td>Provide feedback to collection managers to enhance future collection and analysis.</td>
</tr>
<tr>
<td>T0849</td>
<td>Perform foreign language and dialect identification in initial source data.</td>
</tr>
<tr>
<td>T0850</td>
<td>Perform or support technical network analysis and mapping.</td>
</tr>
<tr>
<td>T0851</td>
<td>Provide requirements and feedback to optimize the development of language processing tools.</td>
</tr>
<tr>
<td>T0852</td>
<td>Perform social network analysis and document as appropriate.</td>
</tr>
<tr>
<td>T0853</td>
<td>Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.</td>
</tr>
<tr>
<td>T0854</td>
<td>Tip critical or time-sensitive information to appropriate customers.</td>
</tr>
<tr>
<td>T0855</td>
<td>Transcribe target voice materials in the target language.</td>
</tr>
<tr>
<td>T0856</td>
<td>Translate (e.g., verbatim, gists, and/or summaries) target graphic material.</td>
</tr>
<tr>
<td>T0857</td>
<td>Translate (e.g., verbatim, gists, and/or summaries) target voice material.</td>
</tr>
<tr>
<td>T0858</td>
<td>Identify foreign language terminology within computer programs (e.g., comments, variable names).</td>
</tr>
<tr>
<td>T0859</td>
<td>Provide near-real time language analysis support (e.g., live operations).</td>
</tr>
<tr>
<td>T0860</td>
<td>Identify cyber/technology-related terminology in the target language.</td>
</tr>
<tr>
<td>T0861</td>
<td>Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.</td>
</tr>
<tr>
<td>T0862</td>
<td>Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.</td>
</tr>
<tr>
<td>T0863</td>
<td>Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.</td>
</tr>
<tr>
<td>T0864</td>
<td>Liaise with regulatory and accrediting bodies.</td>
</tr>
<tr>
<td>T0865</td>
<td>Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.</td>
</tr>
<tr>
<td>T0866</td>
<td>Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.</td>
</tr>
<tr>
<td>T0867</td>
<td>Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.</td>
</tr>
<tr>
<td>T0868</td>
<td>Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.</td>
</tr>
<tr>
<td>T0869</td>
<td>Work with organization senior management to establish an organization-wide Privacy Oversight Committee</td>
</tr>
<tr>
<td>T0870</td>
<td>Serve in a leadership role for Privacy Oversight Committee activities</td>
</tr>
<tr>
<td>T0871</td>
<td>Collaborate on cyber privacy and security policies and procedures</td>
</tr>
<tr>
<td>T0872</td>
<td>Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0873</td>
<td>Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations.</td>
</tr>
<tr>
<td>T0874</td>
<td>Provide strategic guidance to corporate officers regarding information resources and technology.</td>
</tr>
<tr>
<td>T0875</td>
<td>Assist the Security Officer with the development and implementation of an information infrastructure.</td>
</tr>
<tr>
<td>T0876</td>
<td>Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.</td>
</tr>
<tr>
<td>T0877</td>
<td>Work cooperatively with applicable organization units in overseeing consumer information access rights.</td>
</tr>
<tr>
<td>T0878</td>
<td>Serve as the information privacy liaison for users of technology systems.</td>
</tr>
<tr>
<td>T0879</td>
<td>Act as a liaison to the information systems department.</td>
</tr>
<tr>
<td>T0880</td>
<td>Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.</td>
</tr>
<tr>
<td>T0881</td>
<td>Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties.</td>
</tr>
<tr>
<td>T0882</td>
<td>Conduct ongoing privacy training and awareness activities.</td>
</tr>
<tr>
<td>T0883</td>
<td>Work with internal affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security.</td>
</tr>
<tr>
<td>T0884</td>
<td>Work with organization administration, legal counsel and other related parties to represent the organization’s information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.</td>
</tr>
<tr>
<td>T0885</td>
<td>Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee.</td>
</tr>
<tr>
<td>T0886</td>
<td>Work with External Affairs to respond to press and other inquiries with regard to concern over consumer and employee data.</td>
</tr>
<tr>
<td>T0887</td>
<td>Provide leadership for the organization’s privacy program.</td>
</tr>
<tr>
<td>T0888</td>
<td>Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization.</td>
</tr>
<tr>
<td>T0889</td>
<td>Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable.</td>
</tr>
<tr>
<td>T0890</td>
<td>Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures.</td>
</tr>
<tr>
<td>T0891</td>
<td>Resolve allegations of non-compliance with the corporate privacy policies or notice of information practices.</td>
</tr>
<tr>
<td>T0892</td>
<td>Develop and coordinate a risk management and compliance framework for privacy.</td>
</tr>
<tr>
<td>T0893</td>
<td>Undertake a comprehensive review of the company’s data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.</td>
</tr>
<tr>
<td>T0894</td>
<td>Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations.</td>
</tr>
<tr>
<td>T0895</td>
<td>Establish a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization’s privacy policies and procedures.</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>T0896</td>
<td>Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity</td>
</tr>
<tr>
<td>T0897</td>
<td>Provide leadership in the planning, design and evaluation of privacy and security related projects</td>
</tr>
<tr>
<td>T0898</td>
<td>Establish an internal privacy audit program</td>
</tr>
<tr>
<td>T0899</td>
<td>Periodically revise the privacy program in light of changes in laws, regulatory or company policy</td>
</tr>
<tr>
<td>T0900</td>
<td>Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel</td>
</tr>
<tr>
<td>T0901</td>
<td>Assure that the use of technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information</td>
</tr>
<tr>
<td>T0902</td>
<td>Monitor systems development and operations for security and privacy compliance</td>
</tr>
<tr>
<td>T0903</td>
<td>Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected</td>
</tr>
<tr>
<td>T0904</td>
<td>Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization’s other compliance and operational assessment functions</td>
</tr>
<tr>
<td>T0905</td>
<td>Review all system-related information security plans to ensure alignment between security and privacy practices</td>
</tr>
<tr>
<td>T0906</td>
<td>Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization’s policies, procedures and legal requirements</td>
</tr>
<tr>
<td>T0907</td>
<td>Account for and administer individual requests for release or disclosure of personal and/or protected information</td>
</tr>
<tr>
<td>T0908</td>
<td>Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements</td>
</tr>
<tr>
<td>T0909</td>
<td>Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed</td>
</tr>
<tr>
<td>T0910</td>
<td>Act as, or work with, counsel relating to business partner contracts</td>
</tr>
<tr>
<td>T0911</td>
<td>Mitigate effects of a use or disclosure of personal information by employees or business partners</td>
</tr>
<tr>
<td>T0912</td>
<td>Develop and apply corrective action procedures</td>
</tr>
<tr>
<td>T0913</td>
<td>Administer action on all complaints concerning the organization’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel</td>
</tr>
<tr>
<td>T0914</td>
<td>Support the organization’s privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations</td>
</tr>
<tr>
<td>T0915</td>
<td>Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations</td>
</tr>
<tr>
<td>T0916</td>
<td>Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units</td>
</tr>
<tr>
<td>T0917</td>
<td>Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices</td>
</tr>
<tr>
<td>T0918</td>
<td>Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations</td>
</tr>
<tr>
<td>Task</td>
<td>Task Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>T0919</td>
<td>Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials</td>
</tr>
<tr>
<td>T0920</td>
<td>Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of non-compliance</td>
</tr>
<tr>
<td>T0921</td>
<td>Determine business partner requirements related to the organization’s privacy program</td>
</tr>
<tr>
<td>T0922</td>
<td>Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company’s privacy policies and procedures</td>
</tr>
<tr>
<td>T0923</td>
<td>Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations</td>
</tr>
<tr>
<td>T0924</td>
<td>Perform ongoing privacy compliance monitoring activities</td>
</tr>
<tr>
<td>T0925</td>
<td>Monitor advancements in information privacy technologies to ensure organization adoption and compliance</td>
</tr>
<tr>
<td>T0926</td>
<td>Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations</td>
</tr>
<tr>
<td>T0927</td>
<td>Appoint and guide a team of IT security experts</td>
</tr>
<tr>
<td>T0928</td>
<td>Collaborate with key stakeholders to establish a cybersecurity risk management program</td>
</tr>
</tbody>
</table>
## A.5 NCWF Knowledge Descriptions

Table 6 provides a listing of specific knowledge that might be demonstrated by a person in a given cybersecurity position. Selected knowledge descriptions from this list are included in the Detailed Work Role Listing in Appendix B. Because the knowledge aspects have evolved over many years and are expected to continue to do so, they are not sorted in a particular order and will simply continue to grow sequentially.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0001</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>K0002</td>
<td>Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
</tr>
<tr>
<td>K0003</td>
<td>Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.</td>
</tr>
<tr>
<td>K0004</td>
<td>Knowledge of cybersecurity principles.</td>
</tr>
<tr>
<td>K0005</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0006</td>
<td>Knowledge of specific operational impacts of cybersecurity lapses.</td>
</tr>
<tr>
<td>K0007</td>
<td>Knowledge of authentication, authorization, and access control methods.</td>
</tr>
<tr>
<td>K0008</td>
<td>Knowledge of applicable business processes and operations of customer organizations.</td>
</tr>
<tr>
<td>K0009</td>
<td>Knowledge of application vulnerabilities.</td>
</tr>
<tr>
<td>K0010</td>
<td>Knowledge of communication methods, principles, and concepts (e.g., crypto, dual hubs, time multiplexers) that support the network infrastructure.</td>
</tr>
<tr>
<td>K0011</td>
<td>Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.</td>
</tr>
<tr>
<td>K0012</td>
<td>Knowledge of capabilities and requirements analysis.</td>
</tr>
<tr>
<td>K0013</td>
<td>Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.</td>
</tr>
<tr>
<td>K0014</td>
<td>Knowledge of complex data structures.</td>
</tr>
<tr>
<td>K0015</td>
<td>Knowledge of computer algorithms.</td>
</tr>
<tr>
<td>K0016</td>
<td>Knowledge of computer programming principles such as object-oriented design.</td>
</tr>
<tr>
<td>K0017</td>
<td>Knowledge of concepts and practices of processing digital forensic data.</td>
</tr>
<tr>
<td>K0018</td>
<td>Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).</td>
</tr>
<tr>
<td>K0019</td>
<td>Knowledge of cryptography and cryptographic key management concepts.</td>
</tr>
<tr>
<td>K0020</td>
<td>Knowledge of data administration and data standardization policies and standards.</td>
</tr>
<tr>
<td>K0021</td>
<td>Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.</td>
</tr>
<tr>
<td>K0022</td>
<td>Knowledge of data mining and data warehousing principles.</td>
</tr>
<tr>
<td>K0023</td>
<td>Knowledge of database management systems, query languages, table relationships, and views.</td>
</tr>
<tr>
<td>K0024</td>
<td>Knowledge of database systems.</td>
</tr>
<tr>
<td>K0025</td>
<td>Knowledge of digital rights management.</td>
</tr>
<tr>
<td>K0026</td>
<td>Knowledge of disaster recovery continuity of operations plans.</td>
</tr>
<tr>
<td>K0027</td>
<td>Knowledge of organization's enterprise information security architecture system.</td>
</tr>
<tr>
<td>K0028</td>
<td>Knowledge of organization's evaluation and validation requirements.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0029</td>
<td>Knowledge of organization's LAN/WAN pathways.</td>
</tr>
<tr>
<td>K0030</td>
<td>Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.</td>
</tr>
<tr>
<td>K0031</td>
<td>Knowledge of enterprise messaging systems and associated software.</td>
</tr>
<tr>
<td>K0032</td>
<td>Knowledge of fault tolerance.</td>
</tr>
<tr>
<td>K0033</td>
<td>Knowledge of host/network access control mechanisms (e.g., access control list).</td>
</tr>
<tr>
<td>K0034</td>
<td>Knowledge of how network services and protocols interact to provide network communications.</td>
</tr>
<tr>
<td>K0035</td>
<td>Knowledge of how system components are installed, integrated, and optimized.</td>
</tr>
<tr>
<td>K0036</td>
<td>Knowledge of human-computer interaction principles.</td>
</tr>
<tr>
<td>K0037</td>
<td>Knowledge of the Security Assessment and Authorization process.</td>
</tr>
<tr>
<td>K0038</td>
<td>Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.</td>
</tr>
<tr>
<td>K0039</td>
<td>Knowledge of cybersecurity principles and methods that apply to software development.</td>
</tr>
<tr>
<td>K0040</td>
<td>Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.</td>
</tr>
<tr>
<td>K0041</td>
<td>Knowledge of incident categories, incident responses, and timelines for responses.</td>
</tr>
<tr>
<td>K0042</td>
<td>Knowledge of incident response and handling methodologies.</td>
</tr>
<tr>
<td>K0043</td>
<td>Knowledge of industry-standard and organizationally accepted analysis principles and methods.</td>
</tr>
<tr>
<td>K0044</td>
<td>Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
<tr>
<td>K0045</td>
<td>Knowledge of information security systems engineering principles.</td>
</tr>
<tr>
<td>K0046</td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.</td>
</tr>
<tr>
<td>K0047</td>
<td>Knowledge of information technology (IT) architectural concepts and frameworks.</td>
</tr>
<tr>
<td>K0048</td>
<td>Knowledge of Risk Management Framework (RMF) requirements.</td>
</tr>
<tr>
<td>K0049</td>
<td>Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).</td>
</tr>
<tr>
<td>K0050</td>
<td>Knowledge of local area and wide area networking principles and concepts including bandwidth management.</td>
</tr>
<tr>
<td>K0051</td>
<td>Knowledge of low-level computer languages (e.g., assembly languages).</td>
</tr>
<tr>
<td>K0052</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.</td>
</tr>
<tr>
<td>K0053</td>
<td>Knowledge of measures or indicators of system performance and availability.</td>
</tr>
<tr>
<td>K0054</td>
<td>Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.</td>
</tr>
<tr>
<td>K0055</td>
<td>Knowledge of microprocessors.</td>
</tr>
<tr>
<td>K0056</td>
<td>Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).</td>
</tr>
<tr>
<td>K0057</td>
<td>Knowledge of network hardware devices and functions.</td>
</tr>
<tr>
<td>K0058</td>
<td>Knowledge of network traffic analysis methods.</td>
</tr>
<tr>
<td>K0059</td>
<td>Knowledge of new and emerging information technology (IT) and cybersecurity technologies.</td>
</tr>
<tr>
<td>K0060</td>
<td>Knowledge of operating systems.</td>
</tr>
<tr>
<td>K0061</td>
<td>Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0062</td>
<td>Knowledge of packet-level analysis.</td>
</tr>
<tr>
<td>K0063</td>
<td>Knowledge of parallel and distributed computing concepts.</td>
</tr>
<tr>
<td>K0064</td>
<td>Knowledge of performance tuning tools and techniques.</td>
</tr>
<tr>
<td>K0065</td>
<td>Knowledge of policy-based and risk adaptive access controls.</td>
</tr>
<tr>
<td>K0066</td>
<td>Knowledge of Privacy Impact Assessments.</td>
</tr>
<tr>
<td>K0067</td>
<td>Knowledge of process engineering concepts.</td>
</tr>
<tr>
<td>K0068</td>
<td>Knowledge of programming language structures and logic.</td>
</tr>
<tr>
<td>K0069</td>
<td>Knowledge of query languages such as SQL (structured query language).</td>
</tr>
<tr>
<td>K0070</td>
<td>Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).</td>
</tr>
<tr>
<td>K0071</td>
<td>Knowledge of remote access technology concepts.</td>
</tr>
<tr>
<td>K0072</td>
<td>Knowledge of resource management principles and techniques.</td>
</tr>
<tr>
<td>K0073</td>
<td>Knowledge of secure configuration management techniques.</td>
</tr>
<tr>
<td>K0074</td>
<td>Knowledge of key concepts in security management (e.g., Release Management, Patch Management).</td>
</tr>
<tr>
<td>K0075</td>
<td>Knowledge of security system design tools, methods, and techniques.</td>
</tr>
<tr>
<td>K0076</td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods.</td>
</tr>
<tr>
<td>K0077</td>
<td>Knowledge of server and client operating systems.</td>
</tr>
<tr>
<td>K0078</td>
<td>Knowledge of server diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0079</td>
<td>Knowledge of software debugging principles.</td>
</tr>
<tr>
<td>K0080</td>
<td>Knowledge of software design tools, methods, and techniques.</td>
</tr>
<tr>
<td>K0081</td>
<td>Knowledge of software development models (e.g., Waterfall Model, Spiral Model).</td>
</tr>
<tr>
<td>K0082</td>
<td>Knowledge of software engineering.</td>
</tr>
<tr>
<td>K0083</td>
<td>Knowledge of sources, characteristics, and uses of the organization’s data assets.</td>
</tr>
<tr>
<td>K0084</td>
<td>Knowledge of structured analysis principles and methods.</td>
</tr>
<tr>
<td>K0085</td>
<td>Knowledge of system and application security threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0086</td>
<td>Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.</td>
</tr>
<tr>
<td>K0087</td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.</td>
</tr>
<tr>
<td>K0088</td>
<td>Knowledge of systems administration concepts.</td>
</tr>
<tr>
<td>K0089</td>
<td>Knowledge of systems diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0090</td>
<td>Knowledge of system life cycle management principles, including software security and usability.</td>
</tr>
<tr>
<td>K0091</td>
<td>Knowledge of systems testing and evaluation methods.</td>
</tr>
<tr>
<td>K0092</td>
<td>Knowledge of technology integration processes.</td>
</tr>
<tr>
<td>K0093</td>
<td>Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).</td>
</tr>
<tr>
<td>K0094</td>
<td>Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs).</td>
</tr>
<tr>
<td>K0095</td>
<td>Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines).</td>
</tr>
<tr>
<td>K0096</td>
<td>Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0097</td>
<td>Knowledge of the characteristics of physical and virtual data storage media.</td>
</tr>
<tr>
<td>K0098</td>
<td>Knowledge of the cyber defense Service Provider reporting structure and processes within one’s own organization.</td>
</tr>
<tr>
<td>K0099</td>
<td>Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications.</td>
</tr>
<tr>
<td>K0100</td>
<td>Knowledge of the enterprise information technology (IT) architecture.</td>
</tr>
<tr>
<td>K0101</td>
<td>Knowledge of the organization’s enterprise information technology (IT) goals and objectives.</td>
</tr>
<tr>
<td>K0102</td>
<td>Knowledge of the systems engineering process.</td>
</tr>
<tr>
<td>K0103</td>
<td>Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly.</td>
</tr>
<tr>
<td>K0104</td>
<td>Knowledge of Virtual Private Network (VPN) security.</td>
</tr>
<tr>
<td>K0105</td>
<td>Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.</td>
</tr>
<tr>
<td>K0106</td>
<td>Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0107</td>
<td>Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations.</td>
</tr>
<tr>
<td>K0108</td>
<td>Knowledge of basic concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).</td>
</tr>
<tr>
<td>K0109</td>
<td>Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).</td>
</tr>
<tr>
<td>K0110</td>
<td>Knowledge of common adversary tactics, techniques, and procedures in assigned area of responsibility (i.e., historical country-specific tactics, techniques, and procedures; emerging capabilities).</td>
</tr>
<tr>
<td>K0111</td>
<td>Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results.</td>
</tr>
<tr>
<td>K0112</td>
<td>Knowledge of defense-in-depth principles and network security architecture.</td>
</tr>
<tr>
<td>K0113</td>
<td>Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).</td>
</tr>
<tr>
<td>K0114</td>
<td>Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]).</td>
</tr>
<tr>
<td>K0115</td>
<td>Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.</td>
</tr>
<tr>
<td>K0116</td>
<td>Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).</td>
</tr>
<tr>
<td>K0117</td>
<td>Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).</td>
</tr>
<tr>
<td>K0118</td>
<td>Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).</td>
</tr>
<tr>
<td>K0119</td>
<td>Knowledge of hacking methodologies in Windows or Unix/Linux environment.</td>
</tr>
<tr>
<td>K0120</td>
<td>Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.</td>
</tr>
<tr>
<td>K0121</td>
<td>Knowledge of information security program management and project management principles and techniques.</td>
</tr>
<tr>
<td>K0122</td>
<td>Knowledge of investigative implications of hardware, Operating Systems, and network technologies.</td>
</tr>
<tr>
<td>K0123</td>
<td>Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence).</td>
</tr>
<tr>
<td>K0124</td>
<td>Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0125</td>
<td>Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.</td>
</tr>
<tr>
<td>K0126</td>
<td>Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).</td>
</tr>
<tr>
<td>K0127</td>
<td>Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).</td>
</tr>
<tr>
<td>K0128</td>
<td>Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).</td>
</tr>
<tr>
<td>K0129</td>
<td>Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).</td>
</tr>
<tr>
<td>K0130</td>
<td>Knowledge of virtualization technologies and virtual machine development and maintenance.</td>
</tr>
<tr>
<td>K0131</td>
<td>Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.</td>
</tr>
<tr>
<td>K0132</td>
<td>Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.</td>
</tr>
<tr>
<td>K0133</td>
<td>Knowledge of types of digital forensics data and how to recognize them.</td>
</tr>
<tr>
<td>K0134</td>
<td>Knowledge of deployable forensics.</td>
</tr>
<tr>
<td>K0135</td>
<td>Knowledge of web filtering technologies.</td>
</tr>
<tr>
<td>K0136</td>
<td>Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).</td>
</tr>
<tr>
<td>K0137</td>
<td>Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).</td>
</tr>
<tr>
<td>K0138</td>
<td>Knowledge of Wi-Fi.</td>
</tr>
<tr>
<td>K0139</td>
<td>Knowledge of interpreted and compiled computer languages.</td>
</tr>
<tr>
<td>K0140</td>
<td>Knowledge of secure coding techniques.</td>
</tr>
<tr>
<td>K0141</td>
<td>Withdrawn — Integrated into K0420</td>
</tr>
<tr>
<td>K0142</td>
<td>Knowledge of collection management processes, capabilities, and limitations.</td>
</tr>
<tr>
<td>K0143</td>
<td>Knowledge of front-end collection systems, including network traffic collection, filtering, and selection.</td>
</tr>
<tr>
<td>K0144</td>
<td>Knowledge of social dynamics of computer attackers in a global context.</td>
</tr>
<tr>
<td>K0145</td>
<td>Knowledge of security event correlation tools.</td>
</tr>
<tr>
<td>K0146</td>
<td>Knowledge of the organization's core business/mission processes.</td>
</tr>
<tr>
<td>K0147</td>
<td>Knowledge of emerging security issues, risks, and vulnerabilities.</td>
</tr>
<tr>
<td>K0148</td>
<td>Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.</td>
</tr>
<tr>
<td>K0149</td>
<td>Knowledge of organization's risk tolerance and/or risk management approach.</td>
</tr>
<tr>
<td>K0150</td>
<td>Knowledge of enterprise incident response program, roles, and responsibilities.</td>
</tr>
<tr>
<td>K0151</td>
<td>Knowledge of current and emerging threats/threat vectors.</td>
</tr>
<tr>
<td>K0152</td>
<td>Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).</td>
</tr>
<tr>
<td>K0153</td>
<td>Knowledge of software quality assurance process.</td>
</tr>
<tr>
<td>K0154</td>
<td>Knowledge of supply chain risk management standards, processes, and practices.</td>
</tr>
<tr>
<td>K0155</td>
<td>Knowledge of electronic evidence law.</td>
</tr>
<tr>
<td>K0156</td>
<td>Knowledge of legal rules of evidence and court procedure.</td>
</tr>
<tr>
<td>K0157</td>
<td>Knowledge of cyber defense policies, procedures, and regulations.</td>
</tr>
<tr>
<td>K0158</td>
<td>Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).</td>
</tr>
<tr>
<td>K0159</td>
<td>Knowledge of Voice over IP (VoIP).</td>
</tr>
<tr>
<td>K0160</td>
<td>Knowledge of the common attack vectors on the network layer.</td>
</tr>
<tr>
<td>K0161</td>
<td>Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0162</td>
<td>Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).</td>
</tr>
<tr>
<td>K0163</td>
<td>Knowledge of critical information technology (IT) procurement requirements.</td>
</tr>
<tr>
<td>K0164</td>
<td>Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).</td>
</tr>
<tr>
<td>K0165</td>
<td>Knowledge of risk threat assessment.</td>
</tr>
<tr>
<td>K0166</td>
<td>Knowledge of the nature and function of the relevant information structure.</td>
</tr>
<tr>
<td>K0167</td>
<td>Knowledge of basic system administration, network, and operating system hardening techniques.</td>
</tr>
<tr>
<td>K0168</td>
<td>Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.</td>
</tr>
<tr>
<td>K0169</td>
<td>Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.</td>
</tr>
<tr>
<td>K0170</td>
<td>Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.</td>
</tr>
<tr>
<td>K0171</td>
<td>Knowledge of hardware reverse engineering techniques.</td>
</tr>
<tr>
<td>K0172</td>
<td>Knowledge of middleware (e.g., enterprise service bus and message queuing).</td>
</tr>
<tr>
<td>K0173</td>
<td>Withdrawn – Integrated into K0499</td>
</tr>
<tr>
<td>K0174</td>
<td>Knowledge of networking protocols.</td>
</tr>
<tr>
<td>K0175</td>
<td>Knowledge of software reverse engineering techniques.</td>
</tr>
<tr>
<td>K0176</td>
<td>Knowledge of Extensible Markup Language (XML) schemas.</td>
</tr>
<tr>
<td>K0177</td>
<td>Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).</td>
</tr>
<tr>
<td>K0178</td>
<td>Knowledge of secure software deployment methodologies, tools, and practices.</td>
</tr>
<tr>
<td>K0179</td>
<td>Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</td>
</tr>
<tr>
<td>K0180</td>
<td>Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.</td>
</tr>
<tr>
<td>K0181</td>
<td>Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.</td>
</tr>
<tr>
<td>K0182</td>
<td>Knowledge of data carving tools and techniques (e.g., Foremost).</td>
</tr>
<tr>
<td>K0183</td>
<td>Knowledge of reverse engineering concepts.</td>
</tr>
<tr>
<td>K0184</td>
<td>Knowledge of anti-forensics tactics, techniques, and procedures.</td>
</tr>
<tr>
<td>K0185</td>
<td>Knowledge of common forensics tool configuration and support applications (e.g., VMWare, WIRESHARK).</td>
</tr>
<tr>
<td>K0186</td>
<td>Knowledge of debugging procedures and tools.</td>
</tr>
<tr>
<td>K0187</td>
<td>Knowledge of how different file types can be used for anomalous behavior.</td>
</tr>
<tr>
<td>K0188</td>
<td>Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).</td>
</tr>
<tr>
<td>K0189</td>
<td>Knowledge of virtual machine aware malware, debugger aware malware, and packing.</td>
</tr>
<tr>
<td>K0190</td>
<td>Knowledge of encryption methodologies.</td>
</tr>
<tr>
<td>K0191</td>
<td>Knowledge of signature implementation impact.</td>
</tr>
<tr>
<td>K0192</td>
<td>Knowledge of Windows/Unix ports and services.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0193</td>
<td>Knowledge of advanced data remediation security features in databases.</td>
</tr>
<tr>
<td>K0194</td>
<td>Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.</td>
</tr>
<tr>
<td>K0195</td>
<td>Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.</td>
</tr>
<tr>
<td>K0196</td>
<td>Knowledge of Import/Export Regulations related to cryptography and other security technologies.</td>
</tr>
<tr>
<td>K0197</td>
<td>Knowledge of Java-based database access application programming interface (API) (e.g., Java Database Connectivity [JDBC]).</td>
</tr>
<tr>
<td>K0198</td>
<td>Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).</td>
</tr>
<tr>
<td>K0199</td>
<td>Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).</td>
</tr>
<tr>
<td>K0200</td>
<td>Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).</td>
</tr>
<tr>
<td>K0201</td>
<td>Knowledge of symmetric key rotation techniques and concepts.</td>
</tr>
<tr>
<td>K0202</td>
<td>Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).</td>
</tr>
<tr>
<td>K0203</td>
<td>Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).</td>
</tr>
<tr>
<td>K0204</td>
<td>Knowledge of assessment techniques (rubrics, evaluation plans, tests, quizzes).</td>
</tr>
<tr>
<td>K0205</td>
<td>Knowledge of basic system, network, and OS hardening techniques.</td>
</tr>
<tr>
<td>K0206</td>
<td>Knowledge of ethical hacking principles and techniques.</td>
</tr>
<tr>
<td>K0207</td>
<td>Knowledge of circuit analysis.</td>
</tr>
<tr>
<td>K0208</td>
<td>Knowledge of computer based training and e-learning services.</td>
</tr>
<tr>
<td>K0209</td>
<td>Knowledge of covert communication techniques.</td>
</tr>
<tr>
<td>K0210</td>
<td>Knowledge of data backup and restoration concepts.</td>
</tr>
<tr>
<td>K0211</td>
<td>Knowledge of confidentiality, integrity, and availability requirements.</td>
</tr>
<tr>
<td>K0212</td>
<td>Knowledge of cybersecurity-enabled software products.</td>
</tr>
<tr>
<td>K0213</td>
<td>Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne’s Events of Instruction, Kirkpatrick’s model of evaluation).</td>
</tr>
<tr>
<td>K0214</td>
<td>Knowledge of the Risk Management Framework Assessment Methodology.</td>
</tr>
<tr>
<td>K0215</td>
<td>Knowledge of organizational training policies.</td>
</tr>
<tr>
<td>K0216</td>
<td>Knowledge of learning levels (i.e., Bloom’s Taxonomy of learning).</td>
</tr>
<tr>
<td>K0218</td>
<td>Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).</td>
</tr>
<tr>
<td>K0219</td>
<td>Knowledge of local area network (LAN) and wide area network (WAN) principles.</td>
</tr>
<tr>
<td>K0220</td>
<td>Knowledge of modes of learning (e.g., rote learning, observation).</td>
</tr>
<tr>
<td>K0221</td>
<td>Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).</td>
</tr>
<tr>
<td>K0222</td>
<td>Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.</td>
</tr>
<tr>
<td>K0223</td>
<td>Withdrawn – integrated into K0073</td>
</tr>
<tr>
<td>K0224</td>
<td>Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems.</td>
</tr>
<tr>
<td>K0225</td>
<td>Knowledge of the common networking protocol and services deployed at CC/S/A.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0226</td>
<td>Knowledge of organizational training systems.</td>
</tr>
<tr>
<td>K0227</td>
<td>Knowledge of various types of computer architectures.</td>
</tr>
<tr>
<td>K0228</td>
<td>Knowledge of taxonomy and semantic ontology theory.</td>
</tr>
<tr>
<td>K0229</td>
<td>Knowledge of applications that can log errors, exceptions, and application faults and logging.</td>
</tr>
<tr>
<td>K0230</td>
<td>Knowledge of cloud service models and possible limitations for an incident response.</td>
</tr>
<tr>
<td>K0231</td>
<td>Knowledge of crisis management protocols, processes, and techniques.</td>
</tr>
<tr>
<td>K0232</td>
<td>Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE).</td>
</tr>
<tr>
<td>K0233</td>
<td>Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.</td>
</tr>
<tr>
<td>K0234</td>
<td>Knowledge of full spectrum cyber capabilities.</td>
</tr>
<tr>
<td>K0235</td>
<td>Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.</td>
</tr>
<tr>
<td>K0236</td>
<td>Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and PIG to explore data.</td>
</tr>
<tr>
<td>K0237</td>
<td>Knowledge of industry best practices for service desk.</td>
</tr>
<tr>
<td>K0238</td>
<td>Knowledge of machine learning theory and principles.</td>
</tr>
<tr>
<td>K0239</td>
<td>Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.</td>
</tr>
<tr>
<td>K0240</td>
<td>Knowledge of multi-level/security cross domain solutions.</td>
</tr>
<tr>
<td>K0241</td>
<td>Knowledge of organizational human resource policies, processes, and procedures.</td>
</tr>
<tr>
<td>K0242</td>
<td>Knowledge of organizational security policies.</td>
</tr>
<tr>
<td>K0243</td>
<td>Knowledge of organizational training and education policies, processes, and procedures.</td>
</tr>
<tr>
<td>K0244</td>
<td>Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.</td>
</tr>
<tr>
<td>K0245</td>
<td>Knowledge of principles and processes for conducting training and education needs assessment.</td>
</tr>
<tr>
<td>K0246</td>
<td>Knowledge of relevant concepts, procedures, software, equipment, and technology applications.</td>
</tr>
<tr>
<td>K0247</td>
<td>Knowledge of remote access processes, tools, and capabilities related to customer support.</td>
</tr>
<tr>
<td>K0248</td>
<td>Knowledge of strategic theory and practice.</td>
</tr>
<tr>
<td>K0249</td>
<td>Knowledge of sustainment technologies, processes and strategies.</td>
</tr>
<tr>
<td>K0250</td>
<td>Knowledge of Test &amp; Evaluation processes.</td>
</tr>
<tr>
<td>K0251</td>
<td>Knowledge of the judicial process, including the presentation of facts and evidence.</td>
</tr>
<tr>
<td>K0252</td>
<td>Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.</td>
</tr>
<tr>
<td>K0253</td>
<td>Withdrawn – Integrated into K0227</td>
</tr>
<tr>
<td>K0254</td>
<td>Knowledge of binary analysis.</td>
</tr>
<tr>
<td>K0255</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components.</td>
</tr>
<tr>
<td>K0256</td>
<td>Withdrawn – Integrated into K0224</td>
</tr>
<tr>
<td>K0257</td>
<td>Knowledge of information technology (IT) acquisition/procurement requirements.</td>
</tr>
<tr>
<td>K0258</td>
<td>Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).</td>
</tr>
<tr>
<td>K0259</td>
<td>Knowledge of malware analysis concepts and methodologies.</td>
</tr>
<tr>
<td>K0260</td>
<td>Knowledge of Personally Identifiable Information (PII) data security standards.</td>
</tr>
<tr>
<td>K0261</td>
<td>Knowledge of Payment Card Industry (PCI) data security standards.</td>
</tr>
<tr>
<td>K0262</td>
<td>Knowledge of Personal Health Information (PHI) data security standards.</td>
</tr>
<tr>
<td>K0263</td>
<td>Knowledge of information technology (IT) risk management policies, requirements, and procedures.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0264</td>
<td>Knowledge of program protection planning to include information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements.</td>
</tr>
<tr>
<td>K0265</td>
<td>Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.</td>
</tr>
<tr>
<td>K0266</td>
<td>Knowledge of how to evaluate the trustworthiness of the supplier and/or product.</td>
</tr>
<tr>
<td>K0267</td>
<td>Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.</td>
</tr>
<tr>
<td>K0268</td>
<td>Knowledge of forensic footprint identification.</td>
</tr>
<tr>
<td>K0269</td>
<td>Knowledge of mobile communications architecture.</td>
</tr>
<tr>
<td>K0270</td>
<td>Knowledge of the acquisition/procurement life cycle process.</td>
</tr>
<tr>
<td>K0271</td>
<td>Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).</td>
</tr>
<tr>
<td>K0272</td>
<td>Knowledge of network analysis tools used to identify software communications vulnerabilities.</td>
</tr>
<tr>
<td>K0273</td>
<td>Knowledge of general kill chain (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).</td>
</tr>
<tr>
<td>K0274</td>
<td>Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi), paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.</td>
</tr>
<tr>
<td>K0275</td>
<td>Knowledge of configuration management techniques.</td>
</tr>
<tr>
<td>K0276</td>
<td>Knowledge of security management.</td>
</tr>
<tr>
<td>K0277</td>
<td>Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases, including built-in cryptographic key management features.</td>
</tr>
<tr>
<td>K0278</td>
<td>Knowledge of current and emerging data remediation security features in databases.</td>
</tr>
<tr>
<td>K0279</td>
<td>Knowledge of database access application programming interfaces (APIs) (e.g., Java Database Connectivity [JDBC]).</td>
</tr>
<tr>
<td>K0280</td>
<td>Knowledge of systems engineering theories, concepts, and methods.</td>
</tr>
<tr>
<td>K0281</td>
<td>Knowledge of information technology (IT) service catalogues.</td>
</tr>
<tr>
<td>K0282</td>
<td>Withdrawn – Integrated into K0200</td>
</tr>
<tr>
<td>K0283</td>
<td>Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).</td>
</tr>
<tr>
<td>K0284</td>
<td>Knowledge of developing and applying user credential management system.</td>
</tr>
<tr>
<td>K0285</td>
<td>Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.</td>
</tr>
<tr>
<td>K0286</td>
<td>Knowledge of N-tiered typologies including server and client operating systems.</td>
</tr>
<tr>
<td>K0287</td>
<td>Knowledge of an organization's information classification program and procedures for information compromise.</td>
</tr>
<tr>
<td>K0288</td>
<td>Knowledge of industry standard security models.</td>
</tr>
<tr>
<td>K0289</td>
<td>Knowledge of system/server diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0290</td>
<td>Knowledge of systems security testing and evaluation methods.</td>
</tr>
<tr>
<td>K0291</td>
<td>Knowledge of the enterprise information technology (IT) architectural concepts and patterns to include baseline and target architectures.</td>
</tr>
<tr>
<td>K0292</td>
<td>Knowledge of the operations and processes for incident, problem, and event management.</td>
</tr>
<tr>
<td>K0293</td>
<td>Knowledge of integrating the organization’s goals and objectives into the architecture.</td>
</tr>
<tr>
<td>K0294</td>
<td>Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.</td>
</tr>
</tbody>
</table>

71
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0295</td>
<td>Knowledge of confidentiality, integrity, and availability principles.</td>
</tr>
<tr>
<td>K0296</td>
<td>Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.</td>
</tr>
<tr>
<td>K0297</td>
<td>Knowledge of countermeasure design for identified security risks.</td>
</tr>
<tr>
<td>K0298</td>
<td>Knowledge of countermeasures for identified security risks.</td>
</tr>
<tr>
<td>K0299</td>
<td>Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.</td>
</tr>
<tr>
<td>K0300</td>
<td>Knowledge of network mapping and recreating network topologies.</td>
</tr>
<tr>
<td>K0301</td>
<td>Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).</td>
</tr>
<tr>
<td>K0302</td>
<td>Knowledge of the basic operation of computers.</td>
</tr>
<tr>
<td>K0303</td>
<td>Knowledge of the use of sub-netting tools.</td>
</tr>
<tr>
<td>K0304</td>
<td>Knowledge of basic concepts and practices of processing digital forensic data.</td>
</tr>
<tr>
<td>K0305</td>
<td>Knowledge of encryption algorithms, stenography, and other forms of data concealment.</td>
</tr>
<tr>
<td>K0306</td>
<td>Knowledge of basic physical computer components and architectures.</td>
</tr>
<tr>
<td>K0307</td>
<td>Knowledge of common network tools (e.g., ping, traceroute, nslookup).</td>
</tr>
<tr>
<td>K0308</td>
<td>Knowledge of cryptology.</td>
</tr>
<tr>
<td>K0309</td>
<td>Knowledge of emerging technologies that have potential for exploitation by adversaries.</td>
</tr>
<tr>
<td>K0310</td>
<td>Knowledge of hacking methodologies.</td>
</tr>
<tr>
<td>K0311</td>
<td>Knowledge of industry indicators useful for identifying technology trends.</td>
</tr>
<tr>
<td>K0312</td>
<td>Knowledge of intelligence indicators, policies, and procedures including legal authorities and restrictions.</td>
</tr>
<tr>
<td>K0313</td>
<td>Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research &amp; Development).</td>
</tr>
<tr>
<td>K0314</td>
<td>Knowledge of industry technologies and how differences affect exploitation/vulnerabilities.</td>
</tr>
<tr>
<td>K0315</td>
<td>Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.</td>
</tr>
<tr>
<td>K0316</td>
<td>Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.</td>
</tr>
<tr>
<td>K0317</td>
<td>Knowledge of procedures used for documenting and querying reported incidents, problems, and events.</td>
</tr>
<tr>
<td>K0318</td>
<td>Knowledge of operating system command line/prompt.</td>
</tr>
<tr>
<td>K0319</td>
<td>Knowledge of technical delivery capabilities and their limitations.</td>
</tr>
<tr>
<td>K0320</td>
<td>Knowledge of organization's evaluation and validation criteria.</td>
</tr>
<tr>
<td>K0321</td>
<td>Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.</td>
</tr>
<tr>
<td>K0322</td>
<td>Knowledge of embedded systems.</td>
</tr>
<tr>
<td>K0323</td>
<td>Knowledge of system fault tolerance methodologies.</td>
</tr>
<tr>
<td>K0324</td>
<td>Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.</td>
</tr>
<tr>
<td>K0325</td>
<td>Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).</td>
</tr>
<tr>
<td>K0326</td>
<td>Knowledge of cybersecurity methods, such as firewalls, demilitarized zones, and encryption.</td>
</tr>
<tr>
<td>K0327</td>
<td>Knowledge of local area network (LAN), wide area network (WAN) and enterprise principles and concepts, including bandwidth management.</td>
</tr>
<tr>
<td>K0328</td>
<td>Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis.</td>
</tr>
<tr>
<td>K0329</td>
<td>Knowledge of statistics.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0330</td>
<td>Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.</td>
</tr>
<tr>
<td>K0331</td>
<td>Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).</td>
</tr>
<tr>
<td>K0332</td>
<td>Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.</td>
</tr>
<tr>
<td>K0333</td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.</td>
</tr>
<tr>
<td>K0334</td>
<td>Knowledge of network traffic analysis (tools, methodologies, processes).</td>
</tr>
<tr>
<td>K0335</td>
<td>Knowledge of current and emerging cyber technologies.</td>
</tr>
<tr>
<td>K0336</td>
<td>Knowledge of access authentication methods.</td>
</tr>
<tr>
<td>K0337</td>
<td>Withdrawn – Integrated into K0007</td>
</tr>
<tr>
<td>K0338</td>
<td>Knowledge of data mining techniques.</td>
</tr>
<tr>
<td>K0339</td>
<td>Knowledge of how to use network analysis tools to identify vulnerabilities.</td>
</tr>
<tr>
<td>K0340</td>
<td>Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP), Internet Protocol (IP), Open System Interconnection Model (OSI)).</td>
</tr>
<tr>
<td>K0341</td>
<td>Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.</td>
</tr>
<tr>
<td>K0342</td>
<td>Knowledge of penetration testing principles, tools, and techniques.</td>
</tr>
<tr>
<td>K0343</td>
<td>Knowledge of root cause analysis techniques.</td>
</tr>
<tr>
<td>K0344</td>
<td>Knowledge of threat environments.</td>
</tr>
<tr>
<td>K0345</td>
<td>Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).</td>
</tr>
<tr>
<td>K0346</td>
<td>Knowledge of principles and methods for integrating system components.</td>
</tr>
<tr>
<td>K0347</td>
<td>Knowledge and understanding of operational design</td>
</tr>
<tr>
<td>K0348</td>
<td>Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).</td>
</tr>
<tr>
<td>K0349</td>
<td>Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).</td>
</tr>
<tr>
<td>K0350</td>
<td>Knowledge of accepted organization planning systems.</td>
</tr>
<tr>
<td>K0351</td>
<td>Knowledge of all applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.</td>
</tr>
<tr>
<td>K0352</td>
<td>Knowledge of all forms of intelligence support needs, topics, and focus areas.</td>
</tr>
<tr>
<td>K0353</td>
<td>Knowledge of all possible circumstances that would result in changing collection management authorities.</td>
</tr>
<tr>
<td>K0354</td>
<td>Knowledge of all relevant reporting and dissemination procedures.</td>
</tr>
<tr>
<td>K0355</td>
<td>Knowledge of all-source reporting and dissemination procedures.</td>
</tr>
<tr>
<td>K0356</td>
<td>Knowledge of analytic tools and techniques.</td>
</tr>
<tr>
<td>K0357</td>
<td>Knowledge of analytical constructs and their use in assessing the operational environment.</td>
</tr>
<tr>
<td>K0358</td>
<td>Knowledge of analytical standards and the purpose of intelligence confidence levels.</td>
</tr>
<tr>
<td>K0359</td>
<td>Knowledge of approved intelligence dissemination processes.</td>
</tr>
<tr>
<td>K0360</td>
<td>Knowledge of assembly code.</td>
</tr>
<tr>
<td>K0361</td>
<td>Knowledge of asset availability, capabilities and limitations.</td>
</tr>
<tr>
<td>K0362</td>
<td>Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).</td>
</tr>
<tr>
<td>K0363</td>
<td>Knowledge of auditing and logging procedures (including server-based logging).</td>
</tr>
<tr>
<td>K0364</td>
<td>Knowledge of available databases and tools necessary to assess appropriate collection tasking.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0365</td>
<td>Knowledge of basic back-up and recovery procedures including different types of backups (e.g., full, incremental).</td>
</tr>
<tr>
<td>K0366</td>
<td>Knowledge of basic computer components and architectures, including the functions of various peripherals.</td>
</tr>
<tr>
<td>K0367</td>
<td>Knowledge of basic cyber operations activity concepts (e.g., footprinting, scanning and enumeration, penetration testing, white/black listing).</td>
</tr>
<tr>
<td>K0368</td>
<td>Knowledge of basic implants.</td>
</tr>
<tr>
<td>K0369</td>
<td>Knowledge of basic malicious activity concepts (e.g., footprinting, scanning and enumeration).</td>
</tr>
<tr>
<td>K0370</td>
<td>Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).</td>
</tr>
<tr>
<td>K0371</td>
<td>Knowledge of basic principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis).</td>
</tr>
<tr>
<td>K0372</td>
<td>Knowledge of basic programming concepts (e.g., levels, structures, compiled vs. interpreted languages).</td>
</tr>
<tr>
<td>K0373</td>
<td>Knowledge of basic software applications (e.g., data storage and backup, database applications) and their vulnerabilities.</td>
</tr>
<tr>
<td>K0374</td>
<td>Knowledge of basic structure, architecture, and design of modern digital and telephony networks.</td>
</tr>
<tr>
<td>K0375</td>
<td>Knowledge of basic wireless applications, including vulnerabilities in various types of wireless applications.</td>
</tr>
<tr>
<td>K0376</td>
<td>Knowledge of both internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.</td>
</tr>
<tr>
<td>K0377</td>
<td>Knowledge of classification and control markings standards, policies and procedures.</td>
</tr>
<tr>
<td>K0378</td>
<td>Knowledge of classification and control markings standards.</td>
</tr>
<tr>
<td>K0379</td>
<td>Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.</td>
</tr>
<tr>
<td>K0380</td>
<td>Knowledge of collaborative tools and environments.</td>
</tr>
<tr>
<td>K0381</td>
<td>Knowledge of collateral damage and estimating impact(s).</td>
</tr>
<tr>
<td>K0382</td>
<td>Knowledge of collection capabilities and limitations.</td>
</tr>
<tr>
<td>K0383</td>
<td>Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.</td>
</tr>
<tr>
<td>K0384</td>
<td>Knowledge of collection management functionality (e.g., positions, functions, responsibilities, products, reporting requirements).</td>
</tr>
<tr>
<td>K0385</td>
<td>Withdrawn – Integrated into K0142</td>
</tr>
<tr>
<td>K0386</td>
<td>Knowledge of collection management tools.</td>
</tr>
<tr>
<td>K0387</td>
<td>Knowledge of collection planning process and collection plan.</td>
</tr>
<tr>
<td>K0388</td>
<td>Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.</td>
</tr>
<tr>
<td>K0389</td>
<td>Knowledge of collection sources including conventional and non-conventional sources.</td>
</tr>
<tr>
<td>K0390</td>
<td>Knowledge of collection strategies.</td>
</tr>
<tr>
<td>K0391</td>
<td>Knowledge of collection systems, capabilities, and processes.</td>
</tr>
<tr>
<td>K0392</td>
<td>Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).</td>
</tr>
<tr>
<td>K0393</td>
<td>Knowledge of common networking devices and their configurations.</td>
</tr>
<tr>
<td>K0394</td>
<td>Knowledge of common reporting databases and tools.</td>
</tr>
<tr>
<td>K0395</td>
<td>Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0396</td>
<td>Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.</td>
</tr>
<tr>
<td>K0397</td>
<td>Knowledge of concepts for operating systems (e.g., Linux, Unix.)</td>
</tr>
<tr>
<td>K0398</td>
<td>Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).</td>
</tr>
<tr>
<td>K0399</td>
<td>Knowledge of crisis action planning and time sensitive planning procedures.</td>
</tr>
<tr>
<td>K0400</td>
<td>Knowledge of crisis action planning for cyber operations.</td>
</tr>
<tr>
<td>K0401</td>
<td>Knowledge of criteria for evaluating collection products.</td>
</tr>
<tr>
<td>K0402</td>
<td>Knowledge of criticality and vulnerability factors (e.g., value, recuperation, cushion, countermeasures) for target selection and applicability to the cyber domain.</td>
</tr>
<tr>
<td>K0403</td>
<td>Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.</td>
</tr>
<tr>
<td>K0404</td>
<td>Knowledge of current collection requirements.</td>
</tr>
<tr>
<td>K0405</td>
<td>Knowledge of current computer-based intrusion sets.</td>
</tr>
<tr>
<td>K0406</td>
<td>Knowledge of current software and methodologies for active defense and system hardening.</td>
</tr>
<tr>
<td>K0407</td>
<td>Knowledge of customer information needs.</td>
</tr>
<tr>
<td>K0408</td>
<td>Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber attack) principles, capabilities, limitations, and effects.</td>
</tr>
<tr>
<td>K0409</td>
<td>Knowledge of cyber intelligence/information collection capabilities and repositories.</td>
</tr>
<tr>
<td>K0410</td>
<td>Knowledge of cyber laws and their effect on Cyber planning.</td>
</tr>
<tr>
<td>K0411</td>
<td>Knowledge of cyber laws, legal considerations and their effect on cyber planning.</td>
</tr>
<tr>
<td>K0412</td>
<td>Knowledge of cyber lexicon/terminology</td>
</tr>
<tr>
<td>K0413</td>
<td>Knowledge of cyber operation objectives, policies, and legalities.</td>
</tr>
<tr>
<td>K0414</td>
<td>Knowledge of cyber operations support or enabling processes.</td>
</tr>
<tr>
<td>K0415</td>
<td>Knowledge of cyber operations terminology/lexicon.</td>
</tr>
<tr>
<td>K0416</td>
<td>Knowledge of cyber operations.</td>
</tr>
<tr>
<td>K0417</td>
<td>Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).</td>
</tr>
<tr>
<td>K0418</td>
<td>Knowledge of data flow process for terminal or environment collection.</td>
</tr>
<tr>
<td>K0419</td>
<td>Knowledge of database administration and maintenance.</td>
</tr>
<tr>
<td>K0420</td>
<td>Knowledge of database theory.</td>
</tr>
<tr>
<td>K0421</td>
<td>Knowledge of databases, portals and associated dissemination vehicles.</td>
</tr>
<tr>
<td>K0422</td>
<td>Knowledge of deconfliction processes and procedures.</td>
</tr>
<tr>
<td>K0423</td>
<td>Knowledge of deconfliction reporting to include external organization interaction.</td>
</tr>
<tr>
<td>K0424</td>
<td>Knowledge of denial and deception techniques.</td>
</tr>
<tr>
<td>K0425</td>
<td>Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.</td>
</tr>
<tr>
<td>K0426</td>
<td>Knowledge of dynamic and deliberate targeting.</td>
</tr>
<tr>
<td>K0427</td>
<td>Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).</td>
</tr>
<tr>
<td>K0428</td>
<td>Knowledge of encryption algorithms and tools for WLANs.</td>
</tr>
<tr>
<td>K0429</td>
<td>Knowledge of enterprise-wide information management.</td>
</tr>
<tr>
<td>K0430</td>
<td>Knowledge of evasion strategies and techniques.</td>
</tr>
<tr>
<td>K0431</td>
<td>Knowledge of evolving/emerging communications technologies.</td>
</tr>
<tr>
<td>K0432</td>
<td>Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.</td>
</tr>
<tr>
<td>K0433</td>
<td>Knowledge of forensic implications of operating system structure and operations.</td>
</tr>
<tr>
<td>K0434</td>
<td>Knowledge of front-end collection systems, including traffic collection, filtering, and selection.</td>
</tr>
<tr>
<td>K0435</td>
<td>Knowledge of fundamental cyber concepts, principles, limitations, and effects.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0436</td>
<td>Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.</td>
</tr>
<tr>
<td>K0437</td>
<td>Knowledge of general SCADA system components.</td>
</tr>
<tr>
<td>K0438</td>
<td>Knowledge of Global Systems for Mobile Communications (GSM) architecture.</td>
</tr>
<tr>
<td>K0439</td>
<td>Knowledge of governing authorities for targeting.</td>
</tr>
<tr>
<td>K0440</td>
<td>Knowledge of host-based security products and how they affect exploitation and vulnerability.</td>
</tr>
<tr>
<td>K0441</td>
<td>Knowledge of how collection requirements and information needs are translated, tracked, and prioritized across the extended enterprise.</td>
</tr>
<tr>
<td>K0442</td>
<td>Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).</td>
</tr>
<tr>
<td>K0443</td>
<td>Knowledge of how hubs, switches, routers work together in the design of a network.</td>
</tr>
<tr>
<td>K0444</td>
<td>Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).</td>
</tr>
<tr>
<td>K0445</td>
<td>Knowledge of how modern digital and telephony networks impact cyber operations.</td>
</tr>
<tr>
<td>K0446</td>
<td>Knowledge of how modern wireless communications systems impact cyber operations.</td>
</tr>
<tr>
<td>K0447</td>
<td>Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).</td>
</tr>
<tr>
<td>K0448</td>
<td>Knowledge of how to establish priorities for resources.</td>
</tr>
<tr>
<td>K0449</td>
<td>Knowledge of how to extract, analyze, and use metadata.</td>
</tr>
<tr>
<td>K0450</td>
<td>Withdrawn – Integrated into K0036</td>
</tr>
<tr>
<td>K0451</td>
<td>Knowledge of identification and reporting processes.</td>
</tr>
<tr>
<td>K0452</td>
<td>Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.</td>
</tr>
<tr>
<td>K0453</td>
<td>Knowledge of indications and warning.</td>
</tr>
<tr>
<td>K0454</td>
<td>Knowledge of information needs.</td>
</tr>
<tr>
<td>K0455</td>
<td>Knowledge of information security concepts, facilitating technologies and methods.</td>
</tr>
<tr>
<td>K0456</td>
<td>Knowledge of intelligence capabilities and limitations.</td>
</tr>
<tr>
<td>K0457</td>
<td>Knowledge of intelligence confidence levels.</td>
</tr>
<tr>
<td>K0458</td>
<td>Knowledge of intelligence disciplines.</td>
</tr>
<tr>
<td>K0459</td>
<td>Knowledge of intelligence employment requirements (i.e., logistical, communications support, maneuverability, legal restrictions, etc.).</td>
</tr>
<tr>
<td>K0460</td>
<td>Knowledge of intelligence preparation of the environment and similar processes.</td>
</tr>
<tr>
<td>K0461</td>
<td>Knowledge of intelligence production processes.</td>
</tr>
<tr>
<td>K0462</td>
<td>Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.</td>
</tr>
<tr>
<td>K0463</td>
<td>Knowledge of intelligence requirements tasking systems.</td>
</tr>
<tr>
<td>K0464</td>
<td>Knowledge of intelligence support to planning, execution, and assessment.</td>
</tr>
<tr>
<td>K0465</td>
<td>Knowledge of internal and external partner cyber operations capabilities and tools.</td>
</tr>
<tr>
<td>K0466</td>
<td>Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.</td>
</tr>
<tr>
<td>K0467</td>
<td>Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).</td>
</tr>
<tr>
<td>K0468</td>
<td>Knowledge of internal and external partner reporting.</td>
</tr>
<tr>
<td>K0469</td>
<td>Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.</td>
</tr>
<tr>
<td>K0470</td>
<td>Knowledge of Internet and routing protocols.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0471</td>
<td>Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).</td>
</tr>
<tr>
<td>K0472</td>
<td>Knowledge of intrusion detection systems and signature development.</td>
</tr>
<tr>
<td>K0473</td>
<td>Knowledge of intrusion sets.</td>
</tr>
<tr>
<td>K0474</td>
<td>Knowledge of key cyber threat actors and their equities.</td>
</tr>
<tr>
<td>K0475</td>
<td>Knowledge of key factors of the operational environment and threat.</td>
</tr>
<tr>
<td>K0476</td>
<td>Knowledge of language processing tools and techniques.</td>
</tr>
<tr>
<td>K0477</td>
<td>Knowledge of leadership's Intent and objectives.</td>
</tr>
<tr>
<td>K0478</td>
<td>Knowledge of legal considerations in targeting.</td>
</tr>
<tr>
<td>K0479</td>
<td>Knowledge of malware analysis and characteristics.</td>
</tr>
<tr>
<td>K0480</td>
<td>Knowledge of malware.</td>
</tr>
<tr>
<td>K0481</td>
<td>Knowledge of methods and techniques used to detect various exploitation activities</td>
</tr>
<tr>
<td>K0482</td>
<td>Knowledge of methods for ascertaining collection asset posture and availability.</td>
</tr>
<tr>
<td>K0483</td>
<td>Knowledge of methods to integrate and summarize information from any potential sources.</td>
</tr>
<tr>
<td>K0484</td>
<td>Knowledge of midpoint collection (process, objectives, organization, targets, etc.).</td>
</tr>
<tr>
<td>K0485</td>
<td>Knowledge of network administration.</td>
</tr>
<tr>
<td>K0486</td>
<td>Knowledge of network construction and topology.</td>
</tr>
<tr>
<td>K0487</td>
<td>Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).</td>
</tr>
<tr>
<td>K0488</td>
<td>Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network.</td>
</tr>
<tr>
<td>K0489</td>
<td>Knowledge of network topology.</td>
</tr>
<tr>
<td>K0490</td>
<td>Withdrawn – Integrated into K0058</td>
</tr>
<tr>
<td>K0491</td>
<td>Knowledge of networking and internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).</td>
</tr>
<tr>
<td>K0492</td>
<td>Knowledge of non-traditional collection methodologies.</td>
</tr>
<tr>
<td>K0493</td>
<td>Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/VPS, encryption).</td>
</tr>
<tr>
<td>K0494</td>
<td>Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.</td>
</tr>
<tr>
<td>K0495</td>
<td>Knowledge of ongoing and future operations.</td>
</tr>
<tr>
<td>K0496</td>
<td>Knowledge of operational asset constraints.</td>
</tr>
<tr>
<td>K0497</td>
<td>Knowledge of operational effectiveness assessment.</td>
</tr>
<tr>
<td>K0498</td>
<td>Knowledge of operational planning processes.</td>
</tr>
<tr>
<td>K0499</td>
<td>Knowledge of operations security.</td>
</tr>
<tr>
<td>K0500</td>
<td>Knowledge of organization and/or partner collection systems, capabilities, and processes (e.g., collection and protocol processors).</td>
</tr>
<tr>
<td>K0501</td>
<td>Knowledge of organization cyber operations programs, strategies, and resources.</td>
</tr>
<tr>
<td>K0502</td>
<td>Knowledge of organization decision support tools and/or methods.</td>
</tr>
<tr>
<td>K0503</td>
<td>Knowledge of organization formats of resource and asset readiness reporting, its operational relevance and intelligence collection impact.</td>
</tr>
<tr>
<td>K0504</td>
<td>Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.</td>
</tr>
<tr>
<td>K0505</td>
<td>Knowledge of organization objectives and associated demand on collection management.</td>
</tr>
<tr>
<td>K0506</td>
<td>Knowledge of organization objectives, leadership priorities, and decision-making risks.</td>
</tr>
<tr>
<td>K0507</td>
<td>Knowledge of organization or partner exploitation of digital networks.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0508</td>
<td>Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.</td>
</tr>
<tr>
<td>K0509</td>
<td>Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.</td>
</tr>
<tr>
<td>K0510</td>
<td>Knowledge of organizational and partner policies, tools, capabilities, and procedures.</td>
</tr>
<tr>
<td>K0511</td>
<td>Knowledge of organizational hierarchy and cyber decision making processes.</td>
</tr>
<tr>
<td>K0512</td>
<td>Knowledge of organizational planning concepts.</td>
</tr>
<tr>
<td>K0513</td>
<td>Knowledge of organizational priorities, legal authorities and requirements submission processes.</td>
</tr>
<tr>
<td>K0514</td>
<td>Knowledge of organizational structures and associated intelligence capabilities.</td>
</tr>
<tr>
<td>K0515</td>
<td>Knowledge of OSI model and underlying networking protocols (e.g., TCP/IP).</td>
</tr>
<tr>
<td>K0516</td>
<td>Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.</td>
</tr>
<tr>
<td>K0517</td>
<td>Knowledge of PIR approval process.</td>
</tr>
<tr>
<td>K0518</td>
<td>Knowledge of planning activity initiation.</td>
</tr>
<tr>
<td>K0519</td>
<td>Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.</td>
</tr>
<tr>
<td>K0520</td>
<td>Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.</td>
</tr>
<tr>
<td>K0521</td>
<td>Knowledge of priority information, how it is derived, where it is published, how to access, etc.</td>
</tr>
<tr>
<td>K0522</td>
<td>Knowledge of production exploitation and dissemination needs and architectures.</td>
</tr>
<tr>
<td>K0523</td>
<td>Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky) and how differences affect exploitation/vulnerabilities.</td>
</tr>
<tr>
<td>K0524</td>
<td>Knowledge of relevant laws, regulations, policies.</td>
</tr>
<tr>
<td>K0525</td>
<td>Knowledge of required intelligence planning products associated with cyber operational planning.</td>
</tr>
<tr>
<td>K0526</td>
<td>Knowledge of research strategies and knowledge management.</td>
</tr>
<tr>
<td>K0527</td>
<td>Knowledge of risk management and mitigation strategies.</td>
</tr>
<tr>
<td>K0528</td>
<td>Knowledge of satellite-based communication systems.</td>
</tr>
<tr>
<td>K0529</td>
<td>Knowledge of scripting</td>
</tr>
<tr>
<td>K0530</td>
<td>Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.</td>
</tr>
<tr>
<td>K0531</td>
<td>Knowledge of security implications of software configurations.</td>
</tr>
<tr>
<td>K0532</td>
<td>Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, codewords).</td>
</tr>
<tr>
<td>K0533</td>
<td>Knowledge of specific target identifiers, and their usage.</td>
</tr>
<tr>
<td>K0534</td>
<td>Knowledge of staff management, assignment, and allocation processes.</td>
</tr>
<tr>
<td>K0535</td>
<td>Knowledge of strategies and tools for target research.</td>
</tr>
<tr>
<td>K0536</td>
<td>Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).</td>
</tr>
<tr>
<td>K0537</td>
<td>Knowledge of system administration concepts for the Unix/Linux and Windows operating systems (e.g., process management, directory structure, installed applications, Access Controls).</td>
</tr>
<tr>
<td>K0538</td>
<td>Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0539</td>
<td>Knowledge of target communication profiles and their key elements (e.g., target associations, activities, communication infrastructure).</td>
</tr>
<tr>
<td>K0540</td>
<td>Knowledge of target communication tools and techniques.</td>
</tr>
<tr>
<td>K0541</td>
<td>Knowledge of target cultural references, dialects, expressions, idioms, and abbreviations.</td>
</tr>
<tr>
<td>K0542</td>
<td>Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).</td>
</tr>
<tr>
<td>K0543</td>
<td>Knowledge of target estimated repair and recuperation times.</td>
</tr>
<tr>
<td>K0544</td>
<td>Knowledge of target intelligence gathering and operational preparation techniques and life cycles.</td>
</tr>
<tr>
<td>K0545</td>
<td>Knowledge of target language(s).</td>
</tr>
<tr>
<td>K0546</td>
<td>Knowledge of target list development (i.e. RTL, JTL, CTL, etc.).</td>
</tr>
<tr>
<td>K0547</td>
<td>Knowledge of target methods and procedures.</td>
</tr>
<tr>
<td>K0548</td>
<td>Knowledge of target or threat cyber actors and procedures.</td>
</tr>
<tr>
<td>K0549</td>
<td>Knowledge of target vetting and validation procedures.</td>
</tr>
<tr>
<td>K0550</td>
<td>Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.</td>
</tr>
<tr>
<td>K0551</td>
<td>Knowledge of targeting cycles.</td>
</tr>
<tr>
<td>K0552</td>
<td>Knowledge of tasking mechanisms.</td>
</tr>
<tr>
<td>K0553</td>
<td>Knowledge of tasking processes for organic and subordinate collection assets.</td>
</tr>
<tr>
<td>K0554</td>
<td>Knowledge of tasking, collection, processing, exploitation and dissemination.</td>
</tr>
<tr>
<td>K0555</td>
<td>Knowledge of TCP/IP networking protocols.</td>
</tr>
<tr>
<td>K0556</td>
<td>Knowledge of telecommunications fundamentals.</td>
</tr>
<tr>
<td>K0557</td>
<td>Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).</td>
</tr>
<tr>
<td>K0558</td>
<td>Knowledge of the available tools and applications associated with collection requirements and collection management.</td>
</tr>
<tr>
<td>K0559</td>
<td>Knowledge of the basic structure, architecture, and design of converged applications.</td>
</tr>
<tr>
<td>K0560</td>
<td>Knowledge of the basic structure, architecture, and design of modern communication networks.</td>
</tr>
<tr>
<td>K0561</td>
<td>Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).</td>
</tr>
<tr>
<td>K0562</td>
<td>Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.</td>
</tr>
<tr>
<td>K0563</td>
<td>Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.</td>
</tr>
<tr>
<td>K0564</td>
<td>Knowledge of the characteristics of targeted communication networks (e.g., capacity, functionality, paths, critical nodes).</td>
</tr>
<tr>
<td>K0565</td>
<td>Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.</td>
</tr>
<tr>
<td>K0566</td>
<td>Knowledge of the critical information requirements and how they're used in planning.</td>
</tr>
<tr>
<td>K0567</td>
<td>Knowledge of the data flow from collection origin to repositories and tools.</td>
</tr>
<tr>
<td>K0568</td>
<td>Knowledge of the definition of collection management and collection management authority.</td>
</tr>
<tr>
<td>K0569</td>
<td>Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.</td>
</tr>
<tr>
<td>K0570</td>
<td>Knowledge of the factors of threat that could impact collection operations.</td>
</tr>
<tr>
<td>K0571</td>
<td>Knowledge of the feedback cycle in collection processes.</td>
</tr>
<tr>
<td>K0572</td>
<td>Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.</td>
</tr>
<tr>
<td>K0573</td>
<td>Knowledge of the fundamentals of digital forensics in order to extract actionable intelligence.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0574</td>
<td>Knowledge of the impact of language analysis on on-net operator functions.</td>
</tr>
<tr>
<td>K0575</td>
<td>Knowledge of the impacts of internal and external partner staffing estimates.</td>
</tr>
<tr>
<td>K0576</td>
<td>Knowledge of the information environment.</td>
</tr>
<tr>
<td>K0577</td>
<td>Knowledge of the intelligence frameworks, processes, and related systems.</td>
</tr>
<tr>
<td>K0578</td>
<td>Knowledge of the intelligence requirements development and request for information processes.</td>
</tr>
<tr>
<td>K0579</td>
<td>Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-</td>
</tr>
<tr>
<td></td>
<td>elements.</td>
</tr>
<tr>
<td>K0580</td>
<td>Knowledge of the organization’s established format for collection plan.</td>
</tr>
<tr>
<td>K0581</td>
<td>Knowledge of the organization’s planning, operations and targeting cycles.</td>
</tr>
<tr>
<td>K0582</td>
<td>Knowledge of the organizational planning and staffing process.</td>
</tr>
<tr>
<td>K0583</td>
<td>Knowledge of the organizational plans/directives/guidance that describe objectives.</td>
</tr>
<tr>
<td>K0584</td>
<td>Knowledge of the organizational policies/procedures for temporary transfer of collection</td>
</tr>
<tr>
<td></td>
<td>authority.</td>
</tr>
<tr>
<td>K0585</td>
<td>Knowledge of the organizational structure as it pertains to full spectrum cyber operations,</td>
</tr>
<tr>
<td></td>
<td>including the functions, responsibilities, and interrelationships among distinct internal</td>
</tr>
<tr>
<td></td>
<td>elements.</td>
</tr>
<tr>
<td>K0586</td>
<td>Knowledge of the outputs of course of action and exercise analysis.</td>
</tr>
<tr>
<td>K0587</td>
<td>Knowledge of the POC’s, databases, tools and applications necessary to establish environment</td>
</tr>
<tr>
<td></td>
<td>preparation and surveillance products.</td>
</tr>
<tr>
<td>K0588</td>
<td>Knowledge of the priority information requirements from subordinate, lateral and higher</td>
</tr>
<tr>
<td></td>
<td>levels of the organization.</td>
</tr>
<tr>
<td>K0589</td>
<td>Knowledge of the process used to assess the performance and impact of operations.</td>
</tr>
<tr>
<td>K0590</td>
<td>Knowledge of the processes to synchronize operational assessment procedures with the</td>
</tr>
<tr>
<td></td>
<td>critical information requirement process.</td>
</tr>
<tr>
<td>K0591</td>
<td>Knowledge of the production responsibilities and organic analysis and production capabilities.</td>
</tr>
<tr>
<td>K0592</td>
<td>Knowledge of the purpose and contribution of target templates.</td>
</tr>
<tr>
<td>K0593</td>
<td>Knowledge of the range of cyber operations and their underlying intelligence support needs,</td>
</tr>
<tr>
<td></td>
<td>topics, and focus areas.</td>
</tr>
<tr>
<td>K0594</td>
<td>Knowledge of the relationships between end states, objectives, effects, lines of operation,</td>
</tr>
<tr>
<td></td>
<td>etc.</td>
</tr>
<tr>
<td>K0595</td>
<td>Knowledge of the relationships of operational objectives, intelligence requirements, and</td>
</tr>
<tr>
<td></td>
<td>intelligence production tasks.</td>
</tr>
<tr>
<td>K0596</td>
<td>Knowledge of the request for information process.</td>
</tr>
<tr>
<td>K0597</td>
<td>Knowledge of the role of network operations in supporting and facilitating other organization</td>
</tr>
<tr>
<td></td>
<td>operations.</td>
</tr>
<tr>
<td>K0598</td>
<td>Knowledge of the structure and intent of organization specific plans, guidance and</td>
</tr>
<tr>
<td></td>
<td>authorizations.</td>
</tr>
<tr>
<td>K0599</td>
<td>Knowledge of the structure, architecture, and design of modern digital and telephony networks.</td>
</tr>
<tr>
<td>K0600</td>
<td>Knowledge of the structure, architecture, and design of modern wireless communications systems.</td>
</tr>
<tr>
<td>K0601</td>
<td>Knowledge of the systems/architecture/communications used for coordination.</td>
</tr>
<tr>
<td>K0602</td>
<td>Knowledge of the various collection disciplines and capabilities.</td>
</tr>
<tr>
<td>K0603</td>
<td>Knowledge of the ways in which targets or threats use the Internet.</td>
</tr>
<tr>
<td>K0604</td>
<td>Knowledge of threat and/or target systems.</td>
</tr>
<tr>
<td>K0605</td>
<td>Knowledge of tipping, cueing, mixing, and redundancy.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0606</td>
<td>Knowledge of transcript development processes and techniques (e.g., verbatim, gists, summaries).</td>
</tr>
<tr>
<td>K0607</td>
<td>Knowledge of translation processes and techniques.</td>
</tr>
<tr>
<td>K0608</td>
<td>Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).</td>
</tr>
<tr>
<td>K0609</td>
<td>Knowledge of virtual machine technologies.</td>
</tr>
<tr>
<td>K0610</td>
<td>Knowledge of virtualization products (VMware, Virtual PC).</td>
</tr>
<tr>
<td>K0611</td>
<td>Withdrawn – Integrated into K0131</td>
</tr>
<tr>
<td>K0612</td>
<td>Knowledge of what constitutes a “threat” to a network.</td>
</tr>
<tr>
<td>K0613</td>
<td>Knowledge of who the organization’s operational planners are, how and where they can be contacted, and what are their expectations.</td>
</tr>
<tr>
<td>K0614</td>
<td>Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.</td>
</tr>
</tbody>
</table>
A.6 NCWF Skills Descriptions

Table 7 provides a listing of specific skills that might be demonstrated by a person in a given cybersecurity position. Selected skills descriptions from this list are included in the Detailed Work Role Listing in Appendix B. Because the list of skills has evolved over many years and is expected to continue to do so, it is not sorted in a particular order and will simply continue to grow sequentially.

Table 7 - NCWF Skills Descriptions

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0001</td>
<td>Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.</td>
</tr>
<tr>
<td>S0002</td>
<td>Skill in allocating storage capacity in the design of data management systems.</td>
</tr>
<tr>
<td>S0003</td>
<td>Skill of identifying, capturing, containing, and reporting malware.</td>
</tr>
<tr>
<td>S0004</td>
<td>Skill in analyzing network traffic capacity and performance characteristics.</td>
</tr>
<tr>
<td>S0005</td>
<td>Skill in applying and incorporating information technologies into proposed solutions.</td>
</tr>
<tr>
<td>S0006</td>
<td>Skill in applying confidentiality, integrity, and availability principles.</td>
</tr>
<tr>
<td>S0007</td>
<td>Skill in applying host/network access controls (e.g., access control list).</td>
</tr>
<tr>
<td>S0008</td>
<td>Skill in applying organization-specific systems analysis principles and techniques.</td>
</tr>
<tr>
<td>S0009</td>
<td>Skill in assessing the robustness of security systems and designs.</td>
</tr>
<tr>
<td>S0010</td>
<td>Skill in conducting capabilities and requirements analysis.</td>
</tr>
<tr>
<td>S0011</td>
<td>Skill in conducting information searches.</td>
</tr>
<tr>
<td>S0012</td>
<td>Skill in conducting knowledge mapping (e.g., map of knowledge repositories).</td>
</tr>
<tr>
<td>S0013</td>
<td>Skill in conducting queries and developing algorithms to analyze data structures.</td>
</tr>
<tr>
<td>S0014</td>
<td>Skill in conducting software debugging.</td>
</tr>
<tr>
<td>S0015</td>
<td>Skill in conducting test events.</td>
</tr>
<tr>
<td>S0016</td>
<td>Skill in configuring and optimizing software.</td>
</tr>
<tr>
<td>S0017</td>
<td>Skill in creating and utilizing mathematical or statistical models.</td>
</tr>
<tr>
<td>S0018</td>
<td>Skill in creating policies that reflect system security objectives.</td>
</tr>
<tr>
<td>S0019</td>
<td>Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.</td>
</tr>
<tr>
<td>S0020</td>
<td>Skill in developing and deploying signatures.</td>
</tr>
<tr>
<td>S0021</td>
<td>Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data).</td>
</tr>
<tr>
<td>S0022</td>
<td>Skill in designing countermeasures to identified security risks.</td>
</tr>
<tr>
<td>S0023</td>
<td>Skill in designing security controls based on cybersecurity principles and tenets.</td>
</tr>
<tr>
<td>S0024</td>
<td>Skill in designing the integration of hardware and software solutions.</td>
</tr>
<tr>
<td>S0025</td>
<td>Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).</td>
</tr>
<tr>
<td>S0026</td>
<td>Skill in determining an appropriate level of test rigor for a given system.</td>
</tr>
<tr>
<td>S0027</td>
<td>Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.</td>
</tr>
<tr>
<td>S0028</td>
<td>Skill in developing data dictionaries.</td>
</tr>
<tr>
<td>S0029</td>
<td>Skill in developing data models.</td>
</tr>
<tr>
<td>S0030</td>
<td>Skill in developing operations-based testing scenarios.</td>
</tr>
<tr>
<td>S0031</td>
<td>Skill in developing and applying security system access controls.</td>
</tr>
<tr>
<td>S0032</td>
<td>Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.</td>
</tr>
<tr>
<td>S0033</td>
<td>Skill in diagnosing connectivity problems.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0034</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks.</td>
</tr>
<tr>
<td>S0035</td>
<td>Skill in establishing a routing schema.</td>
</tr>
<tr>
<td>S0036</td>
<td>Skill in evaluating the adequacy of security designs.</td>
</tr>
<tr>
<td>S0037</td>
<td>Skill in generating queries and reports.</td>
</tr>
<tr>
<td>S0038</td>
<td>Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.</td>
</tr>
<tr>
<td>S0039</td>
<td>Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.</td>
</tr>
<tr>
<td>S0040</td>
<td>Skill in implementing, maintaining, and improving established network security practices.</td>
</tr>
<tr>
<td>S0041</td>
<td>Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.</td>
</tr>
<tr>
<td>S0042</td>
<td>Skill in maintaining databases.</td>
</tr>
<tr>
<td>S0043</td>
<td>Skill in maintaining directory services.</td>
</tr>
<tr>
<td>S0044</td>
<td>Skill in mimicking threat behaviors.</td>
</tr>
<tr>
<td>S0045</td>
<td>Skill in optimizing database performance.</td>
</tr>
<tr>
<td>S0046</td>
<td>Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).</td>
</tr>
<tr>
<td>S0047</td>
<td>Skill in preserving evidence integrity according to standard operating procedures or national standards.</td>
</tr>
<tr>
<td>S0048</td>
<td>Skill in systems integration testing.</td>
</tr>
<tr>
<td>S0049</td>
<td>Skill in the measuring and reporting of intellectual capital.</td>
</tr>
<tr>
<td>S0050</td>
<td>Skill in design modeling and building use cases (e.g., unified modeling language).</td>
</tr>
<tr>
<td>S0051</td>
<td>Skill in the use of penetration testing tools and techniques.</td>
</tr>
<tr>
<td>S0052</td>
<td>Skill in the use of social engineering techniques.</td>
</tr>
<tr>
<td>S0053</td>
<td>Skill in tuning sensors.</td>
</tr>
<tr>
<td>S0054</td>
<td>Skill in using incident handling methodologies.</td>
</tr>
<tr>
<td>S0055</td>
<td>Skill in using knowledge management technologies.</td>
</tr>
<tr>
<td>S0056</td>
<td>Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).</td>
</tr>
<tr>
<td>S0057</td>
<td>Skill in using protocol analyzers.</td>
</tr>
<tr>
<td>S0058</td>
<td>Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.</td>
</tr>
<tr>
<td>S0059</td>
<td>Skill in using Virtual Private Network (VPN) devices and encryption.</td>
</tr>
<tr>
<td>S0060</td>
<td>Skill in writing code in a currently supported programming language (e.g., Java, C++).</td>
</tr>
<tr>
<td>S0061</td>
<td>Skill in writing test plans.</td>
</tr>
<tr>
<td>S0062</td>
<td>Skill in analyzing memory dumps to extract information.</td>
</tr>
<tr>
<td>S0063</td>
<td>Skill in collecting data from a variety of cyber defense resources.</td>
</tr>
<tr>
<td>S0064</td>
<td>Skill in developing and executing technical training programs and curricula.</td>
</tr>
<tr>
<td>S0065</td>
<td>Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).</td>
</tr>
<tr>
<td>S0066</td>
<td>Skill in identifying gaps in technical capabilities.</td>
</tr>
<tr>
<td>S0067</td>
<td>Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).</td>
</tr>
<tr>
<td>S0068</td>
<td>Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.</td>
</tr>
<tr>
<td>S0069</td>
<td>Skill in setting up a forensic workstation.</td>
</tr>
<tr>
<td>S0070</td>
<td>Skill in talking to others to convey information effectively.</td>
</tr>
<tr>
<td>S0071</td>
<td>Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0072</td>
<td>Skill in using scientific rules and methods to solve problems.</td>
</tr>
<tr>
<td>S0073</td>
<td>Skill in using virtual machines.</td>
</tr>
<tr>
<td>S0074</td>
<td>Skill in physically disassembling PCs.</td>
</tr>
<tr>
<td>S0075</td>
<td>Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).</td>
</tr>
<tr>
<td>S0076</td>
<td>Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware).</td>
</tr>
<tr>
<td>S0077</td>
<td>Skill in securing network communications.</td>
</tr>
<tr>
<td>S0078</td>
<td>Skill in recognizing and categorizing types of vulnerabilities and associated attacks.</td>
</tr>
<tr>
<td>S0079</td>
<td>Skill in protecting a network against malware.</td>
</tr>
<tr>
<td>S0080</td>
<td>Skill in performing damage assessments.</td>
</tr>
<tr>
<td>S0081</td>
<td>Skill in using network analysis tools to identify vulnerabilities.</td>
</tr>
<tr>
<td>S0082</td>
<td>Skill in evaluating test plans for applicability and completeness.</td>
</tr>
<tr>
<td>S0083</td>
<td>Skill in integrating black box security testing tools into quality assurance process of software releases.</td>
</tr>
<tr>
<td>S0084</td>
<td>Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNS, network intrusion detection systems).</td>
</tr>
<tr>
<td>S0085</td>
<td>Skill in conducting audits or reviews of technical systems.</td>
</tr>
<tr>
<td>S0086</td>
<td>Skill in evaluating the trustworthiness of the supplier and/or product.</td>
</tr>
<tr>
<td>S0087</td>
<td>Skill in deep analysis of captured malicious code (e.g., malware forensics).</td>
</tr>
<tr>
<td>S0088</td>
<td>Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).</td>
</tr>
<tr>
<td>S0089</td>
<td>Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).</td>
</tr>
<tr>
<td>S0090</td>
<td>Skill in analyzing anomalous code as malicious or benign.</td>
</tr>
<tr>
<td>S0091</td>
<td>Skill in analyzing volatile data.</td>
</tr>
<tr>
<td>S0092</td>
<td>Skill in identifying obfuscation techniques.</td>
</tr>
<tr>
<td>S0093</td>
<td>Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.</td>
</tr>
<tr>
<td>S0094</td>
<td>Skill in reading Hexadecimal data.</td>
</tr>
<tr>
<td>S0095</td>
<td>Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode).</td>
</tr>
<tr>
<td>S0096</td>
<td>Skill in reading and interpreting signatures (e.g., snort).</td>
</tr>
<tr>
<td>S0097</td>
<td>Skill in applying security controls.</td>
</tr>
<tr>
<td>S0098</td>
<td>Skill in detecting host and network based intrusions via intrusion detection technologies.</td>
</tr>
<tr>
<td>S0099</td>
<td>Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes.</td>
</tr>
<tr>
<td>S0100</td>
<td>Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).</td>
</tr>
<tr>
<td>S0101</td>
<td>Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.</td>
</tr>
<tr>
<td>S0102</td>
<td>Skill in applying technical delivery capabilities.</td>
</tr>
<tr>
<td>S0103</td>
<td>Skill in assessing the predictive power and subsequent generalizability of a model.</td>
</tr>
<tr>
<td>S0104</td>
<td>Skill in conducting Test Readiness Reviews.</td>
</tr>
<tr>
<td>S0105</td>
<td>Skill in data mining techniques.</td>
</tr>
<tr>
<td>S0106</td>
<td>Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing).</td>
</tr>
<tr>
<td>S0107</td>
<td>Skill in designing and documenting overall program Test &amp; Evaluation strategies.</td>
</tr>
<tr>
<td>S0108</td>
<td>Skill in developing workforce and position qualification standards.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0109</td>
<td>Skill in identifying hidden patterns or relationships.</td>
</tr>
<tr>
<td>S0110</td>
<td>Skill in identifying Test &amp; Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.</td>
</tr>
<tr>
<td>S0111</td>
<td>Skill in interfacing with customers.</td>
</tr>
<tr>
<td>S0112</td>
<td>Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.</td>
</tr>
<tr>
<td>S0113</td>
<td>Skill in performing format conversions to create a standard representation of the data.</td>
</tr>
<tr>
<td>S0114</td>
<td>Skill in performing sensitivity analysis.</td>
</tr>
<tr>
<td>S0115</td>
<td>Skill in preparing Test &amp; Evaluation reports.</td>
</tr>
<tr>
<td>S0116</td>
<td>Skill in designing multi-level security/cross domain solutions.</td>
</tr>
<tr>
<td>S0117</td>
<td>Skill in providing Test &amp; Evaluation resource estimate.</td>
</tr>
<tr>
<td>S0118</td>
<td>Skill in developing machine understandable semantic ontologies.</td>
</tr>
<tr>
<td>S0119</td>
<td>Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic).</td>
</tr>
<tr>
<td>S0120</td>
<td>Skill in reviewing logs to identify evidence of past intrusions.</td>
</tr>
<tr>
<td>S0121</td>
<td>Skill in system, network, and OS hardening techniques.</td>
</tr>
<tr>
<td>S0122</td>
<td>Skill in the use of design methods.</td>
</tr>
<tr>
<td>S0123</td>
<td>Skill in transformation analytics (e.g., aggregation, enrichment, processing).</td>
</tr>
<tr>
<td>S0124</td>
<td>Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.</td>
</tr>
<tr>
<td>S0125</td>
<td>Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).</td>
</tr>
<tr>
<td>S0126</td>
<td>Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS).</td>
</tr>
<tr>
<td>S0127</td>
<td>Skill in using data mapping tools.</td>
</tr>
<tr>
<td>S0128</td>
<td>Skill in using manpower and personnel IT systems.</td>
</tr>
<tr>
<td>S0129</td>
<td>Skill in using outlier identification and removal techniques.</td>
</tr>
<tr>
<td>S0130</td>
<td>Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.</td>
</tr>
<tr>
<td>S0131</td>
<td>Skill in analyzing malware.</td>
</tr>
<tr>
<td>S0132</td>
<td>Skill in conducting bit-level analysis.</td>
</tr>
<tr>
<td>S0133</td>
<td>Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.</td>
</tr>
<tr>
<td>S0134</td>
<td>Skill in conducting reviews of systems.</td>
</tr>
<tr>
<td>S0135</td>
<td>Skill in secure test plan design (e.g. unit, integration, system, acceptance).</td>
</tr>
<tr>
<td>S0136</td>
<td>Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.</td>
</tr>
<tr>
<td>S0137</td>
<td>Skill in conducting application vulnerability assessments.</td>
</tr>
<tr>
<td>S0138</td>
<td>Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).</td>
</tr>
<tr>
<td>S0139</td>
<td>Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).</td>
</tr>
<tr>
<td>S0140</td>
<td>Skill in applying the systems engineering process.</td>
</tr>
<tr>
<td>S0141</td>
<td>Skill in assessing security systems designs.</td>
</tr>
<tr>
<td>S0142</td>
<td>Skill in conducting research for troubleshooting novel client-level problems.</td>
</tr>
<tr>
<td>S0143</td>
<td>Skill in conducting system/server planning, management, and maintenance.</td>
</tr>
<tr>
<td>S0144</td>
<td>Skill in correcting physical and technical problems that impact system/server performance.</td>
</tr>
<tr>
<td>S0145</td>
<td>Skill in integrating and applying policies that meet system security objectives.</td>
</tr>
<tr>
<td>S0146</td>
<td>Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0147</td>
<td>Skill in assessing security controls based on cybersecurity principles and tenets.</td>
</tr>
<tr>
<td>S0148</td>
<td>Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.</td>
</tr>
<tr>
<td>S0149</td>
<td>Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.</td>
</tr>
<tr>
<td>S0150</td>
<td>Skill in implementing and testing network infrastructure contingency and recovery plans.</td>
</tr>
<tr>
<td>S0151</td>
<td>Skill in troubleshooting failed system components (i.e., servers)</td>
</tr>
<tr>
<td>S0152</td>
<td>Skill in translating operational requirements into protection needs (i.e., security controls).</td>
</tr>
<tr>
<td>S0153</td>
<td>Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.</td>
</tr>
<tr>
<td>S0154</td>
<td>Skill in installing system and component upgrades.</td>
</tr>
<tr>
<td>S0155</td>
<td>Skill in monitoring and optimizing system/server performance.</td>
</tr>
<tr>
<td>S0156</td>
<td>Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.).</td>
</tr>
<tr>
<td>S0157</td>
<td>Skill in recovering failed systems/servers.</td>
</tr>
<tr>
<td>S0158</td>
<td>Skill in operating system administration.</td>
</tr>
<tr>
<td>S0159</td>
<td>Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.</td>
</tr>
<tr>
<td>S0160</td>
<td>Skill in the use of design modeling (e.g., unified modeling language).</td>
</tr>
<tr>
<td>S0161</td>
<td>Withdrawn – Integrated into S0160</td>
</tr>
<tr>
<td>S0162</td>
<td>Skill in sub-netting.</td>
</tr>
<tr>
<td>S0163</td>
<td>Withdrawn – Integrated into S0060</td>
</tr>
<tr>
<td>S0164</td>
<td>Skill in assessing the application of cryptographic standards.</td>
</tr>
<tr>
<td>S0165</td>
<td>Skill in collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.</td>
</tr>
<tr>
<td>S0166</td>
<td>Skill in identifying gaps in technical delivery capabilities.</td>
</tr>
<tr>
<td>S0167</td>
<td>Skill in recognizing vulnerabilities in security systems.</td>
</tr>
<tr>
<td>S0168</td>
<td>Skill in applying cybersecurity methods, such as firewalls, demilitarized zones, and encryption.</td>
</tr>
<tr>
<td>S0169</td>
<td>Skill in conducting trend analysis.</td>
</tr>
<tr>
<td>S0170</td>
<td>Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).</td>
</tr>
<tr>
<td>S0171</td>
<td>Skill in performing impact/risk assessments.</td>
</tr>
<tr>
<td>S0172</td>
<td>Skill in applying secure coding techniques.</td>
</tr>
<tr>
<td>S0173</td>
<td>Skill in using security event correlation tools.</td>
</tr>
<tr>
<td>S0174</td>
<td>Skill in using code analysis tools.</td>
</tr>
<tr>
<td>S0175</td>
<td>Skill in performing root cause analysis.</td>
</tr>
<tr>
<td>S0176</td>
<td>Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.</td>
</tr>
<tr>
<td>S0177</td>
<td>Skill in analyzing a target's communication networks.</td>
</tr>
<tr>
<td>S0178</td>
<td>Skill in analyzing essential network data (e.g., router configuration files, routing protocols).</td>
</tr>
<tr>
<td>S0179</td>
<td>Skill in analyzing language processing tools to provide feedback to enhance tool development.</td>
</tr>
<tr>
<td>S0180</td>
<td>Withdrawn – Integrated into S0062</td>
</tr>
<tr>
<td>S0181</td>
<td>Skill in analyzing midpoint collection data.</td>
</tr>
<tr>
<td>S0182</td>
<td>Skill in analyzing target communications internals and externals collected from wireless LANs.</td>
</tr>
<tr>
<td>S0183</td>
<td>Skill in analyzing terminal or environment collection data.</td>
</tr>
<tr>
<td>S0184</td>
<td>Skill in analyzing traffic to identify network devices.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0185</td>
<td>Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.</td>
</tr>
<tr>
<td>S0186</td>
<td>Skill in applying crisis planning procedures.</td>
</tr>
<tr>
<td>S0187</td>
<td>Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/association or link analysis; Bayesian, Delphi, and Pattern analyses).</td>
</tr>
<tr>
<td>S0188</td>
<td>Skill in assessing a target's frame of reference (e.g., motivation, technical capability, organizational structure, sensitivities).</td>
</tr>
<tr>
<td>S0189</td>
<td>Skill in assessing and/or estimating effects generated during and after cyber operations.</td>
</tr>
<tr>
<td>S0190</td>
<td>Skill in assessing current tools to identify needed improvements.</td>
</tr>
<tr>
<td>S0191</td>
<td>Skill in assessing the applicability of available analytical tools to various situations.</td>
</tr>
<tr>
<td>S0192</td>
<td>Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.</td>
</tr>
<tr>
<td>S0193</td>
<td>Skill in complying with the legal restrictions for targeted information.</td>
</tr>
<tr>
<td>S0194</td>
<td>Skill in conducting non-attributable research.</td>
</tr>
<tr>
<td>S0195</td>
<td>Skill in conducting research using all available sources.</td>
</tr>
<tr>
<td>S0196</td>
<td>Skill in conducting research using deep web.</td>
</tr>
<tr>
<td>S0197</td>
<td>Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.</td>
</tr>
<tr>
<td>S0198</td>
<td>Skill in conducting social network analysis.</td>
</tr>
<tr>
<td>S0199</td>
<td>Skill in creating and extracting important information from packet captures.</td>
</tr>
<tr>
<td>S0200</td>
<td>Skill in creating collection requirements in support of data acquisition activities.</td>
</tr>
<tr>
<td>S0201</td>
<td>Skill in creating plans in support of remote operations.</td>
</tr>
<tr>
<td>S0202</td>
<td>Skill in data mining techniques (e.g., searching file systems) and analysis.</td>
</tr>
<tr>
<td>S0203</td>
<td>Skill in defining and characterizing all pertinent aspects of the operational environment.</td>
</tr>
<tr>
<td>S0204</td>
<td>Skill in depicting source or collateral data on a network map.</td>
</tr>
<tr>
<td>S0205</td>
<td>Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.</td>
</tr>
<tr>
<td>S0206</td>
<td>Skill in determining installed patches on various operating systems and identifying patch signatures.</td>
</tr>
<tr>
<td>S0207</td>
<td>Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments.</td>
</tr>
<tr>
<td>S0208</td>
<td>Skill in determining the physical location of network devices.</td>
</tr>
<tr>
<td>S0209</td>
<td>Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.</td>
</tr>
<tr>
<td>S0210</td>
<td>Skill in developing intelligence reports.</td>
</tr>
<tr>
<td>S0211</td>
<td>Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.</td>
</tr>
<tr>
<td>S0212</td>
<td>Skill in disseminating items of highest intelligence value in a timely manner.</td>
</tr>
<tr>
<td>S0213</td>
<td>Skill in documenting and communicating complex technical and programmatic information.</td>
</tr>
<tr>
<td>S0214</td>
<td>Skill in evaluating accesses for intelligence value.</td>
</tr>
<tr>
<td>S0215</td>
<td>Skill in evaluating and interpreting metadata.</td>
</tr>
<tr>
<td>S0216</td>
<td>Skill in evaluating available capabilities against desired effects in order to provide effective courses of action.</td>
</tr>
<tr>
<td>S0217</td>
<td>Skill in evaluating data sources for relevance, reliability, and objectivity.</td>
</tr>
<tr>
<td>S0218</td>
<td>Skill in evaluating information for reliability, validity, and relevance.</td>
</tr>
<tr>
<td>S0219</td>
<td>Skill in evaluating information to recognize relevance, priority, etc.</td>
</tr>
<tr>
<td>S0220</td>
<td>Skill in exploiting/querying organizational and/or partner collection databases.</td>
</tr>
<tr>
<td>S0221</td>
<td>Skill in extracting information from packet captures.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0222</td>
<td>Skill in fusion analysis</td>
</tr>
<tr>
<td>S0223</td>
<td>Skill in generating operation plans in support of mission and target requirements.</td>
</tr>
<tr>
<td>S0224</td>
<td>Skill in gisting target communications.</td>
</tr>
<tr>
<td>S0225</td>
<td>Skill in identifying a target’s communications networks.</td>
</tr>
<tr>
<td>S0226</td>
<td>Skill in identifying a target's network characteristics.</td>
</tr>
<tr>
<td>S0227</td>
<td>Skill in identifying alternative analytical interpretations in order to minimize unanticipated outcomes.</td>
</tr>
<tr>
<td>S0228</td>
<td>Skill in identifying critical target elements, to include critical target elements for the cyber domain.</td>
</tr>
<tr>
<td>S0229</td>
<td>Skill in identifying cyber threats which may jeopardize organization and/or partner interests.</td>
</tr>
<tr>
<td>S0230</td>
<td>Withdrawn – Integrated into S0066</td>
</tr>
<tr>
<td>S0231</td>
<td>Skill in identifying how a target communicates.</td>
</tr>
<tr>
<td>S0232</td>
<td>Skill in identifying intelligence gaps and limitations.</td>
</tr>
<tr>
<td>S0233</td>
<td>Skill in identifying language issues that may have an impact on organization objectives.</td>
</tr>
<tr>
<td>S0234</td>
<td>Skill in identifying leads for target development.</td>
</tr>
<tr>
<td>S0235</td>
<td>Skill in identifying non-target regional languages and dialects</td>
</tr>
<tr>
<td>S0236</td>
<td>Skill in identifying the devices that work at each level of protocol models.</td>
</tr>
<tr>
<td>S0237</td>
<td>Skill in identifying, locating, and tracking targets via geospatial analysis techniques</td>
</tr>
<tr>
<td>S0238</td>
<td>Skill in information prioritization as it relates to operations.</td>
</tr>
<tr>
<td>S0239</td>
<td>Skill in interpreting compiled and interpretive programming languages.</td>
</tr>
<tr>
<td>S0240</td>
<td>Skill in interpreting metadata and content as applied by collection systems.</td>
</tr>
<tr>
<td>S0241</td>
<td>Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.</td>
</tr>
<tr>
<td>S0242</td>
<td>Skill in interpreting vulnerability scanner results to identify vulnerabilities.</td>
</tr>
<tr>
<td>S0243</td>
<td>Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).</td>
</tr>
<tr>
<td>S0244</td>
<td>Skill in managing client relationships, including determining client needs/requirements,</td>
</tr>
<tr>
<td></td>
<td>managing client expectations, and demonstrating commitment to delivering quality results.</td>
</tr>
<tr>
<td>S0245</td>
<td>Skill in navigating network visualization software.</td>
</tr>
<tr>
<td>S0246</td>
<td>Skill in number normalization.</td>
</tr>
<tr>
<td>S0247</td>
<td>Skill in performing data fusion from existing intelligence for enabling new and continued collection.</td>
</tr>
<tr>
<td>S0248</td>
<td>Skill in performing target system analysis.</td>
</tr>
<tr>
<td>S0249</td>
<td>Skill in preparing and presenting briefings.</td>
</tr>
<tr>
<td>S0250</td>
<td>Skill in preparing plans and related correspondence.</td>
</tr>
<tr>
<td>S0251</td>
<td>Skill in prioritizing target language material.</td>
</tr>
<tr>
<td>S0252</td>
<td>Skill in processing collected data for follow-on analysis.</td>
</tr>
<tr>
<td>S0253</td>
<td>Skill in providing analysis on target-related matters (e.g., language, cultural, communications).</td>
</tr>
<tr>
<td>S0254</td>
<td>Skill in providing analysis to aid writing phased after action reports.</td>
</tr>
<tr>
<td>S0255</td>
<td>Skill in providing real-time, actionable geolocation information utilizing target infrastructures.</td>
</tr>
<tr>
<td>S0256</td>
<td>Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.</td>
</tr>
<tr>
<td>S0257</td>
<td>Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).</td>
</tr>
<tr>
<td>S0258</td>
<td>Skill in recognizing and interpreting malicious network activity in traffic.</td>
</tr>
<tr>
<td>S0259</td>
<td>Skill in recognizing denial and deception techniques of the target.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0260</td>
<td>Skill in recognizing midpoint opportunities and essential information.</td>
</tr>
<tr>
<td>S0261</td>
<td>Skill in recognizing relevance of information.</td>
</tr>
<tr>
<td>S0262</td>
<td>Skill in recognizing significant changes in a target’s communication patterns.</td>
</tr>
<tr>
<td>S0263</td>
<td>Skill in recognizing technical information that may be used for leads for metadata analysis.</td>
</tr>
<tr>
<td>S0264</td>
<td>Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).</td>
</tr>
<tr>
<td>S0265</td>
<td>Skill in recognizing technical information that may be used for target development including intelligence development.</td>
</tr>
<tr>
<td>S0266</td>
<td>Skill in relevant programming languages (e.g., C++, Python, etc.).</td>
</tr>
<tr>
<td>S0267</td>
<td>Skill in remote command line and Graphic User Interface (GUI) tool usage.</td>
</tr>
<tr>
<td>S0268</td>
<td>Skill in researching essential information.</td>
</tr>
<tr>
<td>S0269</td>
<td>Skill in researching vulnerabilities and exploits utilized in traffic.</td>
</tr>
<tr>
<td>S0270</td>
<td>Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.</td>
</tr>
<tr>
<td>S0271</td>
<td>Skill in reviewing and editing assessment products.</td>
</tr>
<tr>
<td>S0272</td>
<td>Skill in reviewing and editing intelligence products from various sources for cyber operations.</td>
</tr>
<tr>
<td>S0273</td>
<td>Skill in reviewing and editing plans.</td>
</tr>
<tr>
<td>S0274</td>
<td>Skill in reviewing and editing target materials.</td>
</tr>
<tr>
<td>S0275</td>
<td>Skill in server administration.</td>
</tr>
<tr>
<td>S0276</td>
<td>Skill in survey, collection, and analysis of wireless LAN metadata.</td>
</tr>
<tr>
<td>S0277</td>
<td>Skill in synthesizing, analyzing, and prioritizing meaning across data sets.</td>
</tr>
<tr>
<td>S0278</td>
<td>Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).</td>
</tr>
<tr>
<td>S0279</td>
<td>Skill in target development in direct support of collection operations.</td>
</tr>
<tr>
<td>S0280</td>
<td>Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).</td>
</tr>
<tr>
<td>S0281</td>
<td>Skill in technical writing.</td>
</tr>
<tr>
<td>S0282</td>
<td>Skill in testing and evaluating tools for implementation.</td>
</tr>
<tr>
<td>S0283</td>
<td>Skill in transcribing target language communications.</td>
</tr>
<tr>
<td>S0284</td>
<td>Skill in translating target graphic and/or voice language materials.</td>
</tr>
<tr>
<td>S0285</td>
<td>Skill in using Boolean operators to construct simple and complex queries.</td>
</tr>
<tr>
<td>S0286</td>
<td>Skill in using databases to identify target-relevant information.</td>
</tr>
<tr>
<td>S0287</td>
<td>Skill in using geospatial data and applying geospatial resources.</td>
</tr>
<tr>
<td>S0288</td>
<td>Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst’s Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).</td>
</tr>
<tr>
<td>S0289</td>
<td>Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.</td>
</tr>
<tr>
<td>S0290</td>
<td>Skill in using non-attributable networks.</td>
</tr>
<tr>
<td>S0291</td>
<td>Skill in using research methods including multiple, different sources to reconstruct a target network.</td>
</tr>
<tr>
<td>S0292</td>
<td>Skill in using targeting databases and software packages.</td>
</tr>
<tr>
<td>S0293</td>
<td>Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.</td>
</tr>
<tr>
<td>S0294</td>
<td>Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.</td>
</tr>
<tr>
<td>S0295</td>
<td>Skill in using various open source data collection tools (online trade, DNS, mail, etc.).</td>
</tr>
<tr>
<td>S0296</td>
<td>Skill in utilizing feedback in order to improve processes, products, and services.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0297</td>
<td>Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).</td>
</tr>
<tr>
<td>S0298</td>
<td>Skill in verifying the integrity of all files.</td>
</tr>
<tr>
<td>S0299</td>
<td>Skill in wireless network target analysis, templating, and geolocation.</td>
</tr>
<tr>
<td>S0300</td>
<td>Skill in writing (and submitting) requirements to meet gaps in technical capabilities.</td>
</tr>
<tr>
<td>S0301</td>
<td>Skill in writing about facts and ideas in a clear, convincing, and organized manner.</td>
</tr>
<tr>
<td>S0302</td>
<td>Skill in writing effectiveness reports.</td>
</tr>
<tr>
<td>S0303</td>
<td>Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.</td>
</tr>
<tr>
<td>S0304</td>
<td>Skill to access information on current assets available, usage.</td>
</tr>
<tr>
<td>S0305</td>
<td>Skill to access the databases where plans/directives/guidance are maintained.</td>
</tr>
<tr>
<td>S0306</td>
<td>Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.</td>
</tr>
<tr>
<td>S0307</td>
<td>Skill to analyze target or threat sources of strength and morale.</td>
</tr>
<tr>
<td>S0308</td>
<td>Skill to anticipate intelligence capability employment requirements.</td>
</tr>
<tr>
<td>S0309</td>
<td>Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.</td>
</tr>
<tr>
<td>S0310</td>
<td>Skill to apply analytical standards to evaluate intelligence products.</td>
</tr>
<tr>
<td>S0311</td>
<td>Skill to apply the capabilities, limitations and tasking methodologies of available platforms, sensors, architectures and apparatus as they apply to organization objectives.</td>
</tr>
<tr>
<td>S0312</td>
<td>Skill to apply the process used to assess the performance and impact of cyber operations.</td>
</tr>
<tr>
<td>S0313</td>
<td>Skill to articulate a needs statement/requirement and integrate new and emerging collection capabilities, accesses and/or processes into collection operations.</td>
</tr>
<tr>
<td>S0314</td>
<td>Skill to articulate intelligence capabilities available to support execution of the plan.</td>
</tr>
<tr>
<td>S0315</td>
<td>Skill to articulate the needs of joint planners to all-source analysts.</td>
</tr>
<tr>
<td>S0316</td>
<td>Skill to associate Intelligence gaps to priority information requirements and observables.</td>
</tr>
<tr>
<td>S0317</td>
<td>Skill to compare and contrast indicators/observables with requirements.</td>
</tr>
<tr>
<td>S0318</td>
<td>Skill to conceptualize the entirety of the intelligence process in the multiple domains and dimensions.</td>
</tr>
<tr>
<td>S0319</td>
<td>Skill to convert intelligence requirements into intelligence production tasks.</td>
</tr>
<tr>
<td>S0320</td>
<td>Skill to coordinate the development of tailored intelligence products.</td>
</tr>
<tr>
<td>S0321</td>
<td>Skill to correlate intelligence priorities to the allocation of intelligence resources/assets.</td>
</tr>
<tr>
<td>S0322</td>
<td>Skill to craft indicators of operational progress/success.</td>
</tr>
<tr>
<td>S0323</td>
<td>Skill to create and maintain up-to-date planning documents and tracking of services/production.</td>
</tr>
<tr>
<td>S0324</td>
<td>Skill to determine feasibility of collection.</td>
</tr>
<tr>
<td>S0325</td>
<td>Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.</td>
</tr>
<tr>
<td>S0326</td>
<td>Skill to distinguish between notional and actual resources and their applicability to the plan under development.</td>
</tr>
<tr>
<td>S0327</td>
<td>Skill to ensure that the collection strategy leverages all available resources.</td>
</tr>
<tr>
<td>S0328</td>
<td>Skill to evaluate factors of the operational environment to objectives, and information requirements.</td>
</tr>
<tr>
<td>S0329</td>
<td>Skill to evaluate requests for information to determine if response information exists.</td>
</tr>
<tr>
<td>S0330</td>
<td>Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.</td>
</tr>
<tr>
<td>S0331</td>
<td>Skill to express orally and in writing the relationship between intelligence capability limitations and decision making risk and impacts on the overall operation.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S0332</td>
<td>Skill to extract information from available tools and applications associated with collection requirements and collection operations management.</td>
</tr>
<tr>
<td>S0333</td>
<td>Skill to graphically depict decision support materials containing intelligence and partner capability estimates.</td>
</tr>
<tr>
<td>S0334</td>
<td>Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.</td>
</tr>
<tr>
<td>S0335</td>
<td>Skill to identify Intelligence gaps.</td>
</tr>
<tr>
<td>S0336</td>
<td>Skill to identify when priority information requirements are satisfied.</td>
</tr>
<tr>
<td>S0337</td>
<td>Skill to implement established procedures for evaluating collection management and operations activities.</td>
</tr>
<tr>
<td>S0338</td>
<td>Skill to interpret planning guidance to discern level of analytical support required.</td>
</tr>
<tr>
<td>S0339</td>
<td>Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.</td>
</tr>
<tr>
<td>S0340</td>
<td>Skill to monitor target or threat situation and environmental factors.</td>
</tr>
<tr>
<td>S0341</td>
<td>Skill to monitor threat effects to partner capabilities and maintain a running estimate.</td>
</tr>
<tr>
<td>S0342</td>
<td>Skill to optimize collection system performance through repeated adjustment, testing, and readjustment.</td>
</tr>
<tr>
<td>S0343</td>
<td>Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status.</td>
</tr>
<tr>
<td>S0344</td>
<td>Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.</td>
</tr>
<tr>
<td>S0345</td>
<td>Skill to relate intelligence resources/assets to anticipated intelligence requirements.</td>
</tr>
<tr>
<td>S0346</td>
<td>Skill to resolve conflicting collection requirements.</td>
</tr>
<tr>
<td>S0347</td>
<td>Skill to review performance specifications and historical information about collection assets.</td>
</tr>
<tr>
<td>S0348</td>
<td>Skill to specify collections and/or taskings that must be conducted in the near term.</td>
</tr>
<tr>
<td>S0349</td>
<td>Skill to synchronize operational assessment procedures with the critical information requirement process.</td>
</tr>
<tr>
<td>S0350</td>
<td>Skill to synchronize planning activities and required intelligence support.</td>
</tr>
<tr>
<td>S0351</td>
<td>Skill to translate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.</td>
</tr>
<tr>
<td>S0352</td>
<td>Skill to use collaborative tools and environments.</td>
</tr>
<tr>
<td>S0353</td>
<td>Skill to use systems and/or tools to track collection requirements and determine whether or not they are satisfied.</td>
</tr>
<tr>
<td>S0354</td>
<td>Skill in creating policies that reflect the business’s core privacy objectives.</td>
</tr>
<tr>
<td>S0355</td>
<td>Skill in negotiating vendor agreements and evaluating vendor privacy practices.</td>
</tr>
<tr>
<td>S0356</td>
<td>Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).</td>
</tr>
<tr>
<td>S0357</td>
<td>Skill to anticipate new security threats.</td>
</tr>
<tr>
<td>S0358</td>
<td>Skill to remain aware of evolving technical infrastructures.</td>
</tr>
<tr>
<td>S0359</td>
<td>Skill to use critical thinking to analyze organizational patterns and relationships.</td>
</tr>
</tbody>
</table>
A.7 NCWF Ability Descriptions

Table 8 provides a listing of specific abilities that might be demonstrated by a person in a given cybersecurity position. Selected ability descriptions from this list are included in the Detailed Work Role Listing in Appendix B. Because the list of abilities has evolved over many years and is expected to continue to do so, it is not sorted in a particular order and will simply continue to grow sequentially.

Table 8 - NCWF Ability Descriptions

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0001</td>
<td>Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.</td>
</tr>
<tr>
<td>A0002</td>
<td>Ability to match the appropriate knowledge repository technology for a given application or environment.</td>
</tr>
<tr>
<td>A0003</td>
<td>Ability to determine the validity of technology trend data.</td>
</tr>
<tr>
<td>A0004</td>
<td>Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.</td>
</tr>
<tr>
<td>A0005</td>
<td>Ability to decrypt digital data collections.</td>
</tr>
<tr>
<td>A0006</td>
<td>Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.</td>
</tr>
<tr>
<td>A0007</td>
<td>Ability to tailor code analysis for application-specific concerns.</td>
</tr>
<tr>
<td>A0008</td>
<td>Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).</td>
</tr>
<tr>
<td>A0009</td>
<td>Ability to apply supply chain risk management standards.</td>
</tr>
<tr>
<td>A0010</td>
<td>Ability to analyze malware.</td>
</tr>
<tr>
<td>A0011</td>
<td>Ability to answer questions in a clear and concise manner.</td>
</tr>
<tr>
<td>A0012</td>
<td>Ability to ask clarifying questions.</td>
</tr>
<tr>
<td>A0013</td>
<td>Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.</td>
</tr>
<tr>
<td>A0014</td>
<td>Ability to communicate effectively when writing.</td>
</tr>
<tr>
<td>A0015</td>
<td>Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.</td>
</tr>
<tr>
<td>A0016</td>
<td>Ability to facilitate small group discussions.</td>
</tr>
<tr>
<td>A0017</td>
<td>Ability to gauge learner understanding and knowledge level.</td>
</tr>
<tr>
<td>A0018</td>
<td>Ability to prepare and present briefings.</td>
</tr>
<tr>
<td>A0019</td>
<td>Ability to produce technical documentation.</td>
</tr>
<tr>
<td>A0020</td>
<td>Ability to provide effective feedback to students for improving learning.</td>
</tr>
<tr>
<td>A0021</td>
<td>Ability to use and understand complex mathematical concepts (e.g., discrete math).</td>
</tr>
<tr>
<td>A0022</td>
<td>Ability to apply principles of adult learning.</td>
</tr>
<tr>
<td>A0023</td>
<td>Ability to design valid and reliable assessments.</td>
</tr>
<tr>
<td>A0024</td>
<td>Ability to develop clear directions and instructional materials.</td>
</tr>
<tr>
<td>A0025</td>
<td>Ability to accurately define incidents, problems, and events in the trouble ticketing system.</td>
</tr>
<tr>
<td>A0026</td>
<td>Ability to analyze test data.</td>
</tr>
<tr>
<td>A0027</td>
<td>Ability to apply an organization's goals and objectives to develop and maintain architecture.</td>
</tr>
<tr>
<td>A0028</td>
<td>Ability to assess and forecast manpower requirements to meet organizational objectives.</td>
</tr>
<tr>
<td>A0029</td>
<td>Ability to build complex data structures and high-level programming languages.</td>
</tr>
<tr>
<td>A0030</td>
<td>Ability to collect, verify, and validate test data.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A0031</td>
<td>Ability to conduct and implement market research to understand government and industry capabilities and appropriate pricing.</td>
</tr>
<tr>
<td>A0032</td>
<td>Ability to develop curriculum for use within a virtual environment.</td>
</tr>
<tr>
<td>A0033</td>
<td>Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.</td>
</tr>
<tr>
<td>A0034</td>
<td>Ability to develop, update, and/or maintain standard operating procedures (SOPs).</td>
</tr>
<tr>
<td>A0035</td>
<td>Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.</td>
</tr>
<tr>
<td>A0036</td>
<td>Ability to identify basic common coding flaws at a high level.</td>
</tr>
<tr>
<td>A0037</td>
<td>Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.</td>
</tr>
<tr>
<td>A0038</td>
<td>Ability to optimize systems to meet enterprise performance requirements.</td>
</tr>
<tr>
<td>A0039</td>
<td>Ability to oversee the development and update of the lifecycle cost estimate.</td>
</tr>
<tr>
<td>A0040</td>
<td>Ability to translate data and test results into evaluative conclusions.</td>
</tr>
<tr>
<td>A0041</td>
<td>Ability to use data visualization tools (e.g., Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).</td>
</tr>
<tr>
<td>A0042</td>
<td>Ability to develop career path opportunities.</td>
</tr>
<tr>
<td>A0043</td>
<td>Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.</td>
</tr>
<tr>
<td>A0044</td>
<td>Ability to apply programming language structures (e.g., source code review) and logic.</td>
</tr>
<tr>
<td>A0045</td>
<td>Ability to evaluate/ensure the trustworthiness of the supplier and/or product.</td>
</tr>
<tr>
<td>A0046</td>
<td>Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.</td>
</tr>
<tr>
<td>A0047</td>
<td>Ability to develop secure software according to secure software deployment methodologies, tools, and practices.</td>
</tr>
<tr>
<td>A0048</td>
<td>Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</td>
</tr>
<tr>
<td>A0049</td>
<td>Ability to apply secure system design tools, methods and techniques.</td>
</tr>
<tr>
<td>A0050</td>
<td>Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.</td>
</tr>
<tr>
<td>A0051</td>
<td>Ability to execute technology integration processes.</td>
</tr>
<tr>
<td>A0052</td>
<td>Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.</td>
</tr>
<tr>
<td>A0053</td>
<td>Ability to determine the validity of workforce trend data.</td>
</tr>
<tr>
<td>A0054</td>
<td>Ability to apply the Instructional System Design (ISD) methodology.</td>
</tr>
<tr>
<td>A0055</td>
<td>Ability to operate common network tools (e.g., ping, traceroute, nslookup).</td>
</tr>
<tr>
<td>A0056</td>
<td>Ability to ensure security practices are followed throughout the acquisition process.</td>
</tr>
<tr>
<td>A0057</td>
<td>Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.</td>
</tr>
<tr>
<td>A0058</td>
<td>Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).</td>
</tr>
<tr>
<td>A0059</td>
<td>Ability to operate the organization's LAN/WAN pathways.</td>
</tr>
<tr>
<td>A0060</td>
<td>Ability to build architectures and frameworks.</td>
</tr>
<tr>
<td>A0061</td>
<td>Ability to design architectures and frameworks.</td>
</tr>
<tr>
<td>A0062</td>
<td>Ability to monitor measures or indicators of system performance and availability.</td>
</tr>
<tr>
<td>A0063</td>
<td>Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).</td>
</tr>
<tr>
<td>A0064</td>
<td>Ability to interpret and translate customer requirements into operational capabilities.</td>
</tr>
<tr>
<td>A0065</td>
<td>Ability to monitor traffic flows across the network.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>A0066</td>
<td>Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.</td>
</tr>
<tr>
<td>A0067</td>
<td>Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.</td>
</tr>
<tr>
<td>A0068</td>
<td>Ability to apply approved planning development and staffing processes.</td>
</tr>
<tr>
<td>A0069</td>
<td>Ability to apply collaborative skills and strategies.</td>
</tr>
<tr>
<td>A0070</td>
<td>Ability to apply critical reading/thinking skills.</td>
</tr>
<tr>
<td>A0071</td>
<td>Ability to apply language and cultural expertise to analysis.</td>
</tr>
<tr>
<td>A0072</td>
<td>Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.</td>
</tr>
<tr>
<td>A0073</td>
<td>Ability to clearly articulate intelligence requirements into well-formulated research questions and requests for information.</td>
</tr>
<tr>
<td>A0074</td>
<td>Ability to collaborate effectively with others.</td>
</tr>
<tr>
<td>A0075</td>
<td>Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.</td>
</tr>
<tr>
<td>A0076</td>
<td>Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development.</td>
</tr>
<tr>
<td>A0077</td>
<td>Ability to coordinate cyber operations with other organization functions or support activities.</td>
</tr>
<tr>
<td>A0078</td>
<td>Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations.</td>
</tr>
<tr>
<td>A0079</td>
<td>Ability to correctly employ each organization or element into the collection plan and matrix.</td>
</tr>
<tr>
<td>A0080</td>
<td>Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.</td>
</tr>
<tr>
<td>A0081</td>
<td>Ability to develop or recommend planning solutions to problems and situations for which no precedent exists.</td>
</tr>
<tr>
<td>A0082</td>
<td>Ability to effectively collaborate via virtual teams.</td>
</tr>
<tr>
<td>A0083</td>
<td>Ability to evaluate information for reliability, validity, and relevance.</td>
</tr>
<tr>
<td>A0084</td>
<td>Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.</td>
</tr>
<tr>
<td>A0085</td>
<td>Ability to exercise judgment when policies are not well-defined.</td>
</tr>
<tr>
<td>A0086</td>
<td>Ability to expand network access by conducting target analysis and collection in order to identify targets of interest.</td>
</tr>
<tr>
<td>A0087</td>
<td>Ability to focus research efforts to meet the customer’s decision-making needs.</td>
</tr>
<tr>
<td>A0088</td>
<td>Ability to function effectively in a dynamic, fast-paced environment.</td>
</tr>
<tr>
<td>A0089</td>
<td>Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.</td>
</tr>
<tr>
<td>A0090</td>
<td>Ability to identify external partners with common cyber operations interests.</td>
</tr>
<tr>
<td>A0091</td>
<td>Ability to identify intelligence gaps.</td>
</tr>
<tr>
<td>A0092</td>
<td>Ability to identify/describe target vulnerability.</td>
</tr>
<tr>
<td>A0093</td>
<td>Ability to identify/describe techniques/methods for conducting technical exploitation of the target.</td>
</tr>
<tr>
<td>A0094</td>
<td>Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.</td>
</tr>
<tr>
<td>A0095</td>
<td>Ability to interpret and translate customer requirements into operational action.</td>
</tr>
<tr>
<td>A0096</td>
<td>Ability to interpret and understand complex and rapidly evolving concepts.</td>
</tr>
<tr>
<td>A0097</td>
<td>Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>A0098</td>
<td>Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.</td>
</tr>
<tr>
<td>A0099</td>
<td>Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools.</td>
</tr>
<tr>
<td>A0100</td>
<td>Ability to perform wireless collection procedures to include decryption capabilities/tools.</td>
</tr>
<tr>
<td>A0101</td>
<td>Ability to recognize and mitigate cognitive biases which may affect analysis.</td>
</tr>
<tr>
<td>A0102</td>
<td>Ability to recognize and mitigate deception in reporting and analysis.</td>
</tr>
<tr>
<td>A0103</td>
<td>Ability to review processed target language materials for accuracy and completeness.</td>
</tr>
<tr>
<td>A0104</td>
<td>Ability to select the appropriate implant to achieve operational goals.</td>
</tr>
<tr>
<td>A0105</td>
<td>Ability to tailor technical and planning information to a customer’s level of understanding.</td>
</tr>
<tr>
<td>A0106</td>
<td>Ability to think critically.</td>
</tr>
<tr>
<td>A0107</td>
<td>Ability to think like threat actors.</td>
</tr>
<tr>
<td>A0108</td>
<td>Ability to understand objectives and effects.</td>
</tr>
<tr>
<td>A0109</td>
<td>Ability to utilize multiple intelligence sources across all intelligence disciplines.</td>
</tr>
<tr>
<td>A0110</td>
<td>Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.</td>
</tr>
<tr>
<td>A0111</td>
<td>Ability to work across departments and business units to implement organization’s privacy principles and programs, and align privacy objectives with security objectives.</td>
</tr>
<tr>
<td>A0112</td>
<td>Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.</td>
</tr>
<tr>
<td>A0113</td>
<td>Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.</td>
</tr>
<tr>
<td>A0114</td>
<td>Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.</td>
</tr>
<tr>
<td>A0115</td>
<td>Ability to work across departments and business units to implement organization’s privacy principles and programs, and align privacy objectives with security objectives.</td>
</tr>
<tr>
<td>A0116</td>
<td>Ability to prioritize and allocate cybersecurity resources correctly and efficiently.</td>
</tr>
<tr>
<td>A0117</td>
<td>Ability to relate strategy, business, and technology in the context of organizational dynamics.</td>
</tr>
<tr>
<td>A0118</td>
<td>Ability to understand technology, management, and leadership issues related to organization processes and problem solving.</td>
</tr>
<tr>
<td>A0119</td>
<td>Ability to understand the basic concepts and issues related to cyber and its organizational impact.</td>
</tr>
</tbody>
</table>
Appendix B—Work Role Detail Listing

The following section provides a detailed description of each NCWF Work Role. For each of the current Work Roles, as described in the NCWF, the listing below provides the following information:

- A unique NCWF Work Role ID, based upon the NCWF Category and Specialty Area to which that Work Role belongs;
- The Specialty Area supporting the Work Role;
- The formal Work Role name, followed by the OPM job code identifier in parentheses;
- A description of the Work Role;
- A list of the NCWF Tasks that a person in a cybersecurity position that includes the Work Role might be expected to perform;
- A list of the NCWF Knowledge areas that a person in a cybersecurity position that includes the Work Role might be expected to exhibit;
- A list of the NCWF Skills that a person in a cybersecurity position that includes the Work Role might be expected to possess; and,
- A list of the NCWF Abilities that a person in a cybersecurity position that includes the Work Role might be expected to demonstrate.

The following tables describe the NCWF Work Roles. As described in Section 4, this listing will be updated periodically based upon industry feedback and changes to the cybersecurity landscape.

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role Name</th>
<th>Work Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-RM-001</td>
<td>Securely Provision (SP)</td>
<td>Risk Management (RM)</td>
<td>Authorizing Official (611)</td>
<td>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 (CNSSI 4009).</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0145, T0221, T0371, T0495</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0084, K0085, K0089, K0101, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0295, K0322, K0342</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills</td>
<td>S0034</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Role ID</td>
<td>SP-RM-001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Risk Management (RM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Authorizing Official (611)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Role Description</td>
<td>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 (CNSSI 4009).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasks</td>
<td>T0145, T0221, T0371, T0495</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0084, K0085, K0089, K0101, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills</td>
<td>S0034</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-RM-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Risk Management (RM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Security Control Assessor (612)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST 800-37).</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0032, T0072, T0079, T0083, T0141, T0150, T0183, T0184, T0197, T0218, T0221, T0244, T0245, T0251, T0301</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0084, K0085, K0089, K0101, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342</td>
</tr>
<tr>
<td>Skills</td>
<td>S0001, S0006, S0027, S0034, S0038, S0086</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-DEV-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Software Development (DEV)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Software Developer (621)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554</td>
</tr>
<tr>
<td>Skills</td>
<td>S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0007, A0021, A0047</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-DEV-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Software Development (DEV)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Secure Software Assessor (622)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554</td>
</tr>
</tbody>
</table>


| Skills | S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175 |

| Abilities | A0021 |

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-ARC-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Architecture (ARC)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Enterprise Architect (651)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557</td>
</tr>
</tbody>
</table>


| Skills | S0005, S0024, S0050, S0060, S0099, S0122 |

| Abilities | A0008, A0015, A0027, A0038, A0051, A0060 |

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-ARC-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Architecture (ARC)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Security Architect (652)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>SP-RD-001</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Technology R&amp;D (RD)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Research and Development Specialist (661)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547</td>
</tr>
<tr>
<td>Skills</td>
<td>S0005, S0024, S0027, S0050, S0060, S0099, S0116, S0122, S0139, S0152, S0168</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0008, A0015, A0027, A0038, A0048, A0049, A0050, A0061</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-RP-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Requirements Planning (RP)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Systems Requirements Planner (641)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497</td>
</tr>
<tr>
<td>Skills</td>
<td>S0005, S0006, S0008, S0010, S0050, S0134</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0064</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-TE-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Test and Evaluation (TE)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>System Test &amp; Evaluation Specialist (671)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0058, T0080, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>SP-SYS-001</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Development (SYS)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Information Systems Security Developer (631)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544</td>
</tr>
<tr>
<td>Skills</td>
<td>S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>SP-SYS-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Securely Provision (SP)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Development (SYS)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Systems Developer (632)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0012, T0021, T0053, T0056, T0061, T0067, T0070, T0107, T0109, T0119, T0181, T0201, T0205, T0228, T0242, T0304, T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560</td>
</tr>
<tr>
<td>Skills</td>
<td>S0018, S0022, S0023, S0024, S0031, S0034, S0036, S0060, S0085, S0097, S0098, S0136, S0145, S0146, S0160</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OM-DA-001</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Data Administration (DA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Database Administrator (421)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Administers databases and/or data management systems that allow for the storage, query, and utilization of data.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0260, K0261, K0262, K0277, K0278, K0279, K0287, K0420</td>
</tr>
<tr>
<td>Skills</td>
<td>S0002, S0013, S0037, S0042, S0045</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OM-DA-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Data Administration (DA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Data Analyst (422)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0328, K0420</td>
</tr>
<tr>
<td>Skills</td>
<td>S0013, S0017, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0105, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0029, A0035, A0036, A0041, A0066</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OM-KM-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Knowledge Management (KM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Knowledge Manager (431)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420</td>
</tr>
<tr>
<td>Skills</td>
<td>S0011, S0012, S0049, S0055</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0002</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OM-TS-001</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Customer Service and Technical Support (TS)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Technical Support Specialist (411)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0114, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0306, K0317, K0330</td>
</tr>
<tr>
<td>Skills</td>
<td>S0039, S0058, S0142, S0159</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0025, A0034</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OM-NET-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Network Services (NET)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Network Operations Specialist (441)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Plans, implements, and operates network services/systems, to include hardware and virtual environments.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232</td>
</tr>
<tr>
<td>Skills</td>
<td>S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0052, A0055, A0058, A0059, A0062, A0063, A0065</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OM-SA-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Administration (SA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>System Administrator (451)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0181, K0260, K0261, K0262, K0280, K0289, K0318, K0327, K0331, K0346</td>
</tr>
<tr>
<td>Skills</td>
<td>S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OM-AN-001</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Category</td>
<td>Operate and Maintain (OM)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Systems Analysis (AN)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Systems Security Analyst (461)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0015, T0016, T0017, T0085, T0086, T0088, T0123, T0128, T0169, T0177, T0187, T0194, T0202, T0205, T0243, T0309, T0344, T0462, T0469, T0470, T0475, T0477, T0485, T0489, T0492, T0499, T0504, T0508, T0526, T0545, T0548</td>
</tr>
<tr>
<td>Skills</td>
<td>S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0015</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-LG-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Legal Advice and Advocacy (LG)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Legal Advisor (731)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Provides legal advice and recommendations on relevant topics related to cyber law.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0312, K0316, K0341</td>
</tr>
<tr>
<td>Skills</td>
<td>[None specified]</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0046</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-LG-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Legal Advice and Advocacy (LG)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Privacy Compliance Manager (732)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0003, T0004, T0032, T0066, T0098, T0099, T0131, T0133, T0188, T0381, T0384, T0478, T0861, T0862, T0863, T0864, T0865, T0866, T0867, T0868, T0869, T0870, T0871, T0872, T0873, T0874, T0875, T0876, T0877, T0878, T0879, T0880, T0881, T0882, T0883, T0884, T0885, T0886, T0887, T0888, T0889, T0890, T0891, T0892, T0893, T0894, T0895, T0896, T0897, T0898, T0899, T0900, T0901, T0902, T0903, T0904, T0905, T0906, T0907, T0908, T0909, T0910, T0911, T0912, T0913, T0914, T0915, T0916, T0917, T0918, T0919</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0606, K0607, K0608, K0609, K0610, K0611, K0612, K0613, K0614</td>
</tr>
<tr>
<td>Skills</td>
<td>S0354, S0355, S0356</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OV-ED-001</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Training, Education, and Awareness (ED)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Instructional Curriculum Developer (711)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0230, T0247, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0534, T0536, T0926</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0239, K0245, K0246, K0252, K0287</td>
</tr>
<tr>
<td>Skills</td>
<td>S0064, S0066, S0070, S0102, S0166</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0004, A0032, A0054</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-ED-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Training, Education, and Awareness (ED)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Instructor (712)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops and conducts training or education of personnel within cyber domain.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0443, T0444, T0450, T0467, T0519, T0520, T0535, T0536, T0926</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0287, K0319</td>
</tr>
<tr>
<td>Skills</td>
<td>S0064, S0070, S0100, S0101</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0006, A0011, A0012, A0013, A0014, A0016, A0017, A0020, A0022, A0023, A0024, A0057</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-MG-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cybersecurity Management (MG)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Information Systems Security Manager (722)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Responsible for the cybersecurity of a program, organization, system, or enclave.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OV-MG-002</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cybersecurity Management (MG)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>COMSEC Manager (723)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0287</td>
</tr>
<tr>
<td>Skills</td>
<td>S0027</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-PL-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Strategic Planning and Policy (PL)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Workforce Developer and Manager (751)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0074, T0094, T0116, T0222, T0226, T0341, T0355, T0356, T0362, T0363, T0364, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0537, T0552</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0166, K0168, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335</td>
</tr>
<tr>
<td>Skills</td>
<td>S0108, S0128</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-PL-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Strategic Planning and Policy Development</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Policy and Strategy Planner (752)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0166, K0234, K0248, K0309, K0311, K0313, K0335</td>
</tr>
<tr>
<td>Skills</td>
<td>[None specified]</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0003, A0033, A0037, A0042, A0053</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-EX-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Executive Cyber Leadership (EX)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Executive Cyber Leadership (901)</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OV-PM-001</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Acquisition and Program/Project Management (PM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Program Manager (801)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0066, T0072, T0174, T0199, T0200, T0270, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0009, K0010, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0910, K0120, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270</td>
</tr>
<tr>
<td>Skills</td>
<td>S0038</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0009, A0039, A0045, A0056,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-PM-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Acquisition and Program/Project Management (PM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Information Technology (IT) Project Manager (802)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Directly manages information technology projects to provide a unique service or product.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0059, K0072, K0090, K0910, K0120, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270</td>
</tr>
<tr>
<td>Skills</td>
<td>S0038</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0009, A0039, A0045, A0056,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-PM-003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Acquisition and Program/Project Management (PM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Product Support Manager (803)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0551, T0553</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>OV-PM-004</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Acquisition and Program/Project Management (PM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>IT Investment/Portfolio Manager (804)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0059, K0072, K0090, K0120, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270</td>
</tr>
<tr>
<td>Skills</td>
<td>[None specified]</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0009, A0031, A0039, A0045, A0056</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>OV-PM-005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Oversee and Govern (OV)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Acquisition and Program/Project Management (PM)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>IT Program Auditor (805)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270</td>
</tr>
<tr>
<td>Skills</td>
<td>S0038, S0085</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0056</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>PR-DA-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Protect and Defend (PR)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cyber Defense Analysis (DA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Defense Analyst (511)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>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.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>PR-INF-001</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Category</td>
<td>Protect and Defend (PR)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cyber Defense Infrastructure Support (INF)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Defense Infrastructure Support Specialist (521)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0331, K0334, K0340</td>
</tr>
<tr>
<td>Skills</td>
<td>S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>PR-IR-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Protect and Defend (PR)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Incident Response (IR)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Defense Incident Responder (531)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0041, T0047, T0161, T0163, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0333, T0395, T0503, T0510</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0225, K0230, K0259, K0287, K0332</td>
</tr>
<tr>
<td>Skills</td>
<td>S0003, S0047, S0077, S0078, S0079, S0080, S0173</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>PR-VA-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Protect and Defend (PR)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Vulnerability Assessment and Management (VA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Vulnerability Assessment Analyst (541)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Performs assessments of systems and networks within the NE 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.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0085, K0089, K0106, K0139, K0161, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0331, K0342, K0344, K0345</td>
</tr>
<tr>
<td>Skills</td>
<td>S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0001, A0044</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>AN-TA-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Analyze (AN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Threat Analysis (TA)</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Warning Analyst (141)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>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.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0173, K0348, K0349, K0362, K0369, K0370, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614</td>
</tr>
<tr>
<td>Skills</td>
<td>S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0066, A0072, A0075, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>AN-XA-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Analyze (AN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Exploitation Analysis (XA)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Exploitation Analyst (121)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777</td>
</tr>
<tr>
<td>Skills</td>
<td>S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0066, A0075, A0080, A0084, A0074, A0086, A0092, A0093, A0104</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>AN-AN-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Analyze (AN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>All-Source Analysis (AN)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>All-Source Analyst (111)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>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.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834</td>
</tr>
<tr>
<td>Skills</td>
<td>S0194, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254</td>
</tr>
</tbody>
</table>

| Work Role ID | AN-AN-002 |
| Category | Analyze (AN) |
| Specialty Area | All-Source Analysis (AN) |
| Work Role Name | Mission Assessment Specialist (112) |
| Work Role Description | Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness. |
| Tasks | T0582, T0583, T0585, T0586, T0588, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834 |
| Skills | S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303 |

| Work Role ID | AN-TD-001 |
| Category | Analyze (AN) |
| Specialty Area | Targets (TD) |
| Work Role Name | Target Developer (131) |
| Work Role Description | Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation. |
| Tasks | T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835 |
### Work Role ID AN-0102
### Category Analyze (AN)
### Specialty Area Targets (TD)
### Work Role Name Target Network Analyst (132)
### Work Role Description Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.
### Tasks T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807
### Skills S0194, S0203, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302
### Abilities A0066, A0075, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

---

### Work Role ID AN-0101
### Category Analyze (AN)
### Specialty Area Language Analysis (LA)
### Work Role Name Multi-Disciplined Language Analyst (151)
### Work Role Description Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
### Tasks T0650, T0606, T0715, T0745, T0761, T0837, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, T0860
### Skills S0194, S0203, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302
### Abilities A0066, A0075, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073
| Knowledge | K0001, K0002, K0003, K0004, K0005, K0006, K0173, K0348, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0434, K0356, K0359, K0367, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607 |
| Skills | S0187, S0217, S0244, S0259, S0262, S0277, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284 |
| Abilities | A0075, A0089, A0071, A0103 |

Work Role ID | CO-CL-001
Category | Collect and Operate (CO)
Specialty Area | Collection Operations (CL)
Work Role Name | All Source-Collection Manager (311)
Work Role Description | Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Tasks | T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827

| Skills | S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352 |
| Abilities | A0069, A0070, A0076, A0078, A0079 |

Work Role ID | CO-CL-002
Category | Collect and Operate (CO)
Specialty Area | Collection Operations (CL)
Work Role Name | All Source-Collection Requirements Manager (312)
Work Role Description | Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Tasks | T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0745, T0780, T0819, T0822, T0830, T0831, T0832, T0833 |
### Work Role ID: CO-PL-001

**Category:** Collect and Operate (CO)  
**Specialty Area:** Cyber Operational Planning (PL)  
**Work Role Name:** Cyber Intel Planner (331)

**Work Role Description:** 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 in cyberspace.

**Tasks:** T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836

**Knowledge**

**Skills**
- S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329, S0337, S0346, S0348, S0353

**Abilities**
- A0069, A0070, A0078

---

### Work Role ID: CO-PL-002

**Category:** Collect and Operate (CO)  
**Specialty Area:** Cyber Operational Planning (PL)  
**Work Role Name:** Cyber Ops Planner (332)

**Work Role Description:** 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.

**Tasks:**

| Skills | S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350 |
| Abilities | A0066, A0070, A0075, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105 |
### Work Role ID

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>CO-PL-003</th>
</tr>
</thead>
</table>

### Category

Collect and Operate (CO)

### Specialty Area

Cyber Operational Planning (PL)

### Work Role Name

Partner Integration Planner (333)

### Work Role Description

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.

### Tasks

- T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823

### Knowledge


### Skills

- S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349

### Abilities

- A0066, A0070, A0075, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

---

### Work Role ID

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>CO-OP-001</th>
</tr>
</thead>
</table>

### Category

Collect and Operate (CO)

### Specialty Area

Cyber Operations (OP)

### Work Role Name

Cyber Operator (321)

### Work Role Description

Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

### Tasks

- T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829

### Knowledge


### Skills

- S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349

### Abilities

- A0066, A0070, A0075, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105
<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>IN-CI-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Investigate (IN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cyber Investigation</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Crime Investigator (221)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.</td>
</tr>
<tr>
<td>Tasks</td>
<td>[Note: Several of these activities may only to be conducted by personnel with a Law Enforcement or Counter Intelligence Authority.]</td>
</tr>
<tr>
<td>T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523</td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0014, K0017, K0021, K0025, K0027, K0029, K0031, K0033, K0035, K0037, K0039, K0041, K0043, K0045, K0047, K0049, K0051, K0053, K0055, K0057, K0061, K0063, K0065, K0067, K0069, K0071, K0073, K0075, K0077, K0079, K0081, K0083, K0085, K0087, K0089, K0091, K0093</td>
</tr>
<tr>
<td>Skills</td>
<td>S0047, S0068, S0072, S0086, S0165</td>
</tr>
<tr>
<td>Abilities</td>
<td>[None specified]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Role ID</th>
<th>IN-FO-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Investigate (IN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Digital Forensics (FO)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Forensics Analyst (211)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0067, T0076, T0096, T0115, T0146, T0484, T0220, T0235, T0273, T0297, T0398, T0401, T0403, T0411, T0425, T0421, T0424, T0440, T0482, T0490, T0507, T0274, T0059, T0541, T0558, T0078, T0427, T0402, T0419, T0420, T0542, T0308, T0447</td>
</tr>
<tr>
<td>Skills</td>
<td>S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0093, S0095</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0005</td>
</tr>
<tr>
<td>Work Role ID</td>
<td>IN-FO-002</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Category</td>
<td>Investigate (IN)</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Digital Forensics (FO)</td>
</tr>
<tr>
<td>Work Role Name</td>
<td>Cyber Defense Forensics Analyst (212)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0543, T0546</td>
</tr>
<tr>
<td>Knowledge</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0099, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347</td>
</tr>
<tr>
<td>Skills</td>
<td>S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133</td>
</tr>
<tr>
<td>Abilities</td>
<td>A0005, A0043</td>
</tr>
</tbody>
</table>
Appendix C—Acronyms

Selected acronyms and abbreviations used in this paper are defined below:

API          Application programming interface  
CAE          Centers of Academic Excellence  
CDS          Cross-Domain Solutions  
CIO          Chief Information Officer  
CMMI         Capability Maturity Model Integration  
CNSSI        Committee on National Security Systems Instruction  
COMSEC       Communications Security  
COTR         Contracting Officer's Technical Representative  
CSF          Cybersecurity Framework  
CSIP         Cybersecurity Strategy and Implementation Plan  
DNS          Domain Name System  
EISA         Enterprise information security architecture  
FISMA        Federal Information Security Modernization Act  
FOIA         Freedom of Information Act  
HR           Human Resource  
IDS          Intrusion detection system  
IP           Internet Protocol  
IPS          Intrusion Prevention System  
IR           Incident Response  
IRT          Incident Response Teams  
ISD          Instructional System Design  
ITL          Information Technology Laboratory  
KSA          Knowledge, skills, and abilities  
LAN          Local area network  
NCWF         National Cybersecurity Workforce Framework  
NICE         National Initiative for Cybersecurity Education  
OLA          Operating-Level Agreement  
OMB          Office of Management and Budget  
OPM          Office of Personnel Management  
OS           Operating system  
OSI          Open System Interconnection  
P.L.         Public Law  
PCI          Payment Card Industry  
PHI          Personal Health Information  
PIA          Privacy Impact Assessments  
PII          Personally Identifiable Information  
PKI          Public key infrastructure  
R&D          Research and Design  
RFID         Radio Frequency Identification  
RMF          Risk Management Framework  
SA&A         Security Assessment and Authorization  
SDLC         System development life cycle  
SLA          Service-Level Agreements
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOP</td>
<td>Standard operating procedures</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured query language</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TTP</td>
<td>Tactics, techniques, and procedures</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
</tbody>
</table>
Appendix D—References


