NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

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

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William 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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

August 2017

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

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

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
Natl. Inst. Stand. Technol. Spec. Publ. 800-181, 144 pages (August 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

Certain commercial entities, equipment, or materials may be identified in this document 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.

Comments on this publication may be submitted to:

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

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at 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 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.

Keywords

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

Revisions

Please visit the NICE Framework revisions website [1] to determine if there have been any updates to the NICE Framework.

Supplemental Content

A Reference Spreadsheet for the NICE Framework is available at https://www.nist.gov/file/372581.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

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 NIST. We wish to thank Tanya Brewer, Dean Bushmiller, Lynne Clarke, Jerri Damavandy, Lisa Dorr, Ryan Farr, Jim Foti, Jodi Guss, Keith Hall, Chris Kelsall, Elizabeth Lennon, Jeff Marron, Joshua Musicante, Stephen Olechnowicz, Lori Pfannenstein, Chuck Romine, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matthew Smith, Kevin Stine, Bluma Sussman, Caroline Tan, Baris Yakin, and Clarence Williams for their individual contributions to this publication.

The first NICE Framework was posted for public comment in September 2012 and published as final in April 2013 as the National Cybersecurity Workforce Framework version 1.0 [2]. The authors recognize Dr. Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich, and Peggy Maxson for leading its development, along with Montana Williams and Roy Burgess for their leadership in the development of National Cybersecurity Workforce Framework version 2.0 which was posted in April 2014 [3].

Finally, the authors respectfully acknowledge the seminal work in computer security that dates 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.

Trademark Information

All trademarks or registered trademarks belong to their respective organizations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Executive Summary

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) of 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 and prepared to protect our nation from existing and emerging cybersecurity challenges. NICE promotes nationwide initiatives that increase the number of people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work.

As threats that exploit vulnerabilities in our cyberinfrastructure grow and evolve, an integrated cybersecurity workforce must be capable of designing, developing, implementing, and maintaining defensive and offensive cyber strategies. An integrated cybersecurity workforce includes technical and nontechnical roles that are staffed with knowledgeable and experienced people. An integrated cybersecurity workforce can address the cybersecurity challenges inherent to preparing their organizations to successfully implement aspects of their missions and business processes connected to cyberspace.

This publication provides a fundamental reference in support of a workforce capable of meeting an organization's cybersecurity needs by using a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role. It provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

A user of the NICE Framework will reference it for different aspects of workforce development, education, and/or training purposes, and when that material is used at organizational levels, the user should customize what is pulled from the NICE Framework to standards, regulations, needs, and mission of the user's organization. The NICE Framework is a reference starting point for the content of guidance and guidelines on career paths, education, training, and credentialing programs.

The NICE Framework is a resource that will strengthen an organization's ability to communicate consistently and clearly about cybersecurity work and its cybersecurity workforce. Organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

An online reference spreadsheet tool [4] is available on the NICE Framework website [5].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Table of Contents

Executive Summary ..... **iv**
1 Introduction **1**
1.1 NICE Framework Background 1
1.2 Purpose and Applicability 2
1.3 Audience/Users 2
1.3.1 Employers 2
1.3.2 Current and Future Cybersecurity Workers 3
1.3.3 Educators/Trainers 3
1.3.4 Technology Providers 4
1.4 Organization of this Special Publication 4
2 NICE Framework Components and Relationships **5**
2.1 Components of the NICE Framework 5
2.1.1 Categories 5
2.1.2 Specialty Areas 5
2.1.3 Work Roles 5
2.1.4 Knowledge, Skills, and Abilities (KSAs) 5
2.1.5 Tasks 6
2.2 NICE Framework Component Relationships 6
3 Using the NICE Framework **7**
3.1 Identification of Cybersecurity Workforce Needs 7
3.2 Recruitment and Hiring of Highly Skilled Cybersecurity Talent 8
3.3 Education and Training of Cybersecurity Workforce Members 8
3.4 Retention and Development of Highly Skilled Cybersecurity Talent 8
4 Extensions **10**
4.1 Competencies 10
4.2 Job Titles 10
4.3 Cybersecurity Guidance and Guideline documents 10

List of Appendices

Appendix A – Listing of NICE Framework Elements **11**
A.1 NICE Framework Workforce Categories 11
A.2 NICE Framework Specialty Areas 12

A.3 NICE Framework Work Roles 15
A.4 NICE Framework Tasks 24
A.5 NICE Framework Knowledge Descriptions 59
A.6 NICE Framework Skills Descriptions 77
A.7 NICE Framework Ability Descriptions 88
Appendix B – Work Role Detail Listing 95
B.1 Securely Provision (SP) 95
B.2 Operate and Maintain (OM) 101
B.3 Oversee and Govern (OV) 104
B.4 Protect and Defend (PR) 110
B.5 Analyze (AN) 112
B.6 Collect and Operate (CO) 116
B.7 Investigate (IN) 121
Appendix C – Workforce Development Tools 123
C.1 DHS Cybersecurity Workforce Development Toolkit 123
C.1.1 Proficiency Levels and Career Paths 123
C.2 Baldrige Cybersecurity Excellence Builder Tool 123
C.3 Position Description Drafting Tool 124
Appendix D – Cross Reference to Guidance and Guideline Documents 125
D.1 Cybersecurity Framework 125
D.1.2 Example Integration of Cybersecurity Framework with NICE Framework 127
D.2 Systems Security Engineering 129
D.3 U.S. Office of Personnel Management Federal Cybersecurity Codes 130
Appendix E – Acronyms 132
Appendix F – References 134

List of Tables

Table 1 - NICE Framework Workforce Categories 11
Table 2 - NICE Framework Specialty Areas 12
Table 3 - NICE Framework Work Roles 16
Table 4 - NICE Framework Tasks 24
Table 5 - NICE Framework Knowledge Descriptions 59

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Table 6 - NICE Framework Skills Descriptions 77
Table 7 - NICE Framework Ability Descriptions 88
Table 8 - Crosswalk of NICE Framework Workforce Categories to Cybersecurity Framework Functions 127
Table 9 – Crosswalk of Work Role IDs to OPM Cybersecurity Codes 131

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

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 that seeks 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 and economically competitive.

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.

Throughout this document, the combined terms “cybersecurity workforce” is shorthand for a workforce with work roles that have an impact on an organization’s ability to protect its data, systems, and operations. Included are new work roles that have been known traditionally as information technology (IT) security roles. Those roles have been added to this workforce framework to highlight their importance to the overall cybersecurity posture of an organization. Additionally, some of the work roles described herein include the shorter term *cyber* to be inclusive of sectors where cyber has become the conversational norm for this field.

A cybersecurity workforce includes not only technically focused staff, but also those who apply knowledge of cybersecurity when preparing their organization to successfully implement its mission. A knowledgeable and skilled cybersecurity workforce is needed to address cybersecurity risks within an organization’s overall risk management process.

1.1 NICE Framework Background

The concept for the NICE Framework began before the establishment of NICE in 2010 and grew out of the recognition that the cybersecurity workforce had not been defined and assessed. To address this challenge, the Federal Chief Information Officers (CIO) Council took on the task in 2008 to provide a standard framework to understand the cybersecurity roles within the federal government. Input from focus groups with subject matter experts from numerous federal agencies helped the Federal CIO Council produce a research report that referenced where other information technology professional development efforts were already under way, and thirteen specific roles were identified as needed by agencies to conduct cybersecurity work.

Building on this inherently multidisciplinary exploration of the “field” of cybersecurity, the Comprehensive National Cybersecurity Initiative’s included a focus on workforce that tasked several agencies to work together to develop a cybersecurity workforce framework. The first draft was posted for public comment in September 2011. Comments were incorporated into version 1.0 [2].

A subsequent U.S. government-wide review noted specific areas to be further examined and refined. The Department of Homeland Security (DHS) gathered input and validated final

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

recommendations via focus groups with subject matter experts from around the country and across industry, academia, and government resulting in a second version of the NICE Framework, version 2.0 [3], shared publicly in 2014.

The Office of the Secretary of Defense (OSD) expanded on version 2.0 through internal engagements with service components and external engagements with the private sector. The DHS and NIST co-authors worked with OSD to refine their expansion to become this publication with a goal to emphasize private sector applicability and to reinforce the vision that the NICE Framework is a reference resource for both the public and private sectors.

1.2 Purpose and Applicability

This publication serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work.

Using the NICE Framework as a fundamental reference will improve the communication needed to identify, recruit, and develop cybersecurity talent. The NICE Framework will allow employers to use focused, consistent language in professional development programs, in their use of industry certifications and academic credentials, and in their selection of relevant training opportunities for their workforce.

The NICE Framework 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 NICE Framework offers the ability to describe all cybersecurity work. An applicability goal of the NICE Framework is that any cybersecurity job or position can be described by identifying the relevant material from one or more components of the NICE Framework. For each job or position, the context of the mission or business processes and priorities will drive which material is selected from the NICE Framework.

Organizations or sectors can use the NICE Framework to develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1.3 Audience/Users

The NICE Framework can be viewed as a non-prescriptive cybersecurity workforce dictionary. Users of the NICE Framework who reference it should implement it locally for different workforce development, education, or training purposes.

1.3.1 Employers

Use of the NICE Framework's common lexicon enables employers to inventory and develop their cybersecurity workforce. The NICE Framework can be used by employers and organizational leadership to:

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

- 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 selecting relevant KSAs and Tasks, once work roles and tasks are identified;
- Identify the most relevant work roles and develop career paths to guide staff in gaining the requisite skills for those roles; and
- Establish a shared terminology between hiring managers and human resources (HR) staff for the recruiting, retention, and training of a highly-specialized workforce.

1.3.2 Current and Future Cybersecurity Workers

The NICE Framework 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 human resource 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 NICE Framework's common lexicon to provide clear and consistent descriptions of the cybersecurity tasks and training that are needed for those positions.

When training providers and industry certification providers use the common lexicon of the NICE Framework, those in the cybersecurity field, or those who might wish to enter the cybersecurity field, can find training and/or certification providers that can teach 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 to find 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 NICE Framework provides a reference for educators to develop curriculum, certificate or degree programs, training programs, courses, seminars, and exercises or challenges that cover the KSAs and Tasks described in the NICE Framework.

Human resource staffing specialists and guidance counselors can use the NICE Framework as a resource for career exploration.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

1.3.4 Technology Providers

The NICE Framework allows a technology provider to identify the cybersecurity work roles and the KSAs and Tasks associated with hardware and software products and services they provide. A technology provider can then create appropriate support materials to assist members of the cybersecurity workforce in the proper configuration and management of their products.

1.4 Organization of this Special Publication

The remainder of this special publication is organized as follows:

- Chapter 2 defines the components of the NICE Framework: (i) Categories; (ii) Specialty Areas; (iii) Work Roles; (iv) associated supersets of Knowledge, Skills, and Abilities; and (v) Tasks for each work role.
- Chapter 3 describes using the NICE Framework
- Chapter 4 notes areas where other publications, guidelines, guidance, and tools can expand the impact of the NICE Framework.
- Appendix A describes the NICE Framework list of Categories, Specialty Areas, Work Roles, KSAs, and Tasks.
- Appendix B provides a detailed listing of each work role, including the associated KSAs and Tasks.
- Appendix C provides some examples of workforce development tools
- Appendix D provides some examples of guidance or guideline documents that cross reference some of the content of those documents to components in the NICE Framework
- Appendix E gives selected acronyms and abbreviations used in this document.
- Appendix F gives references cited in this document.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

2 NICE Framework Components and Relationships

2.1 Components of the NICE Framework

The NICE Framework organizes cybersecurity and related work. This section introduces and defines the core components of the NICE Framework in support of those areas.

2.1.1 Categories

Categories provide the overarching organizational structure of the NICE Framework. There are seven Categories and all are composed of Specialty Areas and work roles. This organizational structure is based on extensive job analyses, which group 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 National Cybersecurity Workforce Framework version 1.0 [2] and 32 in National Cybersecurity Workforce Framework version 2.0 [3]. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work. In previous versions of the NICE Framework, tasks and KSAs were associated with each specialty area. KSAs and Tasks are now associated with the work roles.

2.1.3 Work Roles

Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.

Work being performed in a job or position is described by selecting one or more work roles from the NICE Framework 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 shown in Appendix A.

2.1.4 Knowledge, Skills, and Abilities (KSAs)

Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.

> **Knowledge** is a body of information applied directly to the performance of a function.
>
> **Skill** is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes,

and controls that have an impact on the cybersecurity posture of an organization or individual.

Ability is competence to perform an observable behavior or a behavior that results in an observable product.

2.1.5 Tasks

A Task is a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.

2.2 NICE Framework Component Relationships

The NICE Framework components describe cybersecurity work. As illustrated in Figure 1, each Category is composed of Specialty Areas, each of which is composed of one or more work roles. Each work role, in turn, includes KSAs and Tasks.

Grouping components in this manner simplifies communication about cybersecurity workforce topics, and helps with alignment to other frameworks. Specific associations of work roles to KSAs and Tasks are shown in Appendix B and in a reference spreadsheet [4] posted to the NICE Framework website [5].

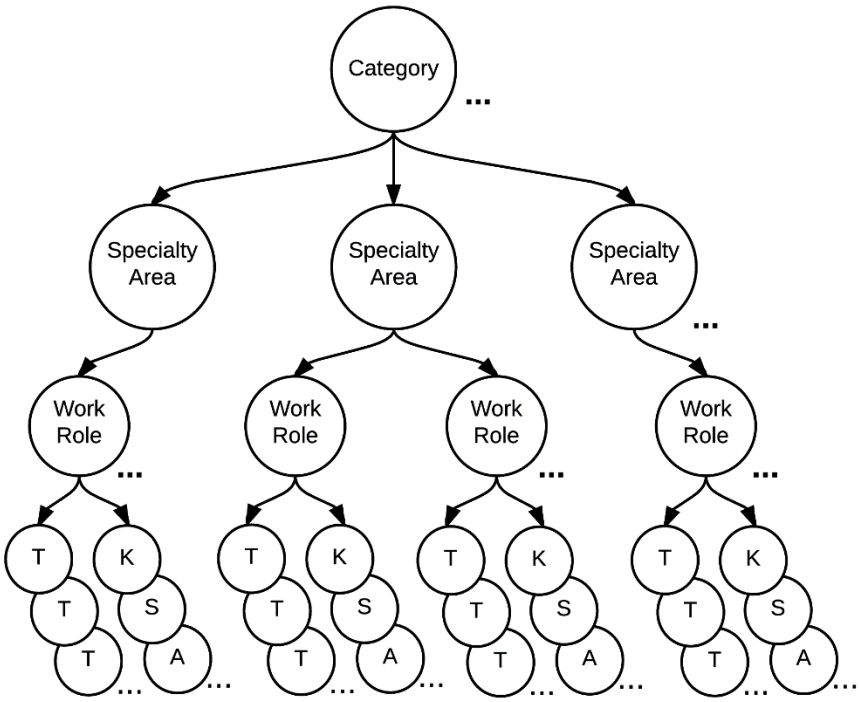

Figure 1 - Relationships among NICE Framework Components

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

3 Using the NICE Framework

Using the NICE Framework to understand organizational needs and assess the extent to which those needs are met can help an organization to plan, implement, and monitor a successful cybersecurity program.

3.1 Identification of Cybersecurity Workforce Needs

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 adequately manage current and future cybersecurity risk, leaders need to consider the cybersecurity workforce capabilities and capacity needed.

Figure 2 illustrates how the NICE Framework is a central reference to help employers build a capable and ready cybersecurity workforce.

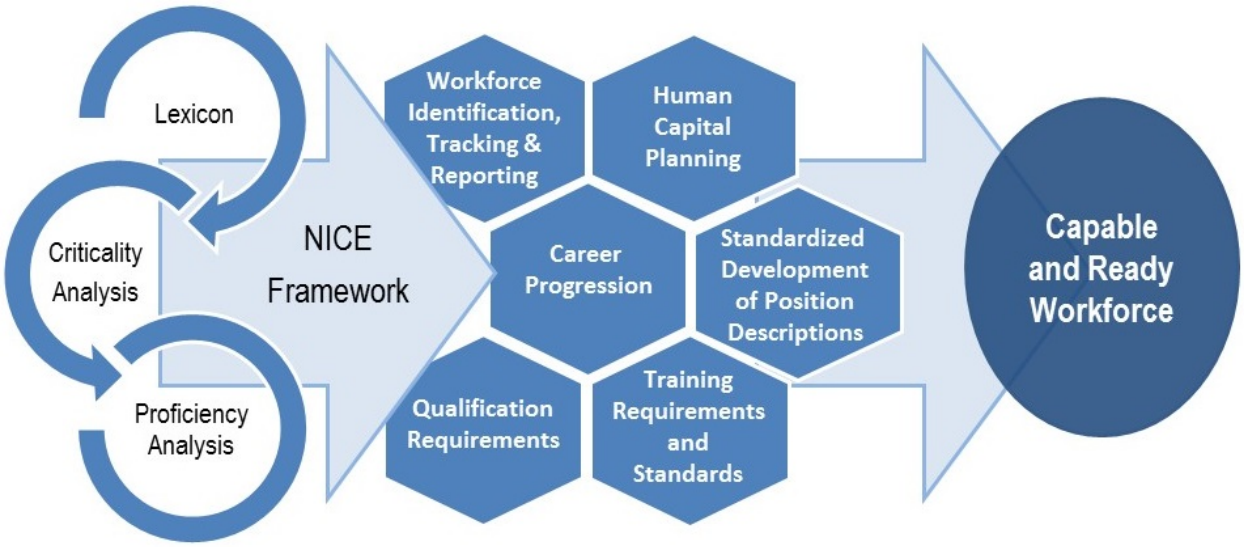

Figure 2 - Building Blocks for a Capable and Ready Cybersecurity Workforce

The circular arrows on the left side of Figure 2 are activities that are likely to have an impact on an organization's ability to develop a capable and ready workforce:

- Using the common lexicon of the NICE Framework clarifies communication between cybersecurity educators, trainers/certifiers, employers, and employees.
- Performing criticality analysis will identify those KSAs and tasks that are critical for successful performance with a given work role and those that are key to multiple work roles.
- Running a proficiency analysis will inform an organization's expectation of the level (e.g. entry-level, expert) for positions, comprised often of more than one work role. The proficiency analysis should enable refinement of selection of the relevant tasks, and KSAs needed for the work roles that make up that position.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix C identifies some existing workforce development tools that support identification of cybersecurity workforce needs.

3.2 Recruitment and Hiring of Highly Skilled Cybersecurity Talent

Referencing the NICE Framework will help organizations to accomplish strategic workforce planning and hiring. NICE Framework material, when used during the creation or revision of position descriptions in vacancy announcements and job postings, will help candidates to seek out specific positions for which they are interested, capable, or qualified. Tasks used to describe a position's duties and responsibilities, and KSAs used to describe the position's needed skills and qualifications, should allow candidates and hiring managers to communicate more effectively. Position descriptions and vacancy announcements using the NICE Framework terminology support more consistent evaluation criteria for vetting and approving candidates.

For organizations who are concerned with workforce gaps, a review of the NICE Framework's list of tasks can determine specific tasks which are not being performed by the organization. Those tasks allow the organization to identify the work role(s) and specialty area(s) that are gaps. The organization is better able to engage with the community of education, training, and credential, and certification providers who map their offerings to the NICE Framework. The organization can identify training that will allow existing staff member to address the gaps. The organization's hiring managers using data pulled from the NICE Framework in this manner can recognize applicants who have the KSAs to perform the cybersecurity tasks.

3.3 Education and Training of Cybersecurity Workforce Members

The NICE Framework' identification of tasks in work roles allows educators to prepare learners with the specific KSAs from which they can demonstrate the ability to perform cybersecurity tasks.

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, enables such institutions to determine common knowledge and abilities that are needed. In turn, developing and delivering curricula that are harmonized with the NICE Framework lexicon allows institutions to prepare students with the skills needed by employers. As the pipeline of students finding desired jobs in cybersecurity increases, more students will be attracted to academic cybersecurity programs as a pathway to a career.

3.4 Retention and Development of Highly Skilled Cybersecurity Talent

A critical aspect of a skilled cybersecurity workforce involves the development and retention 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 may bring new advertising and hiring costs, expenses for training, diminished productivity, and reduced morale. The following list illustrates some of the ways that the NICE Framework supports retention and development of cybersecurity talent:

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

- Organizations can develop career pathways that describe the qualifications necessary for progressively challenging and evolving sets of work roles, such as those enumerated by the NICE Framework.
- A detailed understanding of the KSAs and Tasks helps existing staff to understand the specific steps needed to develop their capabilities, promoting readiness for a desired position.
- An organization might offer staff rotations to provide opportunities to develop and use new skills.
- Organizations can identify personnel that are diligent in improving KSAs in relevant areas, recognizing those who perform well.
- Organizations can create development/improvement plans for staff to help them map out how they can obtain KSAs required for new work roles.
- Group training opportunities can be identified to prepare staff members to enhance common knowledge, skills, and abilities in the work roles of an organization.
- Organizations can use training and examinations that are based for specific cybersecurity skills and abilities to assess proficiency in a realistic environment.
- Organizations 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.
- The NICE Framework is helpful for existing employees who desire to move into a cybersecurity work role from another position. An organization can describe the KSAs needed to allow a reliable employee in a non-cybersecurity work role to become part of the cybersecurity workforce taking on cybersecurity tasks.

4 Extensions

Organizations or sectors can use the NICE Framework to develop additional publications or tools that meet their needs and define or provide guidance on different aspects of workforce development, planning, training, and education.

New reference materials that cross-reference elements of the NICE Framework will be shared via the NICE website [5].

The following areas are a few examples from which additional publications or tools could be developed.

4.1 Competencies

The Department of Labor's Employment and Training Administration [6] 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 [7].

4.2 Job Titles

Job titles are a description of an employee's job or position in an organization. A mapping of sample job titles to specialty areas or work roles would help organizations to use the NICE Framework.

4.3 Cybersecurity Guidance and Guideline documents

NICE Strategic Goal #3, Guide Career Development and Workforce Planning, aims to support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent. One objective within this strategic goal is to publish and raise awareness of the NICE Framework and encourage adoption. Adoption in this case means that the NICE Framework is used as a reference resource for actions related to cybersecurity workforce, training, and education.

One way to encourage adoption of the NICE Framework is to encourage authors of cybersecurity guidance or guideline documents to cross reference their content with components of the NICE Framework. Three example publications are explored in Appendix D.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix A – Listing of NICE Framework Elements

A.1 NICE Framework Workforce Categories

Table 1 provides a description of each Category described by the NICE Framework. Each includes a two-character abbreviation (e.g., SP) for quick reference of the Category and to support the creation of NICE Framework work role identifiers (see Table 3 - NICE Framework work roles). This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 1 - NICE Framework Workforce Categories

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

A.2 NICE Framework Specialty Areas

Table 2 provides a description of each of the NICE Framework Specialty Areas. Each Specialty Area includes a three-character abbreviation (e.g., RSK) for quick reference of the specialty area and to support the creation of NICE Framework work role identifiers (see Table 3 - NICE Framework work roles). This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 2 - NICE Framework Specialty Areas

Categories	Specialty Areas	Specialty Area Descriptions
Securely Provision (SP)	Risk Management (RSK)	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.
	Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
	Systems Architecture (ARC)	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.
	Technology R&D (TRD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning (SRP)	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.
	Test and Evaluation (TST)	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.
	Systems Development (SYS)	Works on the development phases of the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
	Knowledge Management (KMG)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Categories	Specialty Areas	Specialty Area Descriptions
	Customer Service and Technical Support (STS)	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.
	Network Services (NET)	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.
	Systems Administration (ADM)	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis (ANA)	Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	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.
	Training, Education, and Awareness (TEA)	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management (MGT)	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.
	Strategic Planning and Policy (SPP)	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
	Executive Cyber Leadership (EXL)	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
	Program/Project Management (PMA) and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Categories	Specialty Areas	Specialty Area Descriptions
		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 use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
Protect and Defend (PR)	Cybersecurity Defense Analysis (CDA)	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 to protect information, information systems, and networks from threats.
	Cybersecurity Defense Infrastructure Support (INF)	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.
	Incident Response (CIR)	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.
	Vulnerability Assessment and Management (VAM)	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.
Analyze (AN)	Threat Analysis (TWA)	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.
	Exploitation Analysis (EXP)	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis (ASA)	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.
	Targets (TGT)	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis (LNG)	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Categories	Specialty Areas	Specialty Area Descriptions
Collect and Operate (CO)	Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process.
	Cyber Operational Planning (OPL)	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
	Cyber Operations (OPS)	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate (IN)	Cyber Investigation (INV)	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.
	Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

A.3 NICE Framework Work Roles

Table 3 provides a description of each of the work roles described by the NICE Framework. Each work role is identified by the Category and Specialty Area, followed by a sequential number (e.g., SP-RSK-001 is the first work role in the SP Category and RSK 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. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Table 3 - NICE Framework Work Roles

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	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).
		Security Control Assessor	SP-RSK-002	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).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	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.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
	Technology R&D (TRD)	Research & Development Specialist	SP-TRD-001	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	Systems Requirements Planner	SP-SRP-001	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	System Testing and Evaluation Specialist	SP-TST-001	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	SP-SYS-002	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator	OM-DTA-001	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
		Data Analyst	OM-DTA-002	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management (KMG)	Knowledge Manager	OM-KMG-001	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
	Customer Service and Technical Support (STS)	Technical Support Specialist	OM-STS-001	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).
	Network Services (NET)	Network Operations Specialist	OM-NET-001	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration (ADM)	System Administrator	OM-ADM-001	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
	Systems Analysis (ANA)	Systems Security Analyst	OM-ANA-001	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	OV-LGA-001	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Officer/Privacy Compliance Manager	OV-LGA-002	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	OV-TEA-001	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	OV-TEA-002	Develops and conducts training or education of personnel within cyber domain.
		Information Systems Security Manager	OV-MGT-001	Responsible for the cybersecurity of a program, organization, system, or enclave.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
	Cybersecurity Management (MGT)	Communications Security (COMSEC) Manager	OV-MGT-002	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	OV-SPP-001	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.
		Cyber Policy and Strategy Planner	OV-SPP-002	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Executive Cyber Leadership (EXL)	Executive Cyber Leadership	OV-EXL-001	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Program/Project Management (PMA) and Acquisition	Program Manager	OV-PMA-001	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
		IT Project Manager	OV-PMA-002	Directly manages information technology projects.
		Product Support Manager	OV-PMA-003	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	OV-PMA-004	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
		IT Program Auditor	OV-PMA-005	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Analyst	PR-CDA-001	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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
	Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response (CIR)	Cyber Defense Incident Responder	PR-CIR-001	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	PR-VAM-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze (AN)	Threat Analysis (TWA)	Threat/Warning Analyst	AN-TWA-001	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
	Exploitation Analysis (EXP)	Exploitation Analyst	AN-EXP-001	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.
	All-Source Analysis (ASA)	All-Source Analyst	AN-ASA-001	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.
		Mission Assessment Specialist	AN-ASA-002	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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
	Targets (TGT)	Target Developer	AN-TGT-001	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.
		Target Network Analyst	AN-TGT-002	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.
	Language Analysis (LNG)	Multi-Disciplined Language Analyst	AN-LNG-001	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.
Collect and Operate (CO)	Collection Operations (CLO)	All Source-Collection Manager	CO-CLO-001	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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
		All Source-Collection Requirements Manager	CO-CLO-002	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.
	Cyber Operational Planning (OPL)	Cyber Intel Planner	CO-OPL-001	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.
		Cyber Ops Planner	CO-OPL-002	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.
		Partner Integration Planner	CO-OPL-003	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.
	Cyber Operations (OPS)	Cyber Operator	CO-OPS-001	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Investigate (IN)	Cyber Investigation (INV)	Cyber Crime Investigator	IN-INV-001	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Digital Forensics (FOR)	Law Enforcement/Counterintelligence Forensics Analyst	IN-FOR-001	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	IN-FOR-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

A.4 NICE Framework Tasks

Table 4 provides a listing of all the tasks that have been identified as being part of a cybersecurity work role. Each work role includes a subset of the tasks listed here. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 4 - NICE Framework Tasks

Task ID	Task Description
T0001	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.
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
T0006	Advocate organization's official position in legal and legislative proceedings.
T0007	Analyze and define data requirements and specifications.
T0008	Analyze and plan for anticipated changes in data capacity requirements.
T0009	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
T0011	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.
T0014	Apply secure code documentation.
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
T0016	Apply security policies to meet security objectives of the system.
T0017	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.
T0020	Develop content for cyber defense tools.
T0021	Build, test, and modify product prototypes using working models or theoretical models.
T0022	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.
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0024	Collect and maintain data needed to meet system cybersecurity reporting.
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
T0026	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.
T0027	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
T0028	Conduct and/or support authorized penetration testing on enterprise network assets.
T0029	Conduct functional and connectivity testing to ensure continuing operability.
T0030	Conduct interactive training exercises to create an effective learning environment.
T0031	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.
T0032	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).
T0033	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.
T0034	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.
T0035	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
T0036	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
T0037	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.
T0038	Develop threat model based on customer interviews and requirements.
T0039	Consult with customers to evaluate functional requirements.
T0040	Consult with engineering staff to evaluate interface between hardware and software.
T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0042	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
T0045	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.
T0046	Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
T0048	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, CDs, PDAs, mobile phones, GPS, and all tape formats.
T0049	Decrypt seized data using technical means.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0050	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
T0051	Define appropriate levels of system availability based on critical system functions and ensure that 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.
T0052	Define project scope and objectives based on customer requirements.
T0053	Design and develop cybersecurity or cybersecurity-enabled products.
T0054	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
T0055	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.
T0056	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.
T0057	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.
T0058	Determine level of assurance of developed capabilities based on test results.
T0059	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
T0060	Develop an understanding of the needs and requirements of information end-users.
T0061	Develop and direct system testing and validation procedures and documentation.
T0062	Develop and document requirements, capabilities, and constraints for design procedures and processes.
T0063	Develop and document systems administration standard operating procedures.
T0064	Review and validate data mining and data warehousing programs, processes, and requirements.
T0065	Develop and implement network backup and recovery procedures.
T0066	Develop and maintain strategic plans.
T0067	Develop architectures or system components consistent with technical specifications.
T0068	Develop data standards, policies, and procedures.
T0069	Develop detailed security design documentation for component and interface specifications to support system design and development.
T0070	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.
T0071	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).
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.
T0074	Develop policy, programs, and guidelines for implementation.
T0075	Provide technical summary of findings in accordance with established reporting procedures.
T0076	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.
T0077	Develop secure code and error handling.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0078	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.
T0079	Develop specifications to ensure that risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.
T0080	Develop test plans to address specifications and requirements.
T0081	Diagnose network connectivity problem.
T0082	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
T0083	Draft statements of preliminary or residual security risks for system operation.
T0084	Employ secure configuration management processes.
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
T0086	Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.
T0087	Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.
T0088	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
T0089	Ensure that security improvement actions are evaluated, validated, and implemented as required.
T0090	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
T0091	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).
T0093	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.
T0094	Establish and maintain communication channels with stakeholders.
T0095	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.
T0096	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, public relations professionals).
T0097	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.
T0099	Evaluate cost/benefit, economic, and risk analysis in decision-making process.
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.
T0101	Evaluate the effectiveness and comprehensiveness of existing training programs.
T0102	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.
T0103	Examine recovered data for information of relevance to the issue at hand.
T0104	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0105	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.
T0106	Identify alternative information security strategies to address organizational security objective.
T0107	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).
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
T0109	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.
T0110	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
T0111	Identify basic common coding flaws at a high level.
T0112	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
T0114	Identify elements of proof of the crime.
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.
T0116	Identify organizational policy stakeholders.
T0117	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development.
T0118	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.
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.
T0120	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.
T0121	Implement new system design procedures, test procedures, and quality standards.
T0122	Implement security designs for new or existing system(s).
T0123	Implement specific cybersecurity countermeasures for systems and/or applications.
T0124	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).
T0125	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
T0126	Install or replace network hubs, routers, and switches.
T0127	Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.
T0128	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.
T0129	Integrate new systems into existing network architecture.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0130	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.
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.
T0132	Interpret and/or approve security requirements relative to the capabilities of new information technologies.
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
T0134	Lead and align information technology (IT) security priorities with the security strategy.
T0135	Lead and oversee information security budget, staffing, and contracting.
T0136	Maintain baseline system security according to organizational policies.
T0137	Maintain database management systems software.
T0138	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
T0139	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
T0140	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.
T0141	Maintain information systems assurance and accreditation materials.
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
T0143	Make recommendations based on test results.
T0144	Manage accounts, network rights, and access to systems and equipment.
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
T0146	Manage the compilation, cataloging, caching, distribution, and retrieval of data.
T0147	Manage the monitoring of information security data sources to maintain organizational situational awareness.
T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.
T0149	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.
T0150	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
T0152	Monitor and maintain databases to ensure optimal performance.
T0153	Monitor network capacity and performance.
T0154	Monitor and report the usage of knowledge management assets and resources.
T0155	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.
T0156	Oversee and make recommendations regarding configuration management.
T0157	Oversee the information security training and awareness program.
T0158	Participate in an information security risk assessment during the Security Assessment and Authorization process.
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
T0160	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
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.
T0162	Perform backup and recovery of databases to ensure data integrity.
T0163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0164	Perform cyber defense trend analysis and reporting.
T0165	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.
T0166	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.
T0167	Perform file signature analysis.
T0168	Perform hash comparison against established database.
T0169	Perform cybersecurity testing of developed applications and/or systems.
T0170	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
T0171	Perform integrated quality assurance testing for security functionality and resiliency attack.
T0172	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).
T0173	Perform timeline analysis.
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.
T0175	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).
T0176	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
T0178	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
T0179	Perform static media analysis.
T0180	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
T0182	Perform tier 1, 2, and 3 malware analysis.
T0183	Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.
T0184	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
T0185	Plan and manage the delivery of knowledge management projects.
T0186	Plan, execute, and verify data redundancy and system recovery procedures.
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0189	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.
T0190	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).
T0191	Prepare use cases to justify the need for specific information technology (IT) solutions.
T0192	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
T0193	Process crime scenes.
T0194	Properly document all systems security implementation, operations, and maintenance activities and update as necessary.
T0195	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.
T0196	Provide advice on project costs, design concepts, or design changes.
T0197	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances.
T0198	Provide daily summary reports of network events and activity relevant to cyber defense practices.
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
T0200	Provide feedback on network requirements, including network architecture and infrastructure.
T0201	Provide guidelines for implementing developed systems to customers or installation teams.
T0202	Provide cybersecurity guidance to leadership.
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
T0204	Provide input to implementation plans and standard operating procedures.
T0205	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).
T0206	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.
T0207	Provide ongoing optimization and problem-solving support.
T0208	Provide recommendations for possible improvements and upgrades.
T0209	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.
T0210	Provide recommendations on new database technologies and architectures.
T0211	Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.
T0213	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.
T0216	Recognize and accurately report forensic artifacts indicative of a particular operating system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0217	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
T0218	Recommend new or revised security, resilience, and dependability measures based on the results of reviews.
T0219	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
T0222	Review existing and proposed policies with stakeholders.
T0223	Review or conduct audits of information technology (IT) programs and projects.
T0224	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).
T0225	Secure the electronic device or information source.
T0226	Serve on agency and interagency policy boards.
T0227	Recommend policy and coordinate review and approval.
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
T0230	Support the design and execution of exercise scenarios.
T0231	Provide support to security/certification test and evaluation activities.
T0232	Test and maintain network infrastructure including software and hardware devices.
T0233	Track and document cyber defense incidents from initial detection through final resolution.
T0234	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
T0235	Translate functional requirements into technical solutions.
T0236	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.
T0237	Troubleshoot system hardware and software.
T0238	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
T0239	Use federal and organization-specific published documents to manage operations of their computing environment system(s).
T0240	Capture and analyze network traffic associated with malicious activities using network monitoring tools.
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
T0242	Utilize models and simulations to analyze or predict system performance under different operating conditions.
T0243	Verify and update security documentation reflecting the application/system security design features.
T0244	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
T0245	Verify that the software application/network/system accreditation and assurance documentation is current.
T0246	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
T0249	Research current technology to understand capabilities of required system or network.
T0250	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.
T0251	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
T0252	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
T0253	Conduct cursory binary analysis.
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
T0255	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
T0257	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.
T0258	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
T0259	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
T0261	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.
T0262	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
T0264	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
T0265	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.
T0266	Perform penetration testing as required for new or updated applications.
T0267	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
T0268	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
T0269	Design and develop key management functions (as related to cybersecurity).
T0270	Analyze user needs and requirements to plan and conduct system security development.
T0271	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
	availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).
T0272	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
T0273	Develop and document supply chain risks for critical system elements, as appropriate.
T0274	Create auditable evidence of security measures.
T0275	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
T0276	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
T0277	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
T0278	Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
T0280	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.
T0281	Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
T0283	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.
T0284	Design and develop new tools/technologies as related to cybersecurity.
T0285	Perform virus scanning on digital media.
T0286	Perform file system forensic analysis.
T0287	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).
T0288	Perform static malware analysis.
T0289	Utilize deployable forensics toolkit to support operations as necessary.
T0290	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.
T0291	Examine network topologies to understand data flows through the network.
T0292	Recommend computing environment vulnerability corrections.
T0293	Identify and analyze anomalies in network traffic using metadata.
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
T0296	Isolate and remove malware.
T0297	Identify applications and operating systems of a network device based on network traffic.
T0298	Reconstruct a malicious attack or activity based off network traffic.
T0299	Identify network mapping and operating system (OS) fingerprinting activities.
T0300	Develop and document User Experience (UX) requirements including information architecture and user interface requirements.
T0301	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&D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
	Systems Administrators and other cybersecurity staff when performing their day-to-day activities.
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.
T0303	Identify and leverage the enterprise-wide version control system while designing and developing secure applications.
T0304	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.
T0305	Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
T0306	Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.
T0308	Analyze incident data for emerging trends.
T0309	Assess the effectiveness of security controls.
T0310	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.
T0311	Consult with customers about software system design and maintenance.
T0312	Coordinate with intelligence analysts to correlate threat assessment data.
T0313	Design and document quality standards.
T0314	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.
T0315	Develop and deliver technical training to educate others or meet customer needs.
T0316	Develop or assist in the development of computer based training modules or classes.
T0317	Develop or assist in the development of course assignments.
T0318	Develop or assist in the development of course evaluations.
T0319	Develop or assist in the development of grading and proficiency standards.
T0320	Assist in the development of individual/collective development, training, and/or remediation plans.
T0321	Develop or assist in the development of learning objectives and goals.
T0322	Develop or assist in the development of on-the-job training materials or programs.
T0323	Develop or assist in the development of written tests for measuring and assessing learner proficiency.
T0324	Direct software programming and development of documentation.
T0325	Document a system's purpose and preliminary system security concept of operations.
T0326	Employ configuration management processes.
T0327	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.
T0328	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.
T0329	Follow software and systems engineering life cycle standards and processes.
T0330	Maintain assured message delivery systems.
T0331	Maintain incident tracking and solution database.
T0332	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
	potential impact for further action in accordance with the organization's cyber incident response plan.
T0334	Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).
T0335	Build, install, configure, and test dedicated cyber defense hardware.
T0336	Withdrawn: Integrated with T0228
T0337	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
T0338	Write detailed functional specifications that document the architecture development process.
T0339	Lead efforts to promote the organization's use of knowledge management and information sharing.
T0340	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.
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.
T0342	Analyze data sources to provide actionable recommendations.
T0343	Analyze the crisis to ensure public, personal, and resource protection.
T0344	Assess all the configuration management (change configuration/release management) processes.
T0345	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.
T0346	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.
T0347	Assess the validity of source data and subsequent findings.
T0348	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
T0349	Collect metrics and trending data.
T0350	Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.
T0351	Conduct hypothesis testing using statistical processes.
T0352	Conduct learning needs assessments and identify requirements.
T0353	Confer with systems analysts, engineers, programmers, and others to design application.
T0354	Coordinate and manage the overall service provided to a customer end-to-end.
T0355	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.
T0357	Create interactive learning exercises to create an effective learning environment.
T0358	Design and develop system administration and management functionality for privileged access users.
T0359	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.
T0360	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.
T0361	Develop and facilitate data-gathering methods.
T0362	Develop and implement standardized position descriptions based on established cyber work roles.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0363	Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.
T0364	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.
T0365	Develop or assist in the development of training policies and protocols for cyber training.
T0366	Develop strategic insights from large data sets.
T0367	Develop the goals and objectives for cyber curriculum.
T0368	Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.
T0369	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.
T0370	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.
T0371	Establish acceptable limits for the software application, network, or system.
T0372	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.
T0373	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.
T0374	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.
T0375	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.
T0376	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.
T0378	Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).
T0379	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).
T0380	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.
T0381	Present technical information to technical and nontechnical audiences.
T0382	Present data in creative formats.
T0383	Program custom algorithms.
T0384	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.
T0385	Provide actionable recommendations to critical stakeholders based on data analysis and findings.
T0386	Provide criminal investigative support to trial counsel during the judicial process.
T0387	Review and apply cyber career field qualification standards.
T0388	Review and apply organizational policies related to or influencing the cyber workforce.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.
T0391	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.
T0392	Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.
T0393	Validate specifications and requirements for testability.
T0394	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.
T0395	Write and publish after action reviews.
T0396	Process image with appropriate tools depending on analyst's goals.
T0397	Perform Windows registry analysis.
T0398	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.
T0399	Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.
T0400	Correlate incident data and perform cyber defense reporting.
T0401	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
T0402	Effectively allocate storage capacity in the design of data management systems.
T0403	Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) 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).
T0404	Utilize different programming languages to write code, open files, read files, and write output to different files.
T0405	Utilize open 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).
T0406	Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.
T0407	Participate in the acquisition process as necessary.
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.
T0409	Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.
T0410	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.
T0411	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
T0412	Conduct import/export reviews for acquiring systems and software.
T0413	Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.
T0414	Develop supply chain, system, network, performance, and cybersecurity requirements.
T0415	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0416	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.
T0417	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.
T0418	Install, update, and troubleshoot systems/servers.
T0419	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.
T0420	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).
T0421	Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).
T0422	Implement data management standards, requirements, and specifications.
T0423	Analyze computer-generated threats for counter intelligence or criminal activity.
T0424	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.
T0425	Analyze organizational cyber policy.
T0426	Analyze the results of software, hardware, or interoperability testing.
T0427	Analyze user needs and requirements to plan architecture.
T0428	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.
T0430	Gather and preserve evidence used on the prosecution of computer crimes.
T0431	Check system hardware availability, functionality, integrity, and efficiency.
T0432	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.
T0433	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.
T0434	Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.
T0435	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
T0436	Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
T0437	Correlate training and learning to business or mission requirements.
T0438	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).
T0439	Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.
T0440	Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
T0441	Define and integrate current and future mission environments.
T0442	Create training courses tailored to the audience and physical environment.
T0443	Deliver training courses tailored to the audience and physical/virtual environments.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0444	Apply concepts, procedures, software, equipment, and/or technology applications to students.
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.
T0446	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
T0447	Design hardware, operating systems, and software applications to adequately address requirements.
T0448	Develop enterprise architecture or system components required to meet user needs.
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.
T0450	Design training curriculum and course content based on requirements.
T0451	Participate in development of training curriculum and course content.
T0452	Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital.
T0453	Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.
T0454	Define baseline security requirements in accordance with applicable guidelines.
T0455	Develop software system testing and validation procedures, programming, and documentation.
T0456	Develop secure software testing and validation procedures.
T0457	Develop system testing and validation procedures, programming, and documentation.
T0458	Comply with organization systems administration standard operating procedures.
T0459	Implement data mining and data warehousing applications.
T0460	Develop and implement data mining and data warehousing programs.
T0461	Implement and enforce local network usage policies and procedures.
T0462	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.
T0463	Develop cost estimates for new or modified system(s).
T0464	Develop detailed design documentation for component and interface specifications to support system design and development.
T0465	Develop guidelines for implementation.
T0466	Develop mitigation strategies to address cost, schedule, performance, and security risks.
T0467	Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.
T0468	Diagnose and resolve customer reported system incidents, problems, and events.
T0469	Analyze and report organizational security posture trends.
T0470	Analyze and report system security posture trends.
T0471	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).
T0472	Draft, staff, and publish cyber policy.
T0473	Document and update as necessary all definition and architecture activities.
T0474	Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.
T0476	Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.
T0477	Ensure the execution of disaster recovery and continuity of operations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
T0479	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.
T0480	Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).
T0482	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.
T0483	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).
T0484	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
T0485	Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.
T0486	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.
T0487	Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.
T0488	Implement designs for new or existing system(s).
T0489	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.
T0490	Install and configure database management systems and software.
T0491	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.
T0492	Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.
T0493	Lead and oversee budget, staffing, and contracting.
T0494	Administer accounts, network rights, and access to systems and equipment.
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
T0496	Perform asset management/inventory of information technology (IT) resources.
T0497	Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.
T0498	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.
T0499	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.
T0500	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.
T0501	Monitor and maintain system/server configuration.
T0502	Monitor and report client-level computer system performance.
T0503	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.
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0506	Seek consensus on proposed policy changes from stakeholders.
T0507	Oversee installation, implementation, configuration, and support of system components.
T0508	Verify minimum security requirements are in place for all applications.
T0509	Perform an information security risk assessment.
T0510	Coordinate incident response functions.
T0511	Perform developmental testing on systems under development.
T0512	Perform interoperability testing on systems exchanging electronic information with other systems.
T0513	Perform operational testing.
T0514	Diagnose faulty system/server hardware.
T0515	Perform repairs on faulty system/server hardware.
T0516	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
T0517	Integrate results regarding the identification of gaps in security architecture.
T0518	Perform security reviews and identify security gaps in architecture.
T0519	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.
T0520	Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).
T0521	Plan implementation strategy to ensure that enterprise components can be integrated and aligned.
T0522	Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).
T0523	Prepare reports to document the investigation following legal standards and requirements.
T0524	Promote knowledge sharing between information owners/users through an organization's operational processes and systems.
T0525	Provide enterprise cybersecurity and supply chain risk management guidance.
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
T0527	Provide input to implementation plans and standard operating procedures as they relate to information systems security.
T0528	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials
T0529	Provide policy guidance to cyber management, staff, and users.
T0530	Develop a trend analysis and impact report.
T0531	Troubleshoot hardware/software interface and interoperability problems.
T0532	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.
T0533	Review, conduct, or participate in audits of cyber programs and projects.
T0534	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).
T0535	Recommend revisions to curriculum and course content based on feedback from previous training sessions.
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).
T0537	Support the CIO in the formulation of cyber-related policies.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0538	Provide support to test and evaluation activities.
T0539	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.
T0540	Record and manage test data.
T0541	Trace system requirements to design components and perform gap analysis.
T0542	Translate proposed capabilities into technical requirements.
T0544	Verify stability, interoperability, portability, and/or scalability of system architecture.
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.
T0546	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.
T0547	Research and evaluate available technologies and standards to meet customer requirements.
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
T0549	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
T0550	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
T0551	Draft and publish supply chain security and risk management documents.
T0552	Review and approve a supply chain security/risk management policy.
T0553	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.
T0554	Determine and document software patches or the extent of releases that would leave software vulnerable.
T0555	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.
T0556	Assess and design security management functions as related to cyberspace.
T0557	Integrate key management functions as related to cyberspace.
T0558	Analyze user needs and requirements to plan and conduct system development.
T0559	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.
T0560	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).
T0561	Accurately characterize targets.
T0562	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.
T0563	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.
T0564	Analyze feedback to determine extent to which collection products and services are meeting requirements.
T0565	Analyze incoming collection requests.
T0566	Analyze internal operational architecture, tools, and procedures for ways to improve performance.
T0567	Analyze target operational architecture for ways to gain access.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0568	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).
T0569	Answer requests for information.
T0570	Apply and utilize authorized cyber capabilities to enable access to targeted networks.
T0571	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.
T0572	Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.
T0573	Assess and apply operational environment factors and risks to collection management process.
T0574	Apply and obey applicable statutes, laws, regulations and policies.
T0575	Coordinate for intelligence support to operational planning activities.
T0576	Assess all-source intelligence and recommend targets to support cyber operation objectives.
T0577	Assess efficiency of existing information exchange and management systems.
T0578	Assess performance of collection assets against prescribed specifications.
T0579	Assess target vulnerabilities and/or operational capabilities to determine course of action.
T0580	Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly.
T0581	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.
T0582	Provide expertise to course of action development.
T0583	Provide subject matter expertise to the development of a common operational picture.
T0584	Maintain a common intelligence picture.
T0585	Provide subject matter expertise to the development of cyber operations specific indicators.
T0586	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
T0587	Assist in the development and refinement of priority information requirements.
T0588	Provide expertise to the development of measures of effectiveness and measures of performance.
T0589	Assist in the identification of intelligence collection shortfalls.
T0590	Enable synchronization of intelligence support plans across partner organizations as required.
T0591	Perform analysis for target infrastructure exploitation activities.
T0592	Provide input to the identification of cyber-related success criteria.
T0593	Brief threat and/or target current situations.
T0594	Build and maintain electronic target folders.
T0595	Classify documents in accordance with classification guidelines.
T0596	Close requests for information once satisfied.
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.
T0598	Collaborate with development organizations to create and deploy the tools needed to achieve objectives.
T0599	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.
T0600	Collaborate with other internal and external partner organizations on target access and operational issues.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0601	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).
T0602	Collaborate with customer to define information requirements.
T0603	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.
T0604	Compare allocated and available assets to collection demand as expressed through requirements.
T0605	Compile lessons learned from collection management activity's execution of organization collection objectives.
T0606	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.
T0607	Identify and conduct analysis of target communications to identify information essential to support operations.
T0608	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.
T0609	Conduct access enabling of wireless computer and digital networks.
T0610	Conduct collection and processing of wireless computer and digital networks.
T0611	Conduct end-of-operations assessments.
T0612	Conduct exploitation of wireless computer and digital networks.
T0613	Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.
T0614	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.
T0615	Conduct in-depth research and analysis.
T0616	Conduct network scouting and vulnerability analyses of systems within a network.
T0617	Conduct nodal analysis.
T0618	Conduct on-net activities to control and exfiltrate data from deployed technologies.
T0619	Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.
T0620	Conduct open source data collection via various online tools.
T0621	Conduct quality control to determine validity and relevance of information gathered about networks.
T0622	Develop, review and implement all levels of planning guidance in support of cyber operations.
T0623	Conduct survey of computer and digital networks.
T0624	Conduct target research and analysis.
T0625	Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.
T0626	Construct collection plans and matrixes using established guidance and procedures.
T0627	Contribute to crisis action planning for cyber operations.
T0628	Contribute to the development of the organization's decision support tools if necessary.
T0629	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.
T0630	Incorporate intelligence equities into the overall design of cyber operations plans.
T0631	Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.
T0632	Coordinate inclusion of collection plan in appropriate documentation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0633	Coordinate target vetting with appropriate partners.
T0634	Re-task or re-direct collection assets and resources.
T0635	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.
T0636	Coordinate with intelligence planners to ensure that collection managers receive information requirements.
T0637	Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.
T0638	Coordinate, produce, and track intelligence requirements.
T0639	Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.
T0640	Use intelligence estimates to counter potential target actions.
T0641	Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.
T0642	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.
T0643	Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).
T0644	Detect exploits against targeted networks and hosts and react accordingly.
T0645	Determine course of action for addressing changes to objectives, guidance, and operational environment.
T0646	Determine existing collection management webpage databases, libraries and storehouses.
T0647	Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.
T0648	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.
T0649	Determine organizations and/or echelons with collection authority over all accessible collection assets.
T0650	Determine what technologies are used by a given target.
T0651	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.
T0652	Develop all-source intelligence targeting materials.
T0653	Apply analytic techniques to gain more target information.
T0654	Develop and maintain deliberate and/or crisis plans.
T0655	Develop and review specific cyber operations guidance for integration into broader planning activities.
T0656	Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.
T0657	Develop coordinating instructions by collection discipline for each phase of an operation.
T0658	Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives.
T0659	Develop detailed intelligence support to cyber operations requirements.
T0660	Develop information requirements necessary for answering priority information requests.
T0661	Develop measures of effectiveness and measures of performance.
T0662	Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.
T0663	Develop munitions effectiveness assessment or operational assessment materials.
T0664	Develop new techniques for gaining and keeping access to target systems.
T0665	Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0666	Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.
T0667	Develop potential courses of action.
T0668	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.
T0669	Develop strategy and processes for partner planning, operations, and capability development.
T0670	Develop, implement, and recommend changes to appropriate planning procedures and policies.
T0671	Develop, maintain, and assess cyber cooperation security agreements with external partners.
T0672	Devise, document, and validate cyber operation strategy and planning documents.
T0673	Disseminate reports to inform decision makers on collection issues.
T0674	Disseminate tasking messages and collection plans.
T0675	Conduct and document an assessment of the collection results using established procedures.
T0676	Draft cyber intelligence collection and production requirements.
T0677	Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.
T0678	Engage customers to understand customers' intelligence needs and wants.
T0679	Ensure operational planning efforts are effectively transitioned to current operations.
T0680	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.
T0681	Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.
T0682	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.
T0683	Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.
T0684	Estimate operational effects generated through cyber activities.
T0685	Evaluate threat decision-making processes.
T0686	Identify threat vulnerabilities.
T0687	Identify threats to Blue Force vulnerabilities.
T0688	Evaluate available capabilities against desired effects to recommend efficient solutions.
T0689	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.
T0690	Evaluate intelligence estimates to support the planning cycle.
T0691	Evaluate the conditions that affect employment of available cyber intelligence capabilities.
T0692	Generate and evaluate the effectiveness of network analysis strategies.
T0693	Evaluate extent to which collection operations are synchronized with operational requirements.
T0694	Evaluate the effectiveness of collection operations against the collection plan.
T0695	Examine intercept-related metadata and content with an understanding of targeting significance.
T0696	Exploit network devices, security devices, and/or terminals or environments using various methods or tools.
T0697	Facilitate access enabling by physical and/or wireless means.
T0698	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.
T0699	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0700	Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.
T0701	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.
T0702	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.
T0703	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.
T0704	Incorporate cyber operations and communications security support plans into organization objectives.
T0705	Incorporate intelligence and counterintelligence to support plan development.
T0706	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)
T0707	Generate requests for information.
T0708	Identify threat tactics, and methodologies.
T0709	Identify all available partner intelligence capabilities and limitations supporting cyber operations.
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
T0711	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.
T0712	Identify and manage security cooperation priorities with external partners.
T0713	Identify and submit intelligence requirements for the purposes of designating priority information requirements.
T0714	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.
T0715	Identify collection gaps and potential collection strategies against targets.
T0716	Identify coordination requirements and procedures with designated collection authorities.
T0717	Identify critical target elements.
T0718	Identify intelligence gaps and shortfalls.
T0719	Identify cyber intelligence gaps and shortfalls for cyber operational planning.
T0720	Identify gaps in our understanding of target technology and developing innovative collection approaches.
T0721	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.
T0722	Identify network components and their functionality to enable analysis and target development.
T0723	Identify potential collection disciplines for application against priority information requirements.
T0724	Identify potential points of strength and vulnerability within a network.
T0725	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.
T0726	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.
T0727	Identify, locate, and track targets via geospatial analysis techniques.
T0728	Provide input to or develop courses of action based on threat factors.
T0729	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.
T0730	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0731	Initiate requests to guide tasking and assist with collection management.
T0732	Integrate cyber planning/targeting efforts with other organizations.
T0733	Interpret environment preparations assessments to determine a course of action.
T0734	Issue requests for information.
T0735	Lead and coordinate intelligence support to operational planning.
T0736	Lead or enable exploitation operations in support of organization objectives and target requirements.
T0737	Link priority collection requirements to optimal assets and resources.
T0738	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.
T0739	Maintain relationships with internal and external partners involved in cyber planning or related areas.
T0740	Maintain situational awareness and functionality of organic operational infrastructure.
T0741	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.
T0742	Maintain situational awareness of partner capabilities and activities.
T0743	Maintain situational awareness to determine if changes to the operating environment require review of the plan.
T0744	Maintain target lists (i.e., RTL, JTL, CTL, etc.).
T0745	Make recommendations to guide collection in support of customer requirements.
T0746	Modify collection requirements as necessary.
T0747	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.
T0748	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.
T0749	Monitor and report on validated threat activities.
T0750	Monitor completion of reallocated collection efforts.
T0751	Monitor open source websites for hostile content directed towards organizational or partner interests.
T0752	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.
T0753	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.
T0754	Monitor target networks to provide indications and warning of target communications changes or processing failures.
T0755	Monitor the operational environment for potential factors and risks to the collection operation management process.
T0756	Operate and maintain automated systems for gaining and maintaining access to target systems.
T0757	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.
T0758	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
T0759	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.
T0760	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0761	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.
T0764	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.
T0765	Provide subject matter expertise to development of exercises.
T0766	Propose policy which governs interactions with external coordination groups.
T0767	Perform content and/or metadata analysis to meet organization objectives.
T0768	Conduct cyber activities to degrade/remove information resident in computers and computer networks.
T0769	Perform targeting automation activities.
T0770	Characterize websites.
T0771	Provide subject matter expertise to website characterizations.
T0772	Prepare for and provide subject matter expertise to exercises.
T0773	Prioritize collection requirements for collection platforms based on platform capabilities.
T0774	Process exfiltrated data for analysis and/or dissemination to customers.
T0775	Produce network reconstructions.
T0776	Produce target system analysis products.
T0777	Profile network or system administrators and their activities.
T0778	Profile targets and their activities.
T0779	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.
T0780	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.
T0781	Provide aim point and reengagement recommendations.
T0782	Provide analyses and support for effectiveness assessment.
T0783	Provide current intelligence support to critical internal/external stakeholders as appropriate.
T0784	Provide cyber focused guidance and advice on intelligence support plan inputs.
T0785	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
T0786	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.
T0787	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.
T0788	Provide input and assist in post-action effectiveness assessments.
T0789	Provide input and assist in the development of plans and guidance.
T0790	Provide input for targeting effectiveness assessments for leadership acceptance.
T0791	Provide input to the administrative and logistical elements of an operational support plan.
T0792	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
T0793	Provide effectiveness support to designated exercises, and/or time sensitive operations.
T0794	Provide operations and reengagement recommendations.
T0795	Provide planning support between internal and external partners.
T0796	Provide real-time actionable geolocation information.
T0797	Provide target recommendations which meet leadership objectives.
T0798	Provide targeting products and targeting support as designated.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0799	Provide time sensitive targeting support.
T0800	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
T0801	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.
T0802	Review appropriate information sources to determine validity and relevance of information gathered.
T0803	Reconstruct networks in diagram or report format.
T0804	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.
T0805	Report intelligence-derived significant network events and intrusions.
T0806	Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.
T0807	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.
T0808	Review and comprehend organizational leadership objectives and guidance for planning.
T0809	Review capabilities of allocated collection assets.
T0810	Review intelligence collection guidance for accuracy/applicability.
T0811	Review list of prioritized collection requirements and essential information.
T0812	Review and update overarching collection plan, as required.
T0813	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.
T0814	Revise collection matrix based on availability of optimal assets and resources.
T0815	Sanitize and minimize information to protect sources and methods.
T0816	Scope the cyber intelligence planning effort.
T0817	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.
T0818	Serve as a liaison with external partners.
T0819	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.
T0820	Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.
T0821	Specify discipline-specific collections and/or taskings that must be executed in the near term.
T0822	Submit information requests to collection requirement management section for processing as collection requests.
T0823	Submit or respond to requests for deconfliction of cyber operations.
T0824	Support identification and documentation of collateral effects.
T0825	Synchronize cyber international engagement activities and associated resource requirements as appropriate.
T0826	Synchronize cyber portions of security cooperation plans.
T0827	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.
T0828	Test and evaluate locally developed tools for operational use.
T0829	Test internal developed tools and techniques against target tools.
T0830	Track status of information requests, including those processed as collection requests and production requirements, using established procedures.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0831	Translate collection requests into applicable discipline-specific collection requirements.
T0832	Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.
T0833	Validate requests for information according to established criteria.
T0834	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
T0835	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.
T0836	Document lessons learned that convey the results of events and/or exercises.
T0837	Advise managers and operators on language and cultural issues that impact organization objectives.
T0838	Analyze and process information using language and/or cultural expertise.
T0839	Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.
T0840	Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.
T0841	Conduct all-source target research to include the use of open source materials in the target language.
T0842	Conduct analysis of target communications to identify essential information in support of organization objectives.
T0843	Perform quality review and provide feedback on transcribed or translated materials.
T0844	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.
T0845	Identify cyber threat tactics and methodologies.
T0846	Identify target communications within the global network.
T0847	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.
T0848	Provide feedback to collection managers to enhance future collection and analysis.
T0849	Perform foreign language and dialect identification in initial source data.
T0850	Perform or support technical network analysis and mapping.
T0851	Provide requirements and feedback to optimize the development of language processing tools.
T0852	Perform social network analysis and document as appropriate.
T0853	Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.
T0854	Tip critical or time-sensitive information to appropriate customers.
T0855	Transcribe target voice materials in the target language.
T0856	Translate (e.g., verbatim, gist, and/or summaries) target graphic material.
T0857	Translate (e.g., verbatim, gist, and/or summaries) target voice material.
T0858	Identify foreign language terminology within computer programs (e.g., comments, variable names).
T0859	Provide near-real time language analysis support (e.g., live operations).
T0860	Identify cyber/technology-related terminology in the target language.
T0861	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.
T0862	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
	authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
T0863	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.
T0864	Liaise with regulatory and accrediting bodies.
T0865	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.
T0866	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.
T0867	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
T0868	Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.
T0869	Work with organization senior management to establish an organization-wide Privacy Oversight Committee
T0870	Serve in a leadership role for Privacy Oversight Committee activities
T0871	Collaborate on cyber privacy and security policies and procedures
T0872	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation
T0873	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
T0874	Provide strategic guidance to corporate officers regarding information resources and technology
T0875	Assist the Security Officer with the development and implementation of an information infrastructure
T0876	Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
T0877	Work cooperatively with applicable organization units in overseeing consumer information access rights
T0878	Serve as the information privacy liaison for users of technology systems
T0879	Act as a liaison to the information systems department
T0880	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations
T0881	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
T0882	Conduct on-going privacy training and awareness activities
T0883	Work with external 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
T0884	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.
T0885	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0886	Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data
T0887	Provide leadership for the organization's privacy program
T0888	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization
T0889	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
T0890	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures
T0891	Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices
T0892	Develop and coordinate a risk management and compliance framework for privacy
T0893	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.
T0894	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations
T0895	Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures
T0896	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
T0897	Provide leadership in the planning, design and evaluation of privacy and security related projects
T0898	Establish an internal privacy audit program
T0899	Periodically revise the privacy program considering changes in laws, regulatory or company policy
T0900	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
T0901	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information
T0902	Monitor systems development and operations for security and privacy compliance
T0903	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
T0904	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions
T0905	Review all system-related information security plans to ensure alignment between security and privacy practices
T0906	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
T0907	Account for and administer individual requests for release or disclosure of personal and/or protected information
T0908	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0909	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
T0910	Act as, or work with, counsel relating to business partner contracts
T0911	Mitigate effects of a use or disclosure of personal information by employees or business partners
T0912	Develop and apply corrective action procedures
T0913	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
T0914	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
T0915	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations
T0916	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units
T0917	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices
T0918	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations
T0919	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials
T0920	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 noncompliance
T0921	Determine business partner requirements related to the organization's privacy program.
T0922	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.
T0923	Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations.
T0924	Perform ongoing privacy compliance monitoring activities.
T0925	Monitor advancements in information privacy technologies to ensure organization adoption and compliance.
T0926	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.
T0927	Appoint and guide a team of IT security experts.
T0928	Collaborate with key stakeholders to establish a cybersecurity risk management program.
T0929	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.
T0930	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
T0931	Identify the missions, business functions, and mission/business processes the system will support.
T0932	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0933	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.
T0934	Identify stakeholder assets that require protection.
T0935	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.
T0936	Define the stakeholder protection needs and stakeholder security requirements.
T0937	Determine the placement of a system within the enterprise architecture.
T0938	Identify organization-wide common controls that are available for inheritance by organizational systems.
T0939	Conduct a second-level security categorization for organizational systems with the same impact level.
T0940	Determine the boundary of a system.
T0941	Identify the security requirements allocated to a system and to the organization.
T0942	Identify the types of information to be processed, stored, or transmitted by a system.
T0943	Categorize the system and document the security categorization results as part of system requirements.
T0944	Describe the characteristics of a system.
T0945	Register the system with appropriate organizational program/management offices.
T0946	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.
T0947	Develop a strategy for monitoring security control effectiveness; coordinate the system-level strategy with the organization and mission/business process-level monitoring strategy.
T0948	Review and approve security plans.
T0949	Implement the security controls specified in a security plan or other system documentation.
T0950	Document changes to planned security control implementation and establish the configuration baseline for a system.
T0951	Develop, review, and approve a plan to assess the security controls in a system and the organization.
T0952	Assess the security controls in accordance with the assessment procedures defined in a security assessment plan.
T0953	Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment.
T0954	Conduct initial remediation actions on security controls based on the findings and recommendations of a security assessment report; reassess remediated controls.
T0955	Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken.
T0956	Assemble an authorization package and submit the package to an authorizing official for adjudication.
T0957	Determine the risk from the operation or use of a system or the provision or use of common controls.
T0958	Identify and implement a preferred course of action in response to the risk determined.
T0959	Determine if the risk from the operation or use of the system or the provision or use of common controls, is acceptable.
T0960	Monitor changes to a system and its environment of operation.
T0961	Assess the security controls employed within and inherited by the system in accordance with an organization-defined monitoring strategy.
T0962	Respond to risk based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in a plan of action and milestones.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Task ID	Task Description
T0963	Update a security plan, security assessment report, and plan of action and milestones based on the results of a continuous monitoring process.
T0964	Report the security status of a system (including the effectiveness of security controls) to an authorizing official on an ongoing basis in accordance with the monitoring strategy.
T0965	Review the security status of a system (including the effectiveness of security controls) on an ongoing basis to determine whether the risk remains acceptable.
T0966	Implement a system disposal strategy which executes required actions when a system is removed from service.
T0967	Sponsor and promote continuous monitoring within the organization.
T0968	Assign staff as needed to appropriate continuous monitoring working groups.
T0969	Identify reporting requirements to support continuous monitoring activities.
T0970	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.
T0971	Determine how to integrate a continuous monitoring program into the organization's broader information security governance structures and policies.
T0972	Use continuous monitoring scoring and grading metrics to make information security investment decisions to address persistent issues.
T0973	Ensure that the continuous monitoring staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.
T0974	Work with organizational risk analysts to ensure that continuous monitoring reporting covers appropriate levels of the organization.
T0975	Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring.
T0976	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.
T0977	Establish triggers for unacceptable risk thresholds for continuous monitoring data.
T0978	Work with organizational officials to establish system level reporting categories that can be used by the organization's continuous monitoring program.
T0980	Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program.
T0981	Identify the continuous monitoring stakeholders and establish a process to keep them informed about the program.
T0982	Identify security oriented organization reporting requirements that are fulfilled by the continuous monitoring program.
T0983	Use the continuous monitoring data to make information security investment decisions to address persistent issues.
T0984	Define triggers within the continuous monitoring program that can be used to define unacceptable risk and result in action being taken to resolve.
T0985	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.
T0986	Work with security managers to establish appropriate continuous monitoring reporting requirements at the system level.
T0987	Use the continuous monitoring tools and technologies to assess risk on an ongoing basis.
T0988	Establish appropriate reporting requirements in adherence to the criteria identified in the continuous monitoring program for use in automated control assessment.
T0989	Use non-automated assessment methods where the data from the continuous monitoring tools and technologies is not yet of adequate sufficiency or quality.
T0990	Develop processes with the external audit group on how to share information regarding the continuous monitoring program and its impact on security control assessment.

Task ID	Task Description
T0991	Identify reporting requirements for use in automated control assessment to support continuous monitoring.
T0992	Determine how the continuous monitoring results will be used in ongoing authorization.
T0993	Establish continuous monitoring tools and technologies access control process and procedures.
T0994	Ensure that continuous monitoring tools and technologies access control is managed adequately.
T0995	Establish a process to provide technical help to continuous monitoring mitigators.
T0996	Coordinate continuous monitoring reporting requirements across various users.
T0997	Establish responsibilities for supporting implementation of each continuous monitoring tool or technology.
T0998	Establish liaison with scoring and metrics working group to support continuous monitoring.
T0999	Establish and operate a process to manage introduction of new risk to support continuous monitoring.
T1000	Establish continuous monitoring configuration settings issues and coordination sub-group.
T1001	Establish continuous monitoring tools and technologies performance measurement/management requirements.
T1002	Using scores and grades to motivate and assess performance while addressing concerns to support continuous monitoring
T1003	Work with security managers (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements for continuous monitoring at the system level.
T1004	Use continuous monitoring tools to assess risk on an ongoing basis.
T1005	Use the continuous monitoring data to make information security investment decisions to address persistent issues.
T1006	Respond to issues flagged during continuous monitoring, escalate and coordinate a response.
T1007	Review findings from the continuous monitoring program and mitigate risks on a timely basis.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

A.5 NICE Framework Knowledge Descriptions

Table 5 provides a listing of the various kinds of information applied directly to the performance of a function. Selected knowledge ID/descriptions from this list are included for every work role in the Detailed work role Listing in Appendix B. The first six are common to all the cybersecurity work roles. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 5 - NICE Framework Knowledge Descriptions

KSA ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0007	Knowledge of authentication, authorization, and access control methods.
K0008	Knowledge of applicable business processes and operations of customer organizations.
K0009	Knowledge of application vulnerabilities.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K0012	Knowledge of capabilities and requirements analysis.
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0014	Knowledge of complex data structures.
K0015	Knowledge of computer algorithms.
K0016	Knowledge of computer programming principles
K0017	Knowledge of concepts and practices of processing digital forensic data.
K0018	Knowledge of encryption algorithms
K0019	Knowledge of cryptography and cryptographic key management concepts
K0020	Knowledge of data administration and data standardization policies.
K0021	Knowledge of data backup and recovery.
K0022	Knowledge of data mining and data warehousing principles.
K0023	Knowledge of database management systems, query languages, table relationships, and views.
K0024	Knowledge of database systems.
K0025	Knowledge of digital rights management.
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.
K0027	Knowledge of organization's enterprise information security architecture.
K0028	Knowledge of organization's evaluation and validation requirements.
K0029	Knowledge of organization's Local and Wide Area Network connections.
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).
K0031	Knowledge of enterprise messaging systems and associated software.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0032	Knowledge of resiliency and redundancy.
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0034	Knowledge of network services and protocols interactions that provide network communications.
K0035	Knowledge of installation, integration, and optimization of system components.
K0036	Knowledge of human-computer interaction principles.
K0037	Knowledge of Security Assessment and Authorization process.
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
K0041	Knowledge of incident categories, incident responses, and timelines for responses.
K0042	Knowledge of incident response and handling methodologies.
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.
K0048	Knowledge of Risk Management Framework (RMF) requirements.
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.
K0051	Knowledge of low-level computer languages (e.g., assembly languages).
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
K0053	Knowledge of measures or indicators of system performance and availability.
K0054	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.
K0055	Knowledge of microprocessors.
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
K0057	Knowledge of network hardware devices and functions.
K0058	Knowledge of network traffic analysis methods.
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K0060	Knowledge of operating systems.
K0061	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]).
K0062	Knowledge of packet-level analysis.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0063	Knowledge of parallel and distributed computing concepts.
K0064	Knowledge of performance tuning tools and techniques.
K0065	Knowledge of policy-based and risk adaptive access controls.
K0066	Knowledge of Privacy Impact Assessments.
K0067	Knowledge of process engineering concepts.
K0068	Knowledge of programming language structures and logic.
K0069	Knowledge of query languages such as SQL (structured query language).
K0070	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).
K0071	Knowledge of remote access technology concepts.
K0072	Knowledge of resource management principles and techniques.
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
K0075	Knowledge of security system design tools, methods, and techniques.
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.
K0077	Knowledge of server and client operating systems.
K0078	Knowledge of server diagnostic tools and fault identification techniques.
K0079	Knowledge of software debugging principles.
K0080	Knowledge of software design tools, methods, and techniques.
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
K0082	Knowledge of software engineering.
K0083	Knowledge of sources, characteristics, and uses of the organization's data assets.
K0084	Knowledge of structured analysis principles and methods.
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
K0088	Knowledge of systems administration concepts.
K0089	Knowledge of systems diagnostic tools and fault identification techniques.
K0090	Knowledge of system life cycle management principles, including software security and usability.
K0091	Knowledge of systems testing and evaluation methods.
K0092	Knowledge of technology integration processes.
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
K0094	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).
K0095	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines).
K0096	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).
K0097	Knowledge of the characteristics of physical and virtual data storage media.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.
K0100	Knowledge of the enterprise information technology (IT) architecture.
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.
K0102	Knowledge of the systems engineering process.
K0103	Knowledge of the type and frequency of routine hardware maintenance.
K0104	Knowledge of Virtual Private Network (VPN) security.
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0108	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
K0110	Knowledge of adversarial tactics, techniques, and procedures.
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)
K0112	Knowledge of defense-in-depth principles and network security architecture.
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).
K0115	Knowledge that technology that can be exploited.
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0118	Knowledge of processes for seizing and preserving digital evidence.
K0119	Knowledge of hacking methodologies.
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.
K0121	Knowledge of information security program management and project management principles and techniques.
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
K0124	Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain.
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).
K0128	Knowledge of types and collection of persistent data.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0129	Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).
K0130	Knowledge of virtualization technologies and virtual machine development and maintenance.
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K0133	Knowledge of types of digital forensics data and how to recognize them.
K0134	Knowledge of deployable forensics.
K0135	Knowledge of web filtering technologies.
K0136	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).
K0138	Knowledge of Wi-Fi.
K0139	Knowledge of interpreted and compiled computer languages.
K0140	Knowledge of secure coding techniques.
K0141	Withdrawn – Integrated into K0420
K0142	Knowledge of collection management processes, capabilities, and limitations.
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
K0144	Knowledge of social dynamics of computer attackers in a global context.
K0145	Knowledge of security event correlation tools.
K0146	Knowledge of the organization's core business/mission processes.
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.
K0149	Knowledge of organization's risk tolerance and/or risk management approach.
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.
K0151	Knowledge of current and emerging threats/threat vectors.
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).
K0153	Knowledge of software quality assurance process.
K0154	Knowledge of supply chain risk management standards, processes, and practices.
K0155	Knowledge of electronic evidence law.
K0156	Knowledge of legal rules of evidence and court procedure.
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.
K0158	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
K0159	Knowledge of Voice over IP (VoIP).
K0160	Knowledge of the common attack vectors on the network layer.
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0163	Knowledge of critical information technology (IT) procurement requirements.
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).
K0165	Knowledge of risk/threat assessment.
K0167	Knowledge of system administration, network, and operating system hardening techniques.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0168	Knowledge of applicable 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.
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
K0171	Knowledge of hardware reverse engineering techniques.
K0172	Knowledge of middleware (e.g., enterprise service bus and message queuing).
K0174	Knowledge of networking protocols.
K0175	Knowledge of software reverse engineering techniques.
K0176	Knowledge of Extensible Markup Language (XML) schemas.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0178	Knowledge of secure software deployment methodologies, tools, and practices.
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).
K0183	Knowledge of reverse engineering concepts.
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
K0186	Knowledge of debugging procedures and tools.
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).
K0190	Knowledge of encryption methodologies.
K0191	Signature implementation impact for viruses, malware, and attacks.
K0192	Knowledge of Windows/Unix ports and services.
K0193	Knowledge of advanced data remediation security features in databases.
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
K0195	Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.
K0197	Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
K0198	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).
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
K0201	Knowledge of symmetric key rotation techniques and concepts.
K0202	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).
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
K0204	Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).
K0205	Knowledge of basic system, network, and OS hardening techniques.
K0206	Knowledge of ethical hacking principles and techniques.
K0207	Knowledge of circuit analysis.
K0208	Knowledge of computer based training and e-learning services.
K0209	Knowledge of covert communication techniques.
K0210	Knowledge of data backup and restoration concepts.
K0211	Knowledge of confidentiality, integrity, and availability requirements.
K0212	Knowledge of cybersecurity-enabled software products.
K0213	Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).
K0214	Knowledge of the Risk Management Framework Assessment Methodology.
K0215	Knowledge of organizational training policies.
K0216	Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).
K0217	Knowledge of Learning Management Systems and their use in managing learning.
K0218	Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).
K0220	Knowledge of modes of learning (e.g., rote learning, observation).
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
K0223	Withdrawn – integrated into K0073
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
K0226	Knowledge of organizational training systems.
K0227	Knowledge of various types of computer architectures.
K0228	Knowledge of taxonomy and semantic ontology theory.
K0229	Knowledge of applications that can log errors, exceptions, and application faults and logging.
K0230	Knowledge of cloud service models and how those models can limit incident response.
K0231	Knowledge of crisis management protocols, processes, and techniques.
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.
K0234	Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).
K0235	Knowledge of how to leverage research and development centers, think tanks, academic research, and industry systems.
K0236	Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and Pig to explore data.
K0237	Knowledge of industry best practices for service desk.
K0238	Knowledge of machine learning theory and principles.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0239	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.
K0240	Knowledge of multi-level security systems and cross domain solutions.
K0241	Knowledge of organizational human resource policies, processes, and procedures.
K0242	Knowledge of organizational security policies.
K0243	Knowledge of organizational training and education policies, processes, and procedures.
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.
K0245	Knowledge of principles and processes for conducting training and education needs assessment.
K0246	Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
K0247	Knowledge of remote access processes, tools, and capabilities related to customer support.
K0248	Knowledge of strategic theory and practice.
K0249	Knowledge of sustainment technologies, processes and strategies.
K0250	Knowledge of Test & Evaluation processes for learners.
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.
K0252	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.
K0253	Withdrawn – Integrated into K0227
K0254	Knowledge of binary analysis.
K0255	Knowledge of network architecture concepts including topology, protocols, and components.
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).
K0259	Knowledge of malware analysis concepts and methodologies.
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
K0261	Knowledge of Payment Card Industry (PCI) data security standards.
K0262	Knowledge of Personal Health Information (PHI) data security standards.
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.
K0264	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.
K0266	Knowledge of how to evaluate the trustworthiness of the supplier and/or product.
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
K0268	Knowledge of forensic footprint identification.
K0269	Knowledge of mobile communications architecture.
K0270	Knowledge of the acquisition/procurement life cycle process.
K0271	Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0274	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.
K0275	Knowledge of configuration management techniques.
K0276	Knowledge of security management.
K0277	Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).
K0278	Knowledge of current and emerging data remediation security features in databases.
K0280	Knowledge of systems engineering theories, concepts, and methods.
K0281	Knowledge of information technology (IT) service catalogues.
K0282	Withdrawn – Integrated into K0200
K0283	Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).
K0284	Knowledge of developing and applying user credential management system.
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.
K0286	Knowledge of N-tiered typologies (e.g. including server and client operating systems).
K0287	Knowledge of an organization's information classification program and procedures for information compromise.
K0288	Knowledge of industry standard security models.
K0289	Knowledge of system/server diagnostic tools and fault identification techniques.
K0290	Knowledge of systems security testing and evaluation methods.
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
K0292	Knowledge of the operations and processes for incident, problem, and event management.
K0293	Knowledge of integrating the organization’s goals and objectives into the architecture.
K0294	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
K0295	Knowledge of confidentiality, integrity, and availability principles.
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
K0297	Knowledge of countermeasure design for identified security risks.
K0298	Knowledge of countermeasures for identified security risks.
K0299	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.
K0300	Knowledge of network mapping and recreating network topologies.
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
K0302	Knowledge of the basic operation of computers.
K0303	Knowledge of the use of sub-netting tools.
K0304	Knowledge of concepts and practices of processing digital forensic data.
K0305	Knowledge of data concealment (e.g. encryption algorithms and stenography).
K0308	Knowledge of cryptology.
K0309	Knowledge of emerging technologies that have potential for exploitation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0310	Knowledge of hacking methodologies.
K0311	Knowledge of industry indicators useful for identifying technology trends.
K0312	Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).
K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.
K0315	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.
K0316	Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.
K0317	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.
K0318	Knowledge of operating system command-line tools.
K0319	Knowledge of technical delivery capabilities and their limitations.
K0320	Knowledge of organization's evaluation and validation criteria.
K0321	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.
K0322	Knowledge of embedded systems.
K0323	Knowledge of system fault tolerance methodologies.
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
K0326	Knowledge of demilitarized zones.
K0330	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).
K0335	Knowledge of current and emerging cyber technologies.
K0336	Knowledge of access authentication methods.
K0337	Withdrawn – Integrated into K0007
K0338	Knowledge of data mining techniques.
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0341	Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0343	Knowledge of root cause analysis techniques.
K0344	Knowledge of an organization's threat environment.
K0346	Knowledge of principles and methods for integrating system components.
K0347	Knowledge and understanding of operational design.
K0349	Knowledge of website types, administration, functions, and content management system (CMS).
K0350	Knowledge of accepted organization planning systems.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.
K0352	Knowledge of forms of intelligence support needs, topics, and focus areas.
K0353	Knowledge of possible circumstances that would result in changing collection management authorities.
K0354	Knowledge of relevant reporting and dissemination procedures.
K0355	Knowledge of all-source reporting and dissemination procedures.
K0356	Knowledge of analytic tools and techniques for language, voice and/or graphic material.
K0357	Knowledge of analytical constructs and their use in assessing the operational environment.
K0358	Knowledge of analytical standards and the purpose of intelligence confidence levels.
K0359	Knowledge of approved intelligence dissemination processes.
K0361	Knowledge of asset availability, capabilities and limitations.
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
K0363	Knowledge of auditing and logging procedures (including server-based logging).
K0364	Knowledge of available databases and tools necessary to assess appropriate collection tasking.
K0367	Knowledge of penetration testing.
K0368	Knowledge of implants that enable cyber collection and/or preparation activities.
K0371	Knowledge of principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis).
K0372	Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages).
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0375	Knowledge of wireless applications vulnerabilities.
K0376	Knowledge of internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.
K0377	Knowledge of classification and control markings standards, policies and procedures.
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.
K0380	Knowledge of collaborative tools and environments.
K0381	Knowledge of collateral damage and estimating impact(s).
K0382	Knowledge of collection capabilities and limitations.
K0383	Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.
K0384	Knowledge of collection management functionality (e.g., positions, functions, responsibilities, products, reporting requirements).
K0385	Withdrawn – Integrated into K0142
K0386	Knowledge of collection management tools.
K0387	Knowledge of collection planning process and collection plan.
K0388	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.
K0389	Knowledge of collection sources including conventional and non-conventional sources.
K0390	Knowledge of collection strategies.
K0391	Knowledge of collection systems, capabilities, and processes.
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0393	Knowledge of common networking devices and their configurations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0394	Knowledge of common reporting databases and tools.
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.
K0397	Knowledge of security concepts in operating systems (e.g., Linux, Unix.)
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
K0399	Knowledge of crisis action planning and time sensitive planning procedures.
K0400	Knowledge of crisis action planning for cyber operations.
K0401	Knowledge of criteria for evaluating collection products.
K0402	Knowledge of criticality and vulnerability factors (e.g., value, recuperation, cushion, countermeasures) for target selection and applicability to the cyber domain.
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.
K0404	Knowledge of current collection requirements.
K0405	Knowledge of current computer-based intrusion sets.
K0406	Knowledge of current software and methodologies for active defense and system hardening.
K0407	Knowledge of customer information needs.
K0408	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber-attack) principles, capabilities, limitations, and effects.
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.
K0410	Knowledge of cyber laws and their effect on Cyber planning.
K0411	Knowledge of cyber laws and legal considerations and their effect on cyber planning.
K0412	Knowledge of cyber lexicon/terminology
K0413	Knowledge of cyber operation objectives, policies, and legalities.
K0414	Knowledge of cyber operations support or enabling processes.
K0415	Knowledge of cyber operations terminology/lexicon.
K0416	Knowledge of cyber operations.
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).
K0418	Knowledge of data flow process for terminal or environment collection.
K0419	Knowledge of database administration and maintenance.
K0420	Knowledge of database theory.
K0421	Knowledge of databases, portals and associated dissemination vehicles.
K0422	Knowledge of deconfliction processes and procedures.
K0423	Knowledge of deconfliction reporting to include external organization interaction.
K0424	Knowledge of denial and deception techniques.
K0425	Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.
K0426	Knowledge of dynamic and deliberate targeting.
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).
K0428	Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).
K0429	Knowledge of enterprise-wide information management.
K0430	Knowledge of evasion strategies and techniques.
K0431	Knowledge of evolving/emerging communications technologies.
K0432	Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.
K0433	Knowledge of forensic implications of operating system structure and operations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.
K0437	Knowledge of general Supervisory control and data acquisition (SCADA) system components.
K0438	Knowledge of mobile cellular communications architecture (e.g., LTE, CDMA, GSM/EDGE and UMTS/HSPA).
K0439	Knowledge of governing authorities for targeting.
K0440	Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.
K0442	Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).
K0443	Knowledge of how hubs, switches, routers work together in the design of a network.
K0444	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.
K0446	Knowledge of how modern wireless communications systems impact cyber operations.
K0447	Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).
K0448	Knowledge of how to establish priorities for resources.
K0449	Knowledge of how to extract, analyze, and use metadata.
K0450	Withdrawn – Integrated into K0036
K0451	Knowledge of identification and reporting processes.
K0452	Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0453	Knowledge of indications and warning.
K0454	Knowledge of information needs.
K0455	Knowledge of information security concepts, facilitating technologies and methods.
K0456	Knowledge of intelligence capabilities and limitations.
K0457	Knowledge of intelligence confidence levels.
K0458	Knowledge of intelligence disciplines.
K0459	Knowledge of intelligence employment requirements (i.e., logistical, communications support, maneuverability, legal restrictions, etc.).
K0460	Knowledge of intelligence preparation of the environment and similar processes.
K0461	Knowledge of intelligence production processes.
K0462	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.
K0463	Knowledge of intelligence requirements tasking systems.
K0464	Knowledge of intelligence support to planning, execution, and assessment.
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.
K0466	Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.
K0467	Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).
K0468	Knowledge of internal and external partner reporting.
K0469	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0470	Knowledge of Internet and routing protocols.
K0471	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K0472	Knowledge of intrusion detection systems and signature development.
K0473	Knowledge of intrusion sets.
K0474	Knowledge of key cyber threat actors and their equities.
K0475	Knowledge of key factors of the operational environment and threat.
K0476	Knowledge of language processing tools and techniques.
K0477	Knowledge of leadership's Intent and objectives.
K0478	Knowledge of legal considerations in targeting.
K0479	Knowledge of malware analysis and characteristics.
K0480	Knowledge of malware.
K0481	Knowledge of methods and techniques used to detect various exploitation activities.
K0482	Knowledge of methods for ascertaining collection asset posture and availability.
K0483	Knowledge of methods to integrate and summarize information from any potential sources.
K0484	Knowledge of midpoint collection (process, objectives, organization, targets, etc.).
K0485	Knowledge of network administration.
K0486	Knowledge of network construction and topology.
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0488	Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network.
K0489	Knowledge of network topology.
K0490	Withdrawn – Integrated into K0058
K0491	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.).
K0492	Knowledge of non-traditional collection methodologies.
K0493	Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/VPS, encryption).
K0494	Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.
K0495	Knowledge of ongoing and future operations.
K0496	Knowledge of operational asset constraints.
K0497	Knowledge of operational effectiveness assessment.
K0498	Knowledge of operational planning processes.
K0499	Knowledge of operations security.
K0500	Knowledge of organization and/or partner collection systems, capabilities, and processes (e.g., collection and protocol processors).
K0501	Knowledge of organization cyber operations programs, strategies, and resources.
K0502	Knowledge of organization decision support tools and/or methods.
K0503	Knowledge of organization formats of resource and asset readiness reporting, its operational relevance and intelligence collection impact.
K0504	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.
K0505	Knowledge of organization objectives and associated demand on collection management.
K0506	Knowledge of organization objectives, leadership priorities, and decision-making risks.
K0507	Knowledge of organization or partner exploitation of digital networks.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0508	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.
K0509	Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.
K0510	Knowledge of organizational and partner policies, tools, capabilities, and procedures.
K0511	Knowledge of organizational hierarchy and cyber decision-making processes.
K0512	Knowledge of organizational planning concepts.
K0513	Knowledge of organizational priorities, legal authorities and requirements submission processes.
K0514	Knowledge of organizational structures and associated intelligence capabilities.
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
K0517	Knowledge of post implementation review (PIR) approval process.
K0518	Knowledge of planning activity initiation.
K0519	Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.
K0520	Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.
K0521	Knowledge of priority information, how it is derived, where it is published, how to access, etc.
K0522	Knowledge of production exploitation and dissemination needs and architectures.
K0523	Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities.
K0524	Knowledge of relevant laws, regulations, and policies.
K0525	Knowledge of required intelligence planning products associated with cyber operational planning.
K0526	Knowledge of research strategies and knowledge management.
K0527	Knowledge of risk management and mitigation strategies.
K0528	Knowledge of satellite-based communication systems.
K0529	Knowledge of scripting
K0530	Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.
K0531	Knowledge of security implications of software configurations.
K0532	Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, code words).
K0533	Knowledge of specific target identifiers, and their usage.
K0534	Knowledge of staff management, assignment, and allocation processes.
K0535	Knowledge of strategies and tools for target research.
K0536	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).
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities
K0539	Knowledge of target communication profiles and their key elements (e.g., target associations, activities, communication infrastructure).
K0540	Knowledge of target communication tools and techniques.
K0541	Knowledge of target cultural references, dialects, expressions, idioms, and abbreviations.
K0542	Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0543	Knowledge of target estimated repair and recuperation times.
K0544	Knowledge of target intelligence gathering and operational preparation techniques and life cycles.
K0545	Knowledge of target language(s).
K0546	Knowledge of target list development (i.e. Restricted, Joint, Candidate, etc.).
K0547	Knowledge of target methods and procedures.
K0548	Knowledge of target or threat cyber actors and procedures.
K0549	Knowledge of target vetting and validation procedures.
K0550	Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.
K0551	Knowledge of targeting cycles.
K0552	Knowledge of tasking mechanisms.
K0553	Knowledge of tasking processes for organic and subordinate collection assets.
K0554	Knowledge of tasking, collection, processing, exploitation and dissemination.
K0555	Knowledge of TCP/IP networking protocols.
K0556	Knowledge of telecommunications fundamentals.
K0557	Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).
K0558	Knowledge of the available tools and applications associated with collection requirements and collection management.
K0559	Knowledge of the basic structure, architecture, and design of converged applications.
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0562	Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.
K0563	Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.
K0564	Knowledge of the characteristics of targeted communication networks (e.g., capacity, functionality, paths, critical nodes).
K0565	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.
K0566	Knowledge of the critical information requirements and how they're used in planning.
K0567	Knowledge of the data flow from collection origin to repositories and tools.
K0568	Knowledge of the definition of collection management and collection management authority.
K0569	Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.
K0570	Knowledge of the factors of threat that could impact collection operations.
K0571	Knowledge of the feedback cycle in collection processes.
K0572	Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.
K0573	Knowledge of the fundamentals of digital forensics to extract actionable intelligence.
K0574	Knowledge of the impact of language analysis on on-net operator functions.
K0575	Knowledge of the impacts of internal and external partner staffing estimates.
K0576	Knowledge of the information environment.
K0577	Knowledge of the intelligence frameworks, processes, and related systems.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

KSA ID	Description
K0578	Knowledge of the intelligence requirements development and request for information processes.
K0579	Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.
K0580	Knowledge of the organization's established format for collection plan.
K0581	Knowledge of the organization's planning, operations and targeting cycles.
K0582	Knowledge of the organizational planning and staffing process.
K0583	Knowledge of the organizational plans/directives/guidance that describe objectives.
K0584	Knowledge of the organizational policies/procedures for temporary transfer of collection authority.
K0585	Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.
K0586	Knowledge of the outputs of course of action and exercise analysis.
K0587	Knowledge of the POC's, databases, tools and applications necessary to establish environment preparation and surveillance products.
K0588	Knowledge of the priority information requirements from subordinate, lateral and higher levels of the organization.
K0589	Knowledge of the process used to assess the performance and impact of operations.
K0590	Knowledge of the processes to synchronize operational assessment procedures with the critical information requirement process.
K0591	Knowledge of the production responsibilities and organic analysis and production capabilities.
K0592	Knowledge of the purpose and contribution of target templates.
K0593	Knowledge of the range of cyber operations and their underlying intelligence support needs, topics, and focus areas.
K0594	Knowledge of the relationships between end states, objectives, effects, lines of operation, etc.
K0595	Knowledge of the relationships of operational objectives, intelligence requirements, and intelligence production tasks.
K0596	Knowledge of the request for information process.
K0597	Knowledge of the role of network operations in supporting and facilitating other organization operations.
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.
K0599	Knowledge of the structure, architecture, and design of modern digital and telephony networks.
K0600	Knowledge of the structure, architecture, and design of modern wireless communications systems.
K0601	Knowledge of the systems/architecture/communications used for coordination.
K0602	Knowledge of collection disciplines and capabilities.
K0603	Knowledge of the ways in which targets or threats use the Internet.
K0604	Knowledge of threat and/or target systems.
K0605	Knowledge of tipping, cueing, mixing, and redundancy.
K0606	Knowledge of transcript development processes and techniques (e.g., verbatim, gist, summaries).
K0607	Knowledge of translation processes and techniques.

KSA ID	Description
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).
K0609	Knowledge of virtual machine technologies.
K0610	Knowledge of virtualization products (VMware, Virtual PC).
K0611	Withdrawn – Integrated into K0131
K0612	Knowledge of what constitutes a “threat” to a network.
K0613	Knowledge of who the organization’s operational planners are, how and where they can be contacted, and what are their expectations.
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.
K0615	Knowledge of privacy disclosure statements based on current laws.
K0616	Knowledge of continuous monitoring, its processes, and Continuous Diagnostics and Mitigation (CDM) program activities.
K0617	Knowledge of Automated security control assessments
K0618	Knowledge of hardware asset management and the value of tracking the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
K0619	Knowledge of software asset management and the value of tracking the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
K0620	Knowledge of continuous monitoring technologies and tools.
K0621	Knowledge of risk scoring.
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.
K0623	Knowledge of risk assessment methodologies.
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
K0625	Knowledge that patching and software updates are impractical for some networked devices.
K0626	Knowledge of secure update mechanisms.
K0627	Knowledge of the importance of ingress filtering to protect against automated threats that rely on spoofed network addresses.
K0628	Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
K0629	Knowledge of white/black listing
K0630	Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

A.6 NICE Framework Skills Descriptions

Table 6 provides a listing of cybersecurity skills. A skill is the observable competence to perform a learned psychomotor act. Selected skills descriptions from this list are included for each work role in the Detailed work role Listing in Appendix B. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 6 - NICE Framework Skills Descriptions

Skill ID	Description
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0002	Skill in allocating storage capacity in the design of data management systems.
S0003	Skill of identifying, capturing, containing, and reporting malware.
S0004	Skill in analyzing network traffic capacity and performance characteristics.
S0005	Skill in applying and incorporating information technologies into proposed solutions.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0007	Skill in applying host/network access controls (e.g., access control list).
S0008	Skill in applying organization-specific systems analysis principles and techniques.
S0009	Skill in assessing the robustness of security systems and designs.
S0010	Skill in conducting capabilities and requirements analysis.
S0011	Skill in conducting information searches.
S0012	Skill in conducting knowledge mapping (e.g., map of knowledge repositories).
S0013	Skill in conducting queries and developing algorithms to analyze data structures.
S0014	Skill in conducting software debugging.
S0015	Skill in conducting test events.
S0016	Skill in configuring and optimizing software.
S0017	Skill in creating and utilizing mathematical or statistical models.
S0018	Skill in creating policies that reflect system security objectives.
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.
S0020	Skill in developing and deploying signatures.
S0021	Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).
S0022	Skill in designing countermeasures to identified security risks.
S0023	Skill in designing security controls based on cybersecurity principles and tenets.
S0024	Skill in designing the integration of hardware and software solutions.
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
S0026	Skill in determining an appropriate level of test rigor for a given system.
S0027	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.
S0028	Skill in developing data dictionaries.
S0029	Skill in developing data models.
S0030	Skill in developing operations-based testing scenarios.
S0031	Skill in developing and applying security system access controls.
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0033	Skill in diagnosing connectivity problems.
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
S0035	Skill in establishing a routing schema.
S0036	Skill in evaluating the adequacy of security designs.
S0037	Skill in generating queries and reports.
S0038	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.
S0039	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.
S0040	Skill in implementing, maintaining, and improving established network security practices.
S0041	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).
S0043	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
S0044	Skill in mimicking threat behaviors.
S0045	Skill in optimizing database performance.
S0046	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0048	Skill in systems integration testing.
S0049	Skill in the measuring and reporting of intellectual capital.
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).
S0051	Skill in the use of penetration testing tools and techniques.
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
S0053	Skill in tuning sensors.
S0054	Skill in using incident handling methodologies.
S0055	Skill in using knowledge management technologies.
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).
S0057	Skill in using protocol analyzers.
S0058	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).
S0061	Skill in writing test plans.
S0062	Skill in analyzing memory dumps to extract information.
S0063	Skill in collecting data from a variety of cyber defense resources.
S0064	Skill in developing and executing technical training programs and curricula.
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
S0066	Skill in identifying gaps in technical capabilities.
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.
S0069	Skill in setting up a forensic workstation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0070	Skill in talking to others to convey information effectively.
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).
S0072	Skill in using scientific rules and methods to solve problems.
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
S0074	Skill in physically disassembling PCs.
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).
S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
S0077	Skill in securing network communications.
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
S0080	Skill in performing damage assessments.
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).
S0082	Skill in evaluating test plans for applicability and completeness.
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.
S0084	Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
S0085	Skill in conducting audits or reviews of technical systems.
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
S0090	Skill in analyzing anomalous code as malicious or benign.
S0091	Skill in analyzing volatile data.
S0092	Skill in identifying obfuscation techniques.
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.
S0094	Skill in reading Hexadecimal data.
S0095	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).
S0096	Skill in reading and interpreting signatures (e.g., snort).
S0097	Skill in applying security controls.
S0100	Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).
S0101	Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.
S0102	Skill in applying technical delivery capabilities.
S0103	Skill in assessing the predictive power and subsequent generalizability of a model.
S0104	Skill in conducting Test Readiness Reviews.
S0106	Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing).
S0107	Skill in designing and documenting overall program Test & Evaluation strategies.
S0108	Skill in developing workforce and position qualification standards.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0109	Skill in identifying hidden patterns or relationships.
S0110	Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.
S0111	Skill in interfacing with customers.
S0112	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.
S0113	Skill in performing format conversions to create a standard representation of the data.
S0114	Skill in performing sensitivity analysis.
S0115	Skill in preparing Test & Evaluation reports.
S0116	Skill in designing multi-level security/cross domain solutions.
S0117	Skill in providing Test & Evaluation resource estimate.
S0118	Skill in developing machine understandable semantic ontologies.
S0119	Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic).
S0120	Skill in reviewing logs to identify evidence of past intrusions.
S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).
S0122	Skill in the use of design methods.
S0123	Skill in transformation analytics (e.g., aggregation, enrichment, processing).
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.
S0125	Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).
S0126	Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS).
S0127	Skill in using data mapping tools.
S0128	Skill in using manpower and personnel IT systems.
S0129	Skill in using outlier identification and removal techniques.
S0130	Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.
S0131	Skill in analyzing malware.
S0132	Skill in conducting bit-level analysis.
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.
S0134	Skill in conducting reviews of systems.
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).
S0136	Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
S0137	Skill in conducting application vulnerability assessments.
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).
S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
S0140	Skill in applying the systems engineering process.
S0141	Skill in assessing security systems designs.
S0142	Skill in conducting research for troubleshooting novel client-level problems.
S0143	Skill in conducting system/server planning, management, and maintenance.
S0144	Skill in correcting physical and technical problems that impact system/server performance.
S0145	Skill in integrating and applying policies that meet system security objectives.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0146	Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.
S0150	Skill in implementing and testing network infrastructure contingency and recovery plans.
S0151	Skill in troubleshooting failed system components (i.e., servers)
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).
S0153	Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.
S0154	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).
S0155	Skill in monitoring and optimizing system/server performance.
S0156	Skill in performing packet-level analysis.
S0157	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).
S0158	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).
S0159	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.
S0160	Skill in the use of design modeling (e.g., unified modeling language).
S0161	Withdrawn – Integrated into S0160
S0162	Skill in sub-netting.
S0163	Withdrawn – Integrated into S0060
S0164	Skill in assessing the application of cryptographic standards.
S0166	Skill in identifying gaps in technical delivery capabilities.
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.
S0169	Skill in conducting trend analysis.
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
S0171	Skill in performing impact/risk assessments.
S0172	Skill in applying secure coding techniques.
S0173	Skill in using security event correlation tools.
S0174	Skill in using code analysis tools.
S0175	Skill in performing root cause analysis.
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.
S0177	Skill in analyzing a target's communication networks.
S0178	Skill in analyzing essential network data (e.g., router configuration files, routing protocols).
S0179	Skill in analyzing language processing tools to provide feedback to enhance tool development.
S0180	Withdrawn – Integrated into S0062

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0181	Skill in analyzing midpoint collection data.
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs.
S0183	Skill in analyzing terminal or environment collection data.
S0184	Skill in analyzing traffic to identify network devices.
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.
S0186	Skill in applying crisis planning procedures.
S0187	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).
S0188	Skill in assessing a target's frame of reference (e.g., motivation, technical capability, organizational structure, sensitivities).
S0189	Skill in assessing and/or estimating effects generated during and after cyber operations.
S0190	Skill in assessing current tools to identify needed improvements.
S0191	Skill in assessing the applicability of available analytical tools to various situations.
S0192	Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.
S0193	Skill in complying with the legal restrictions for targeted information.
S0194	Skill in conducting non-attributable research.
S0195	Skill in conducting research using all available sources.
S0196	Skill in conducting research using deep web.
S0197	Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.
S0198	Skill in conducting social network analysis.
S0199	Skill in creating and extracting important information from packet captures.
S0200	Skill in creating collection requirements in support of data acquisition activities.
S0201	Skill in creating plans in support of remote operations. (i.e., hot/warm/cold/alternative sites, disaster recovery).
S0202	Skill in data mining techniques (e.g., searching file systems) and analysis.
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.
S0204	Skill in depicting source or collateral data on a network map.
S0205	Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.
S0207	Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments.
S0208	Skill in determining the physical location of network devices.
S0209	Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.
S0210	Skill in developing intelligence reports.
S0211	Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
S0212	Skill in disseminating items of highest intelligence value in a timely manner.
S0213	Skill in documenting and communicating complex technical and programmatic information.
S0214	Skill in evaluating accesses for intelligence value.
S0215	Skill in evaluating and interpreting metadata.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0216	Skill in evaluating available capabilities against desired effects to provide effective courses of action.
S0217	Skill in evaluating data sources for relevance, reliability, and objectivity.
S0218	Skill in evaluating information for reliability, validity, and relevance.
S0219	Skill in evaluating information to recognize relevance, priority, etc.
S0220	Skill in exploiting/querying organizational and/or partner collection databases.
S0221	Skill in extracting information from packet captures.
S0222	Skill in fusion analysis
S0223	Skill in generating operation plans in support of mission and target requirements.
S0224	Skill in gisting target communications.
S0225	Skill in identifying a target's communications networks.
S0226	Skill in identifying a target's network characteristics.
S0227	Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
S0230	Withdrawn – Integrated into S0066
S0231	Skill in identifying how a target communicates.
S0232	Skill in identifying intelligence gaps and limitations.
S0233	Skill in identifying language issues that may have an impact on organization objectives.
S0234	Skill in identifying leads for target development.
S0235	Skill in identifying non-target regional languages and dialects
S0236	Skill in identifying the devices that work at each level of protocol models.
S0237	Skill in identifying, locating, and tracking targets via geospatial analysis techniques
S0238	Skill in information prioritization as it relates to operations.
S0239	Skill in interpreting compiled and interpretive programming languages.
S0240	Skill in interpreting metadata and content as applied by collection systems.
S0241	Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.
S0242	Skill in interpreting vulnerability scanner results to identify vulnerabilities.
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).
S0244	Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.
S0245	Skill in navigating network visualization software.
S0246	Skill in number normalization.
S0247	Skill in performing data fusion from existing intelligence for enabling new and continued collection.
S0248	Skill in performing target system analysis.
S0249	Skill in preparing and presenting briefings.
S0250	Skill in preparing plans and related correspondence.
S0251	Skill in prioritizing target language material.
S0252	Skill in processing collected data for follow-on analysis.
S0253	Skill in providing analysis on target-related matters (e.g., language, cultural, communications).
S0254	Skill in providing analysis to aid writing phased after action reports.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0255	Skill in providing real-time, actionable geolocation information utilizing target infrastructures.
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.
S0257	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).
S0258	Skill in recognizing and interpreting malicious network activity in traffic.
S0259	Skill in recognizing denial and deception techniques of the target.
S0260	Skill in recognizing midpoint opportunities and essential information.
S0261	Skill in recognizing relevance of information.
S0262	Skill in recognizing significant changes in a target's communication patterns.
S0263	Skill in recognizing technical information that may be used for leads for metadata analysis.
S0264	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).
S0265	Skill in recognizing technical information that may be used for target development including intelligence development.
S0266	Skill in relevant programming languages (e.g., C++, Python, etc.).
S0267	Skill in remote command line and Graphic User Interface (GUI) tool usage.
S0268	Skill in researching essential information.
S0269	Skill in researching vulnerabilities and exploits utilized in traffic.
S0270	Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.
S0271	Skill in reviewing and editing assessment products.
S0272	Skill in reviewing and editing intelligence products from various sources for cyber operations.
S0273	Skill in reviewing and editing plans.
S0274	Skill in reviewing and editing target materials.
S0275	Skill in server administration.
S0276	Skill in survey, collection, and analysis of wireless LAN metadata.
S0277	Skill in synthesizing, analyzing, and prioritizing meaning across data sets.
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
S0279	Skill in target development in direct support of collection operations.
S0280	Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).
S0281	Skill in technical writing.
S0282	Skill in testing and evaluating tools for implementation.
S0283	Skill in transcribing target language communications.
S0284	Skill in translating target graphic and/or voice language materials.
S0285	Skill in using Boolean operators to construct simple and complex queries.
S0286	Skill in using databases to identify target-relevant information.
S0287	Skill in using geospatial data and applying geospatial resources.
S0288	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.).
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.
S0290	Skill in using non-attributable networks.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0291	Skill in using research methods including multiple, different sources to reconstruct a target network.
S0292	Skill in using targeting databases and software packages.
S0293	Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
S0294	Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.
S0295	Skill in using various open source data collection tools (online trade, DNS, mail, etc.).
S0296	Skill in utilizing feedback to improve processes, products, and services.
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
S0298	Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).
S0299	Skill in wireless network target analysis, templating, and geolocation.
S0300	Skill in writing (and submitting) requirements to meet gaps in technical capabilities.
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner.
S0302	Skill in writing effectiveness reports.
S0303	Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
S0304	Skill to access information on current assets available, usage.
S0305	Skill to access the databases where plans/directives/guidance are maintained.
S0306	Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.
S0307	Skill to analyze target or threat sources of strength and morale.
S0308	Skill to anticipate intelligence capability employment requirements.
S0309	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.
S0310	Skill to apply analytical standards to evaluate intelligence products.
S0311	Skill to apply the capabilities, limitations and tasking methodologies of available platforms, sensors, architectures and apparatus as they apply to organization objectives.
S0312	Skill to apply the process used to assess the performance and impact of cyber operations.
S0313	Skill to articulate a needs statement/requirement and integrate new and emerging collection capabilities, accesses and/or processes into collection operations.
S0314	Skill to articulate intelligence capabilities available to support execution of the plan.
S0315	Skill to articulate the needs of joint planners to all-source analysts.
S0316	Skill to associate Intelligence gaps to priority information requirements and observables.
S0317	Skill to compare indicators/observables with requirements.
S0318	Skill to conceptualize the entirety of the intelligence process in the multiple domains and dimensions.
S0319	Skill to convert intelligence requirements into intelligence production tasks.
S0320	Skill to coordinate the development of tailored intelligence products.
S0321	Skill to correlate intelligence priorities to the allocation of intelligence resources/assets.
S0322	Skill to craft indicators of operational progress/success.
S0323	Skill to create and maintain up-to-date planning documents and tracking of services/production.
S0324	Skill to determine feasibility of collection.
S0325	Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Skill ID	Description
S0326	Skill to distinguish between notional and actual resources and their applicability to the plan under development.
S0327	Skill to ensure that the collection strategy leverages all available resources.
S0328	Skill to evaluate factors of the operational environment to objectives, and information requirements.
S0329	Skill to evaluate requests for information to determine if response information exists.
S0330	Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.
S0331	Skill to express orally and in writing the relationship between intelligence capability limitations and decision-making risk and impacts on the overall operation.
S0332	Skill to extract information from available tools and applications associated with collection requirements and collection operations management.
S0333	Skill to graphically depict decision support materials containing intelligence and partner capability estimates.
S0334	Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.
S0335	Skill to identify Intelligence gaps.
S0336	Skill to identify when priority information requirements are satisfied.
S0337	Skill to implement established procedures for evaluating collection management and operations activities.
S0338	Skill to interpret planning guidance to discern level of analytical support required.
S0339	Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.
S0340	Skill to monitor target or threat situation and environmental factors.
S0341	Skill to monitor threat effects to partner capabilities and maintain a running estimate.
S0342	Skill to optimize collection system performance through repeated adjustment, testing, and re-adjustment.
S0343	Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status.
S0344	Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.
S0345	Skill to relate intelligence resources/assets to anticipated intelligence requirements.
S0346	Skill to resolve conflicting collection requirements.
S0347	Skill to review performance specifications and historical information about collection assets.
S0348	Skill to specify collections and/or taskings that must be conducted in the near term.
S0349	Skill to synchronize operational assessment procedures with the critical information requirement process.
S0350	Skill to synchronize planning activities and required intelligence support.
S0351	Skill to translate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.
S0352	Skill to use collaborative tools and environments for collection operations.
S0353	Skill to use systems and/or tools to track collection requirements and determine if they are satisfied.
S0354	Skill in creating policies that reflect the business's core privacy objectives.
S0355	Skill in negotiating vendor agreements and evaluating vendor privacy practices.

Skill ID	Description
S0356	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).
S0357	Skill to anticipate new security threats.
S0358	Skill to remain aware of evolving technical infrastructures.
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.
S0360	Skill to analyze and assess internal and external partner cyber operations capabilities and tools.
S0361	Skill to analyze and assess internal and external partner intelligence processes and the development of information requirements and essential information.
S0362	Skill to analyze and assess internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).
S0363	Skill to analyze and assess internal and external partner reporting.
S0364	Skill to develop insights about the context of an organization's threat environment
S0365	Skill to design incident response for cloud service models.
S0366	Skill to identify successful capabilities to find solutions to less common and more complex system problems.
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
S0368	Skill to use risk scoring to inform performance-based and cost-effective approaches to help organizations to identify, assess, and manage cybersecurity risk.
S0369	Skill to identify sources, characteristics, and uses of the organization's data assets.
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.
S0371	Skill to respond and take local actions in response to threat sharing alerts from service providers.
S0372	Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.
S0373	Skill to ensure that accountability information is collected for information system and information and communications technology supply chain infrastructure components.
S0374	Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

A.7 NICE Framework Ability Descriptions

Table 7 provides a listing of cybersecurity abilities. Ability is competence to perform an observable behavior or a behavior that results in an observable product. Selected ability descriptions from this list are included in each work role in the Detailed work role Listing in Appendix B. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 7 - NICE Framework Ability Descriptions

Ability ID	Description
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
A0002	Ability to match the appropriate knowledge repository technology for a given application or environment.
A0003	Ability to determine the validity of technology trend data.
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
A0005	Ability to decrypt digital data collections.
A0006	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.
A0007	Ability to tailor code analysis for application-specific concerns.
A0008	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]).
A0009	Ability to apply supply chain risk management standards.
A0010	Ability to analyze malware.
A0011	Ability to answer questions in a clear and concise manner.
A0012	Ability to ask clarifying questions.
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
A0014	Ability to communicate effectively when writing.
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A0016	Ability to facilitate small group discussions.
A0017	Ability to gauge learner understanding and knowledge level.
A0018	Ability to prepare and present briefings.
A0019	Ability to produce technical documentation.
A0020	Ability to provide effective feedback to students for improving learning.
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).
A0022	Ability to apply principles of adult learning.
A0023	Ability to design valid and reliable assessments.
A0024	Ability to develop clear directions and instructional materials.
A0025	Ability to accurately define incidents, problems, and events in the trouble ticketing system.
A0026	Ability to analyze test data.
A0027	Ability to apply an organization's goals and objectives to develop and maintain architecture.
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.
A0029	Ability to build complex data structures and high-level programming languages.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Ability ID	Description
A0030	Ability to collect, verify, and validate test data.
A0031	Ability to conduct and implement market research to understand government and industry capabilities and appropriate pricing.
A0032	Ability to develop curriculum for use within a virtual environment.
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.
A0034	Ability to develop, update, and/or maintain standard operating procedures (SOPs).
A0035	Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
A0036	Ability to identify basic common coding flaws at a high level.
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.
A0038	Ability to optimize systems to meet enterprise performance requirements.
A0039	Ability to oversee the development and update of the life cycle cost estimate.
A0040	Ability to translate data and test results into evaluative conclusions.
A0041	Ability to use data visualization tools (e.g., Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).
A0042	Ability to develop career path opportunities.
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.
A0044	Ability to apply programming language structures (e.g., source code review) and logic.
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.
A0046	Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
A0049	Ability to apply secure system design tools, methods and techniques.
A0050	Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.
A0051	Ability to execute technology integration processes.
A0052	Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
A0053	Ability to determine the validity of workforce trend data.
A0054	Ability to apply the Instructional System Design (ISD) methodology.
A0055	Ability to operate common network tools (e.g., ping, traceroute, nslookup).
A0056	Ability to ensure security practices are followed throughout the acquisition process.
A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
A0058	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
A0059	Ability to operate the organization's LAN/WAN pathways.
A0060	Ability to build architectures and frameworks.
A0061	Ability to design architectures and frameworks.
A0062	Ability to monitor measures or indicators of system performance and availability.
A0063	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
A0064	Ability to interpret and translate customer requirements into operational capabilities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Ability ID	Description
A0065	Ability to monitor traffic flows across the network.
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
A0067	Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
A0068	Ability to apply approved planning development and staffing processes.
A0069	Ability to apply collaborative skills and strategies.
A0070	Ability to apply critical reading/thinking skills.
A0071	Ability to apply language and cultural expertise to analysis.
A0072	Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.
A0073	Ability to clearly articulate intelligence requirements into well-formulated research questions and requests for information.
A0074	Ability to collaborate effectively with others.
A0076	Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development.
A0077	Ability to coordinate cyber operations with other organization functions or support activities.
A0078	Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations.
A0079	Ability to correctly employ each organization or element into the collection plan and matrix.
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
A0081	Ability to develop or recommend planning solutions to problems and situations for which no precedent exists.
A0082	Ability to effectively collaborate via virtual teams.
A0083	Ability to evaluate information for reliability, validity, and relevance.
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
A0085	Ability to exercise judgment when policies are not well-defined.
A0086	Ability to expand network access by conducting target analysis and collection to identify targets of interest.
A0087	Ability to focus research efforts to meet the customer's decision-making needs.
A0088	Ability to function effectively in a dynamic, fast-paced environment.
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.
A0090	Ability to identify external partners with common cyber operations interests.
A0091	Ability to identify intelligence gaps.
A0092	Ability to identify/describe target vulnerability.
A0093	Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.
A0095	Ability to interpret and translate customer requirements into operational action.
A0096	Ability to interpret and understand complex and rapidly evolving concepts.
A0097	Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Ability ID	Description
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.
A0099	Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools.
A0100	Ability to perform wireless collection procedures to include decryption capabilities/tools.
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.
A0102	Ability to recognize and mitigate deception in reporting and analysis.
A0103	Ability to review processed target language materials for accuracy and completeness.
A0104	Ability to select the appropriate implant to achieve operational goals.
A0105	Ability to tailor technical and planning information to a customer's level of understanding.
A0106	Ability to think critically.
A0107	Ability to think like threat actors.
A0108	Ability to understand objectives and effects.
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.
A0110	Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
A0112	Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
A0113	Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
A0114	Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
A0115	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
A0116	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.
A0120	Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture.
A0121	Ability to design incident response for cloud service models.
A0122	Ability to design capabilities to find solutions to less common and more complex system problems.
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
A0124	Ability to establish and maintain automated security control assessments
A0125	Ability to author a privacy disclosure statement based on current laws.
A0126	Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
A0127	Ability to deploy continuous monitoring technologies and tools.
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Ability ID	Description
A0129	Ability to ensure information security management processes are integrated with strategic and operational planning processes.
A0130	Ability to ensure that senior officials within the organization provide information security for the information and systems that support the operations and assets under their control.
A0131	Ability to ensure the organization has adequately trained personnel to assist in complying with security requirements in legislation, Executive Orders, policies, directives, instructions, standards, and guidelines.
A0132	Ability to coordinate with senior leadership of an organization to provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization.
A0133	Ability to coordinate with senior leadership of an organization to develop a risk management strategy for the organization providing a strategic view of security-related risks for the organization.
A0134	Ability to coordinate with senior leadership of an organization to facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization.
A0135	Ability to coordinate with senior leadership of an organization to provide oversight for all risk management-related activities across the organization to help ensure consistent and effective risk acceptance decisions.
A0136	Ability to coordinate with senior leadership of an organization to ensure that authorization decisions consider all factors necessary for mission and business success.
A0137	Ability to coordinate with senior leadership of an organization to provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation.
A0138	Ability to coordinate with senior leadership of an organization to promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility.
A0139	Ability to coordinate with senior leadership of an organization to ensure that the shared responsibility for supporting organizational mission/business functions using external providers of systems, services, and applications receives the needed visibility and is elevated to the appropriate decision-making authorities.
A0140	Ability to coordinate with senior leadership of an organization to identify the organizational risk posture based on the aggregated risk from the operation and use of the systems for which the organization is responsible.
A0141	Ability to work closely with authorizing officials and their designated representatives to help ensure that an organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation.
A0142	Ability to work closely with authorizing officials and their designated representatives to help ensure that security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles.
A0143	Ability to work closely with authorizing officials and their designated representatives to help ensure that organizational systems and common controls are covered by approved security plans and possess current authorizations.
A0144	Ability to work closely with authorizing officials and their designated representatives to help ensure that security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner.
A0145	Ability to work closely with authorizing officials and their designated representatives to help ensure that there is centralized reporting of security-related activities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Ability ID	Description
A0146	Ability to establish the rules for appropriate use and protection of the information and retains that responsibility even when the information is shared with or provided to other organizations.
A0147	Ability to approve security plans, memorandums of agreement or understanding, plans of action and milestones, and determine whether significant changes in the systems or environments of operation require reauthorization.
A0148	Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls.
A0149	Ability, in close coordination with system security officers, advise authorizing officials, chief information officers, senior information security officers, and the senior accountable official for risk management/risk executive (function), on a range of security-related issues (e.g. establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches; security alerts; and potential adverse effects of identified vulnerabilities).
A0150	Ability to conduct systems security engineering activities (NIST SP 800-16).
A0151	Ability to capture and refine security requirements and ensure that the requirements are effectively integrated into the component products and systems through purposeful security architecting, design, development, and configuration.
A0152	Ability to employ best practices when implementing security controls within a system including software engineering methodologies; system and security engineering principles; secure design, secure architecture, and secure coding techniques.
A0153	Ability to coordinate their security-related activities with security architects, senior information security officers, system owners, common control providers, and system security officers.
A0154	Ability to conduct a comprehensive assessment of the management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine the effectiveness of the controls (i.e., the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).
A0155	Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
A0156	Ability to prepare the final security assessment report containing the results and findings from the assessment.
A0157	Ability to assesses a security plan to help ensure that the plan provides a set of security controls for the system that meet the stated security requirements.
A0158	Ability to ensure that functional and security requirements are appropriately addressed in a contract and that the contractor meets the functional and security requirements as stated in the contract.
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
A0160	Ability to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.

Ability ID	Description
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).
A0162	Ability to ensure information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition/review and are involved in, or approve of, each milestone decision through the entire system life cycle for systems.
A0162	Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy.
A0163	Ability to interpret Communications Security (COMSEC) terminology, guidelines and procedures.
A0164	Ability to identify the roles and responsibilities for appointed Communications Security (COMSEC) personnel.
A0165	Ability to manage Communications Security (COMSEC) material accounting, control and use procedure.
A0166	Ability to identify types of Communications Security (COMSEC) Incidents and how they’re reported
A0167	Ability to recognize the importance of auditing Communications Security (COMSEC) material and accounts.
A0168	Ability to Identify the requirements of In-Process accounting for Communications Security (COMSEC)
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.
A0171	Ability to conduct training and education needs assessment.
A0172	Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks.
A0173	Ability to recognize that changes to systems or environment can change residual risks in relation to risk appetite.
A0174	Ability to Find and navigate the dark web using the TOR network to locate markets and forums.
A0175	Ability to examine digital media on multiple operating system platforms.
A0176	Ability to maintain databases. (i.e., backup, restore, delete data, transaction log files, etc.).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix B – Work Role Detail Listing

This appendix provides a detailed description of each NICE Framework work role. For each work role, the listing below provides the following information:

- The work role name;
- A unique NICE Framework work role ID, based upon abbreviations of the NICE Framework Category and Specialty Area to which that work role belongs;
- The Specialty Area in which the work role resides;
- The Category in which the work role resides;
- A description of the work role;
- A list of the NICE Framework Tasks that a person in a cybersecurity position that includes the work role might be expected to perform;
- A list of the NICE Framework Knowledge areas that a person in a cybersecurity position that includes the work role might be expected to exhibit;
- A list of the NICE Framework Skills that a person in a cybersecurity position that includes the work role might be expected to possess; and
- A list of the NICE Framework Abilities that a person in a cybersecurity position that includes the work role might be expected to demonstrate.

The following tables describe the NICE Framework work roles with a simple listing of tasks, knowledge, skills, and abilities. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4]. The Reference Spreadsheet provide more verbose listings of the tasks, knowledge, skills, abilities. The work roles will be updated periodically [1].

B.1 Securely Provision (SP)

Work Role Name	**Authorizing Official**
Work Role ID	**SP-RSK-001**
Specialty Area	**Risk Management (RSK)**
Category	**Securely Provision (SP)**
Work Role Description	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).
Tasks	T0145, T0221, T0371, T0495
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Skills	S0034, S0367
Abilities	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Security Control Assessor**
Work Role ID	**SP-RSK-002**
Specialty Area	**Risk Management (RSK)**
Category	**Securely Provision (SP)**
Work Role Description	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).
Tasks	T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624
Skills	S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374
Abilities	A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170

Work Role Name	**Software Developer**
Work Role ID	**SP-DEV-001**
Specialty Area	**Software Development (DEV)**
Category	**Securely Provision (SP)**
Work Role Description	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
Skills	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
Abilities	A0007, A0021, A0047, A0123, A0170

Work Role Name	**Secure Software Assessor**
Work Role ID	**SP-DEV-002**
Specialty Area	**Software Development (DEV)**
Category	**Securely Provision (SP)**
Work Role Description	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624
Skills	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367
Abilities	A0021, A0123, A0170

Work Role Name	**Enterprise Architect**
Work Role ID	**SP-ARC-001**
Specialty Area	**Systems Architecture (ARC)**
Category	**Securely Provision (SP)**
Work Role Description	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.
Tasks	T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0027, K0028, K0030, K0035, K0037, K0043, K0044, K0052, K0056, K0060, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0102, K0170, K0179, K0180, K0198, K0200, K0203, K0207, K0211, K0212, K0214, K0227, K0240, K0264, K0275, K0286, K0287, K0291, K0293, K0299, K0322, K0323, K0325, K0326, K0332, K0333, K0487, K0516
Skills	S0005, S0024, S0027, S0050, S0060, S0122, S0367, S0374
Abilities	A0008, A0015, A0027, A0038, A0051, A0060, A0123, A0170

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Security Architect**
Work Role ID	**SP-ARC-002**
Specialty Area	**Systems Architecture (ARC)**
Category	**Securely Provision (SP)**
Work Role Description	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
Tasks	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0374, K0565
Skills	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
Abilities	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

Work Role Name	**Research and Development Specialist**
Work Role ID	**SP-TRD-001**
Specialty Area	**Technology R&D (TRD)**
Category	**Securely Provision (SP)**
Work Role Description	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
Tasks	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499
Skills	S0005, S0017, S0072, S0140, S0148, S0172
Abilities	A0001, A0018, A0019, A0170

Work Role Name	**Systems Requirements Planner**
Work Role ID	**SP-SRP-001**
Specialty Area	**Systems Requirements Planning (SRP)**
Category	**Securely Provision (SP)**
Work Role Description	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
Tasks	T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622
Skills	S0005, S0006, S0008, S0010, S0050, S0134, S0367
Abilities	A0064, A0123, A0170

Work Role Name	**System Test & Evaluation Specialist**
Work Role ID	**SP-TST-001**
Specialty Area	**Test and Evaluation (TST)**
Category	**Securely Provision (SP)**
Work Role Description	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
Tasks	T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332
Skills	S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367
Abilities	A0026, A0030, A0040, A0123

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Information Systems Security Developer**
Work Role ID	**SP-SYS-001**
Specialty Area	**Systems Development (SYS)**
Category	**Securely Provision (SP)**
Work Role Description	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Skills	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160, S0367
Abilities	A0001, A0008, A0012, A0013, A0015, A0019, A0026, A0040, A0048, A0049, A0050, A0056, A0061, A0074, A0089, A0098, A0108, A0119, A0123, A0170

Work Role Name	**Systems Developer**
Work Role ID	**SP-SYS-002**
Specialty Area	**Systems Development (SYS)**
Category	**Securely Provision (SP)**
Work Role Description	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Skills	S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367
Abilities	A0123, A0170

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.2 Operate and Maintain (OM)

Work Role Name	**Database Administrator**
Work Role ID	**OM-DTA-001**
Specialty Area	**Data Administration (DTAA)**
Category	**Operate and Maintain (OM)**
Work Role Description	Administers databases and/or data management systems that allow for the secure storage, query, and utilization of data.
Tasks	T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420
Skills	S0002, S0013, S0037, S0042, S0045
Abilities	A0176

Work Role Name	**Data Analyst**
Work Role ID	**OM-DTA-002**
Specialty Area	**Data Administration (DTA)**
Category	**Operate and Maintain (OM)**
Work Role Description	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
Tasks	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
Skills	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
Abilities	A0029, A0035, A0036, A0041, A0066

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Knowledge Manager**
Work Role ID	**OM-KMG-001**
Specialty Area	**Knowledge Management (KMG)**
Category	**Operate and Maintain (OM)**
Work Role Description	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
Tasks	T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420
Skills	S0011, S0012, S0049, S0055
Abilities	A0002

Work Role Name	**Technical Support Specialist**
Work Role ID	**OM-STS-001**
Specialty Area	**Customer Service and Technical Support (STS)**
Category	**Operate and Maintain (OM)**
Work Role Description	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).
Tasks	T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330
Skills	S0039, S0058, S0142, S0159, S0365
Abilities	A0025, A0034, A0122

Work Role Name	**Network Operations Specialist**
Work Role ID	**OM-NET-001**
Specialty Area	**Network Services (NET)**
Category	**Operate and Maintain (OM)**
Work Role Description	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Tasks	T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622
Skills	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
Abilities	A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159

Work Role Name	**System Administrator**
Work Role ID	**OM-ADM-001**
Specialty Area	**Systems Administration (ADM)**
Category	**Operate and Maintain (OM)**
Work Role Description	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
Tasks	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
Skills	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Abilities	S0154, S0158

Work Role Name	**Systems Security Analyst**
Work Role ID	**OM-ANA-001**
Specialty Area	**Systems Analysis (ANA)**
Category	**Operate and Maintain (OM)**
Work Role Description	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0019, K0024, K0035, K0036, K0040, K0044, K0049, K0052, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0333, K0339
Skills	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167, S0367
Abilities	A0015, A0123

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.3 Oversee and Govern (OV)

Work Role Name	**Cyber Legal Advisor**
Work Role ID	**OV-LGA-001**
Specialty Area	**Legal Advice and Advocacy (LGA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Provides legal advice and recommendations on relevant topics related to cyber law.
Tasks	T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
Skills	S0356
Abilities	A0046

Work Role Name	**Privacy Officer/Privacy Compliance Manager**
Work Role ID	**OV-LGA-002**
Specialty Area	**Legal Advice and Advocacy (LGA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
Tasks	T0003, T0004, T0029, T0930, 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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0612, K0613, K0614, K0615
Skills	S0354, S0355, S0356
Abilities	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115, A0125

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Cyber Instructional Curriculum Developer**
Work Role ID	**OV-TEA-001**
Specialty Area	**Training, Education, and Awareness (TEA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
Tasks	T0230, T0247, T0248, T0249, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628
Skills	S0064, S0066, S0070, S0102, S0166, S0296
Abilities	A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Work Role Name	**Cyber Instructor**
Work Role ID	**OV-TEA-002**
Specialty Area	**Training, Education, and Awareness (TEA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Develops and conducts training or education of personnel within cyber domain.
Tasks	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
Skills	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
Abilities	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Information Systems Security Manager**
Work Role ID	**OV-MGT-001**
Specialty Area	**Cybersecurity Management (MGT)**
Category	**Oversee and Govern (OV)**
Work Role Description	Responsible for the cybersecurity of a program, organization, system, or enclave.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
Skills	S0018, S0027, S0086
Abilities	A0128, A0161, A0170

Work Role Name	**Communications Security (COMSEC) Manager**
Work Role ID	**OV-MGT-002**
Specialty Area	**Cybersecurity Management (MGT)**
Category	**Oversee and Govern (OV)**
Work Role Description	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
Tasks	T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622
Skills	S0027, S0059, S0138
Abilities	A0162, A0163, A0164, A0165, A0166, A0167, A0168

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Cyber Workforce Developer and Manager**
Work Role ID	**OV-SPP-001**
Specialty Area	**Strategic Planning and Policy (SPP)**
Category	**Oversee and Govern (OV)**
Work Role Description	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.
Tasks	T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
Skills	S0108, S0128
Abilities	A0023, A0028, A0033, A0037, A0042, A0053

Work Role Name	**Cyber Policy and Strategy Planner**
Work Role ID	**OV-SPP-002**
Specialty Area	**Strategic Planning and Policy Development (SPP)**
Category	**Oversee and Govern (OV)**
Work Role Description	Develops and maintains cybersecurity plans, strategy and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
Tasks	T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624
Skills	S0176, S0250
Abilities	A0003, A0033, A0037

Work Role Name	**Executive Cyber Leadership**
Work Role ID	**OV-EXL-001**
Specialty Area	**Executive Cyber Leadership (EXL)**
Category	**Oversee and Govern (OV)**
Work Role Description	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
Tasks	T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628
Skills	S0018, S0356, S0357, S0358, S0359
Abilities	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Program Manager**
Work Role ID	**OV-PMA-001**
Specialty Area	**Program/Project Management and Acquisition (PMA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
Tasks	T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Skills	S0038, S0372
Abilities	A0009, A0039, A0045, A0056,

Work Role Name	**Information Technology (IT) Project Manager**
Work Role ID	**OV-PMA-002**
Specialty Area	**Program/Project Management and Acquisition (PMA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Directly manages information technology projects.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Skills	S0038, S0372
Abilities	A0009, A0039, A0045, A0056

Work Role Name	**Product Support Manager**
Work Role ID	**OV-PMA-003**
Specialty Area	**Program/Project Management and Acquisition (PMA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Tasks	T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
Skills	S0038, S0372
Abilities	A0009, A0031, A0039, A0045, A0056

Work Role Name	**IT Investment/Portfolio Manager**
Work Role ID	**OV-PMA-004**
Specialty Area	**Program/Project Management and Acquisition (PMA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
Tasks	T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270
Skills	S0372
Abilities	A0039

Work Role Name	**IT Program Auditor**
Work Role ID	**OV-PMA-005**
Specialty Area	**Program/Project Management and Acquisition (PMA)**
Category	**Oversee and Govern (OV)**
Work Role Description	Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.
Tasks	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
Skills	S0038, S0085, S0372
Abilities	A0056

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.4 Protect and Defend (PR)

Work Role Name	**Cyber Defense Analyst**
Work Role ID	**PR-CDA-001**
Specialty Area	**Cyber Defense Analysis (CDA)**
Category	**Protect and Defend (PR)**
Work Role Description	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.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

Work Role Name	**Cyber Defense Infrastructure Support Specialist**
Work Role ID	**PR-INF-001**
Specialty Area	**Cyber Defense Infrastructure Support (INF)**
Category	**Protect and Defend (PR)**
Work Role Description	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
Tasks	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058. K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334
Skills	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367
Abilities	A0123

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Cyber Defense Incident Responder**
Work Role ID	**PR-CIR-001**
Specialty Area	**Incident Response (CIR)**
Category	**Protect and Defend (PR)**
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Abilities	A0121, A0128

Work Role Name	**Vulnerability Assessment Analyst**
Work Role ID	**PR-VAM-001**
Specialty Area	**Vulnerability Assessment and Management (VAM)**
Category	**Protect and Defend (PR)**
Work Role Description	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.
Tasks	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
Skills	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
Abilities	A0001, A0044, A0120, A0123

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.5 Analyze (AN)

Work Role Name	**Threat/Warning Analyst**
Work Role ID	**AN-TWA-001**
Specialty Area	**Warning/Threat Analysis (TWA)**
Category	**Analyze (AN)**
Work Role Description	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614
Skills	S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303
Abilities	A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

Work Role Name	**Exploitation Analyst**
Work Role ID	**AN-EXP-001**
Specialty Area	**Exploitation Analysis (EXP)**
Category	**Analyze (AN)**
Work Role Description	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.
Tasks	T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608
Skills	S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300
Abilities	A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104

Work Role Name	**All-Source Analyst**
Work Role ID	**AN-ASA-001**
Specialty Area	**All-Source Analysis (ASA)**
Category	**Analyze (AN)**
Work Role Description	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.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0362, K0444, K0471, K0560, K0377, K0392, K0395, K0405, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0480, K0511, K0516, K0556, K0561, K0565, K0603, K0604, K0610, K0612, K0614, K0357, K0410, K0457, K0465, K0507, K0533, K0542, K0549, K0551, K0577, K0598
Skills	S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360
Abilities	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

Work Role Name	**Mission Assessment Specialist**
Work Role ID	**AN-ASA-002**
Specialty Area	**All-Source Analysis (ASA)**
Category	**Analyze (AN)**
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, T0589, 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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614
Skills	S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360
Abilities	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Target Developer**
Work Role ID	**AN-TGT-001**
Specialty Area	**Targets (TGT)**
Category	**Analyze (AN)**
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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0142, K0349, K0362, K0444, K0471, K0560, K0392, K0395, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0460, K0464, K0516, K0556, K0561, K0565, K0603, K0604, K0614, K0457, K0465, K0507, K0549, K0551, K0598, K0417, K0458, K0357, K0533, K0542, K0351, K0379, K0473, K0381, K0402, K0413, K0426, K0439, K0461, K0466, K0478, K0479, K0497, K0499, K0543, K0546, K0547, K0555
Skills	S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361
Abilities	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Work Role Name	**Target Network Analyst**
Work Role ID	**AN-TGT-002**
Specialty Area	**Targets (TGT)**
Category	**Analyze (AN)**
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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600
Skills	S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301
Abilities	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Work Role Name	**Multi-Disciplined Language Analyst**
Work Role ID	**AN-LNG-001**
Specialty Area	**Language Analysis (LNG)**
Category	**Analyze (AN)**
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, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, TO860
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607
Skills	S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284
Abilities	A0013, A0089, A0071, A0103

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.6 Collect and Operate (CO)

Work Role Name	**All Source-Collection Manager**
Work Role ID	**CO-CLO-001**
Specialty Area	**Collection Operations (CLO)**
Category	**Collect and Operate (CO)**
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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
Skills	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362
Abilities	A0069, A0070, A0076, A0078, A0079

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**All Source-Collection Requirements Manager**
Work Role ID	**CO-CLO-002**
Specialty Area	**Collection Operations (CLO)**
Category	**Collect and Operate (CO)**
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, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612
Skills	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362
Abilities	A0069, A0070, A0078

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Cyber Intel Planner**
Work Role ID	**CO-OPL-001**
Specialty Area	**Cyber Operational Planning (OPL)**
Category	**Collect and Operate (CO)**
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	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602
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, S0360
Abilities	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Work Role Name	**Cyber Ops Planner**
Work Role ID	**CO-OPL-002**
Specialty Area	**Cyber Operational Planning (OPL)**
Category	**Collect and Operate (CO)**
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	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	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565 K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614
Skills	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360
Abilities	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Work Role Name	**Partner Integration Planner**
Work Role ID	**CO-OPL-003**
Specialty Area	**Cyber Operational Planning (OPL)**
Category	**Collect and Operate (CO)**
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	T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599
Skills	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360
Abilities	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Work Role Name	**Cyber Operator**
Work Role ID	**CO-OPS-001**
Specialty Area	**Cyber Operations (OPS)**
Category	**Collect and Operate (CO)**
Work Role Description	Conducts collection, processing, and/or geolocation of systems 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	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
Skills	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
Abilities	A0095, A0097, A0099, A0100

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

B.7 Investigate (IN)

Work Role Name	**Cyber Crime Investigator**
Work Role ID	**IN-INV-001**
Specialty Area	**Cyber Investigation (INV)**
Category	**Investigate (IN)**
Work Role Description	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
Tasks	[**Note**: Several of these activities may only to be conducted by personnel with a Law Enforcement or Counter Intelligence Authority.] T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, K0624
Skills	S0047, S0068, S0072, S0086
Abilities	A0174, A0175

Work Role Name	**Law Enforcement/Counterintelligence Forensics Analyst**
Work Role ID	**IN-FOR-001**
Specialty Area	**Digital Forensics (FOR)**
Category	**Investigate (IN)**
Work Role Description	Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
Tasks	T0059, T0096, T0220, T0308, T0398, T0419, T0401, T0403, T0411, T0425
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, 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, K0305, K0624
Skills	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
Abilities	A0005, A0175

Work Role Name	**Cyber Defense Forensics Analyst**
Work Role ID	**IN-FOR-002**
Specialty Area	**Digital Forensics (FOR)**
Category	**Investigate (IN)**
Work Role Description	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Tasks	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, 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, K0624
Skills	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
Abilities	A0005, A0043

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix C – Workforce Development Tools

C.1 DHS Cybersecurity Workforce Development Toolkit

The DHS Cybersecurity Workforce Development Toolkit (CWDT) [8] helps any organization understand its cybersecurity workforce and staffing needs to protect its information, customers, and networks. This toolkit includes cybersecurity career path templates and recruitment resources to recruit and retain top cybersecurity talent. The CWDT provides tools to help understand an organization's cybersecurity workforce risks and take inventory of an organization's workforce. CWDT tools leverage the specialty areas and KSAs and Tasks in the NICE Framework. CWDT notes that the first step in preparing to build a cybersecurity workforce is a shared vision for organizing one's cybersecurity workforce. Having a shared vision supports leaders as they respond to changing environments and provides 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 an organization to evaluate the maturity of its cybersecurity workforce planning capability.

The (CWDT) offers profiles as a guide to focus on retaining staff at every level whether entry-level, mid-career, or seasoned cybersecurity professionals.

C.1.1 Proficiency Levels and Career Paths

Developing and sharing career paths with employees will help them identify their proficiency levels and advance in cybersecurity career paths.

The CWDT includes a three-step process to develop cybersecurity career paths for one's organization.

- Step 1 – Familiarize yourself with proficiency levels and review sample career paths.
- Step 2 – Use a CWDT template to create custom cybersecurity-specific career paths for your organization filling in "*Suggested Experience & Credentials,*" "*Competencies and Sample Skills / KSAs,*" and "*Suggested Training & Development Activities.*"
- Step 3 – Share career paths with cybersecurity managers and staff.

C.2 Baldrige Cybersecurity Excellence Builder Tool

Once an organization has determined its cybersecurity requirements (such as through a cybersecurity audit or an internal self-assessment), it can reference the NICE Framework to identify the work roles and tasks that will help fulfill those requirements. While general terms, such as "cyber professionals," have historically been used to measure needs, the specificity provided by the NICE Framework provides a better approach to describe the dozens of discrete job functions needed. By identifying the required and available competencies, and by identifying gaps between required and available skills, the organization can identify critical needs. The NICE Framework helps an organization to answer the following questions, drawn from the Baldrige Cybersecurity Excellence Builder Tool [9], 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?

As more organizations assess their cybersecurity workforce, the common lexicon in the NICE Framework enables capacity and capability assessment across multiple organizations, industry sectors, and regions.

C.3 Position Description Drafting Tool

The DHS Cyberskills Management Support Initiative PushbuttonPD Tool [10] 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. Any organization can experiment with the PushbuttonPD Tool to see how it pulls NICE Framework material into a job description.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix D – Cross Reference to Guidance and Guideline Documents

NICE Strategic Goal #3 Guide Career Development and Workforce Planning aims to support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent. One objective within this strategic goal is to publish and raise awareness of the NICE Framework and encourage adoption. Adoption in this case means that the NICE Framework is used as a reference resource for actions related to cybersecurity workforce, training, and education.

One way to encourage adoption of the NICE Framework is to push authors of cybersecurity guidance or guideline documents to cross reference some of the content of those documents to components in the NICE Framework. Appendix D includes examples of publication cross referencing that could encourage adoption of the NICE Framework.

D.1 Cybersecurity Framework

In 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity [11], commonly referred to as the Cybersecurity Framework. Developed in response to Executive Order (EO) 13636 [12], the Cybersecurity Framework provides 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.

A companion document to the Cybersecurity Framework, the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* [13] 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 Cybersecurity Framework consists of three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Each Cybersecurity Framework component reinforces the connection between business drivers and cybersecurity activities. The Framework Core 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 detail below.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and 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, helps 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 represent the cross-sector guidance most frequently referenced during the Framework development process.

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 NICE Framework Categories. Table 8 describes the relationships among the Cybersecurity Framework Functions and NICE Framework Categories.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Table 8 - Crosswalk of NICE Framework Workforce Categories to Cybersecurity Framework Functions

NICE Framework Category	Category Description	Related Cybersecurity Framework Function(s)
Securely Provision (SP)	Conceptualizes, designs, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	Identify (ID), Protect (PR)
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	Protect (PR), Detect (DE)
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so that the organization may effectively conduct cybersecurity work.	Identify (ID), Protect (PR), Detect (DE), Recover (RC)
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Protect (PR), Detect (DE), Respond (RS)
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	Identify (ID), Detect (DE), Respond (RS)
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	Detect (DE), Protect (PR), Respond (RS)
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Detect (DE), Respond (RS), Recover (RC)

D.1.2 Example Integration of Cybersecurity Framework with NICE Framework

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

Cybersecurity Framework's **Respond** Function includes a **Mitigation (RS.MI)** Category. The Category includes a Subcategory, **RS.MI-2,** pointing to an outcome of, "Incidents are mitigated." While Cybersecurity Framework describes this outcome, and provides several informative references regarding the security controls to achieve it, Cybersecurity Framework does not provide any informative guidance regarding who should be responsible for attaining the outcome, or what KSAs would apply.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Reviewing the NICE Framework, 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 Cybersecurity Framework **RS.MI-2** 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 Cybersecurity Framework 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; identify 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).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

- **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.
- **T0164** - 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 Cybersecurity Framework
RS.MI-2 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.

D.2 Systems Security Engineering

NIST Special Publication (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [14], addresses the engineering-driven actions necessary to develop more defensible and survivable systems—including the components that compose those systems and the services that depend on them. It starts with and builds upon a set of well-established International Standards for systems and software engineering, and infuses systems security engineering techniques, methods, and practices into those systems and software engineering activities. The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective, and to use established engineering processes to ensure that such requirements and needs are addressed with the appropriate fidelity and rigor across the entire life cycle of the system. Increasing the trustworthiness of systems is a significant undertaking that requires a substantial investment in the requirements, architecture, design, and development of systems, components, applications, and networks—and a fundamental cultural change to the current “business as usual” approach.

Introducing a disciplined, structured, and standards-based set of systems security engineering activities and tasks provides an important starting point and forcing function to initiate needed

change. The ultimate objective is to obtain trustworthy secure systems that are fully capable of supporting critical missions and business operations while protecting stakeholder assets, and to do so with a level of assurance that is consistent with the risk tolerance of those stakeholders.

Mapping components of the NICE Framework to the specialty discipline described in NIST SP 800-160 will validate those components. Practitioners of the system security engineering specialty discipline will likely become subject matter experts who can justify additional KSAs and tasks to be added to the NICE Framework.

D.3 U.S. Office of Personnel Management Federal Cybersecurity Codes

On January 4, 2017, the U.S. Office of Personnel Management (OPM) issued a memorandum [15] titled “Guidance for federal agencies assigning new cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions”. The memorandum notes that the Federal Cybersecurity Workforce Assessment Act of 2015 [16] requires OPM to establish procedures to implement the NICE coding structure and to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions. Table 9 shows the mapping of NICE Framework Work Role IDs which represent the interdisciplinary nature of cybersecurity work to OPM cybersecurity codes which are compatible with the OPM Enterprise Human Resources Integration system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Table 9 – Crosswalk of Work Role IDs to OPM Cybersecurity Codes

Work Role ID	OPM Code	Work Role ID	OPM Code	Work Role ID	OPM Code
SP-RSK-001	611	OV-LGA-001	731	AN-TWA-001	141
SP-RSK-002	612	OV-LGA-002	732	AN-EXP-001	121
SP-DEV-001	621	OV-TEA-001	711	AN-ASA-001	111
SP-DEV-002	622	OV-TEA-002	712	AN-ASA-002	112
SP-ARC-001	651	OV-MGT-001	722	AN-TGT-001	131
SP-ARC-002	652	OV-MGT-002	723	AN-TGT-002	132
SP-TRD-001	661	OV-SPP-001	751	AN-LNG-001	151
SP-SRP-001	641	OV-SPP-002	752	CO-CLO-001	311
SP-TST-001	671	OV-EXL-001	901	CO-CLO-002	312
SP-SYS-001	631	OV-PMA-001	801	CO-OPL-001	331
SP-SYS-002	632	OV-PMA-002	802	CO-OPL-002	332
OM-DTA-001	421	OV-PMA-003	804	CO-OPL-003	333
OM-DTA-002	422	OV-PMA-004	804	CO-OPS-001	321
OM-KMG-001	431	OV-PMA-005	805	IN-INV-001	221
OM-STS-001	411	PR-CDA-001	511	IN-FOR-001	211
OM-NET-001	441	PR-INF-001	521	IN-FOR-002	212
OM-ADM-001	451	PR-CIR-001	531		
OM-ANA-001	461	PR-VAM-001	541		

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix E – Acronyms

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

API	Application programming interface
CDM	Continuous Diagnostics and Mitigation
CDS	Cross-Domain Solutions
CIO	Chief Information Officer
CKMS	Crypto Key Management System
CMMI	Capability Maturity Model Integration
CMS	Content Management System
CNSSI	Committee on National Security Systems Instruction
COMSEC	Communications Security
COTR	Contracting Officer's Technical Representative
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
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
SOP	Standard operating procedures

SQL	Structured query language
TCP	Transmission Control Protocol
TTP	Tactics, techniques, and procedures
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

Appendix F– References

[1] NICE Framework Revision webpage, National Institute of Standards and Technology [Website], https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework/revisions

[2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0*, https://www.nist.gov/file/359276

[3] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, https://www.nist.gov/file/359261

[4] Reference Spreadsheet for NIST Special Publication 800-181 https://www.nist.gov/file/372581

[5] NICE Framework, National Institute of Standards and Technology [Website], https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[6] U.S. Department of Labor, Employment and Training Administration (ETA) [Website]. https://www.doleta.gov

[7] Competency Model Clearinghouse, Cybersecurity Competency Model, https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[8] U.S. Department of Homeland Security, Cybersecurity Workforce Development Toolkit (CWDT), https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

[9] Baldrige Cybersecurity Excellence Program, National Institute of Standards and Technology [Website], https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[10] U.S. Department of Homeland Security, CMSI PushButtonPD™ Tool Website, https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[11] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, National Institute of Standards and Technology February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[12] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[13] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[14] NIST Special Publication (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, November 2016, https://doi.org/10.6028/NIST.SP.800-160

[15] Memorandum on Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions, January 2017, https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity

[16] H.R.2029 - Consolidated Appropriations Act, 2016 which contains Division N-Cybersecurity Act of 2015, https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181