National Initiative for Cybersecurity Education

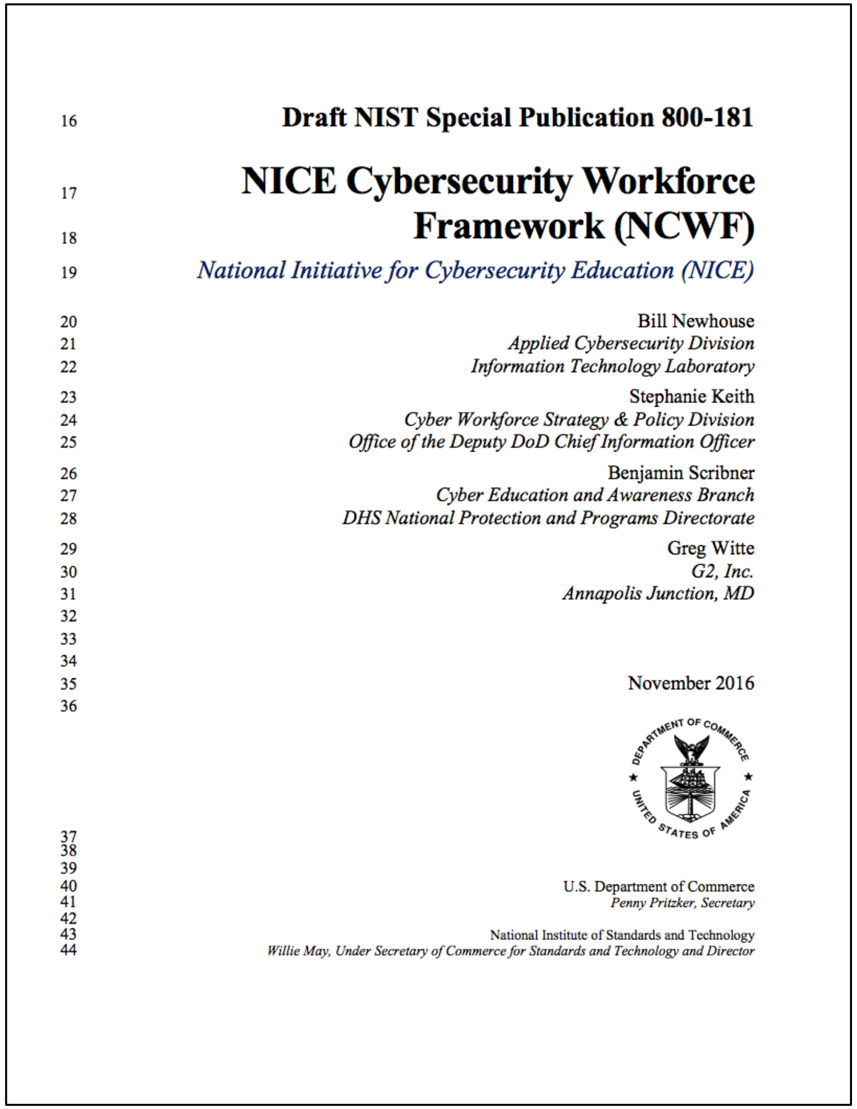
NIST Special Publication, 800-181

NICE Cybersecurity Workforce Framework

Douglas Rausch
Cybersecurity Program Director, Bellevue University
Lead Skills-based Training & Performance-based
Certification and Range sub-group

A Little History

- Version 1.0 (an interactive pdf and website)
  - posted April 2013
- Version 2.0 (a spreadsheet)
  - posted May 2014
- Draft NIST SP 800-181
  - posted Nov 2016, comments were taken through Jan 6, 2017



Draft NIST Special Publication 800-181

NICE Cybersecurity Workforce Framework (NCWF)

National Initiative for Cybersecurity Education (NICE)

Bill Newhouse
Applied Cybersecurity Division
Information Technology Laboratory

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

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

Greg Witte
G2, Inc.
Annapolis Junction, MD

November 2016

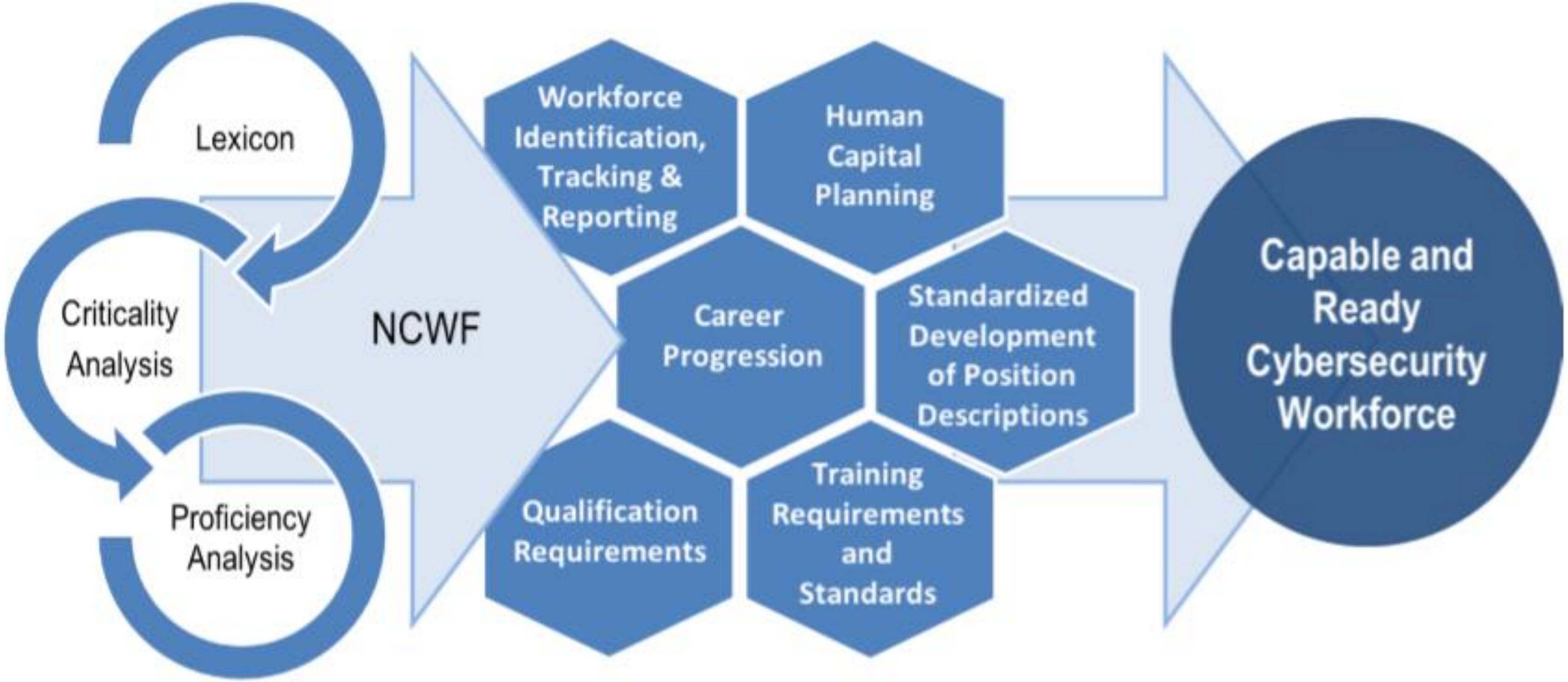
U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Drafting Team

- NICE Program Office
- Cyber Workforce Division in the Office of the Deputy DoD Chief Information Officer – Cybersecurity
- Cybersecurity Education and Awareness Branch, Stakeholder Engagement and Cyber Infrastructure Resilience Division, Department of Homeland Security
- OPM
- (and a cast of thousands, or at least hundreds/tens)

NIST – NICE Framework Version 3.0

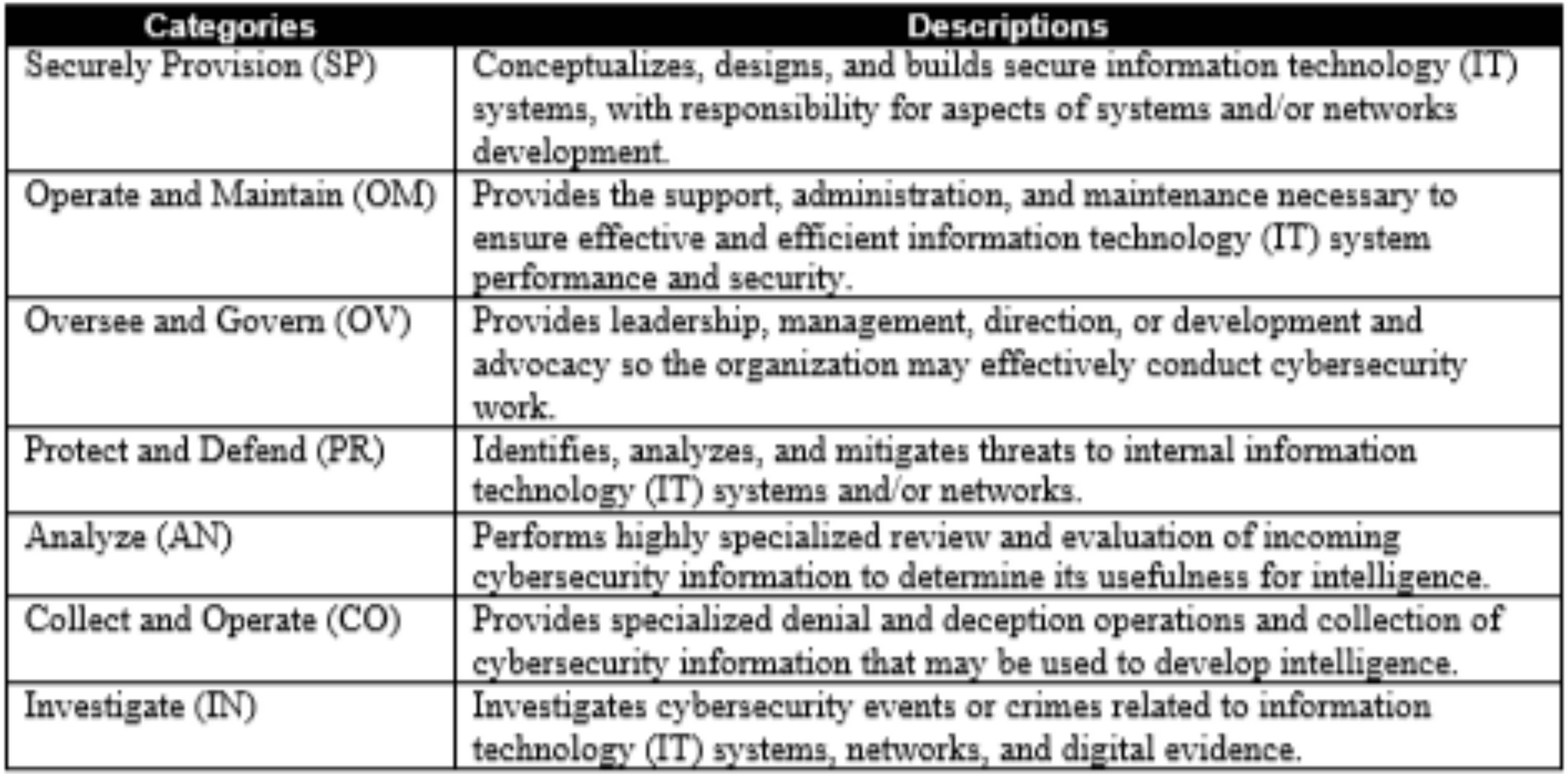

Lexicon
Criticality Analysis
Proficiency Analysis
NCWF
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Cybersecurity Workforce

The publication

- Organizes cybersecurity work into seven high level categories and over 50 Work Roles within those seven Categories
- NEW: Offers a superset of Tasks for each Work Role
- NEW: Offers a superset list of Knowledge, Skills, and Abilities (KSAs) for each work role

Categories

A high-level grouping of common cybersecurity functions

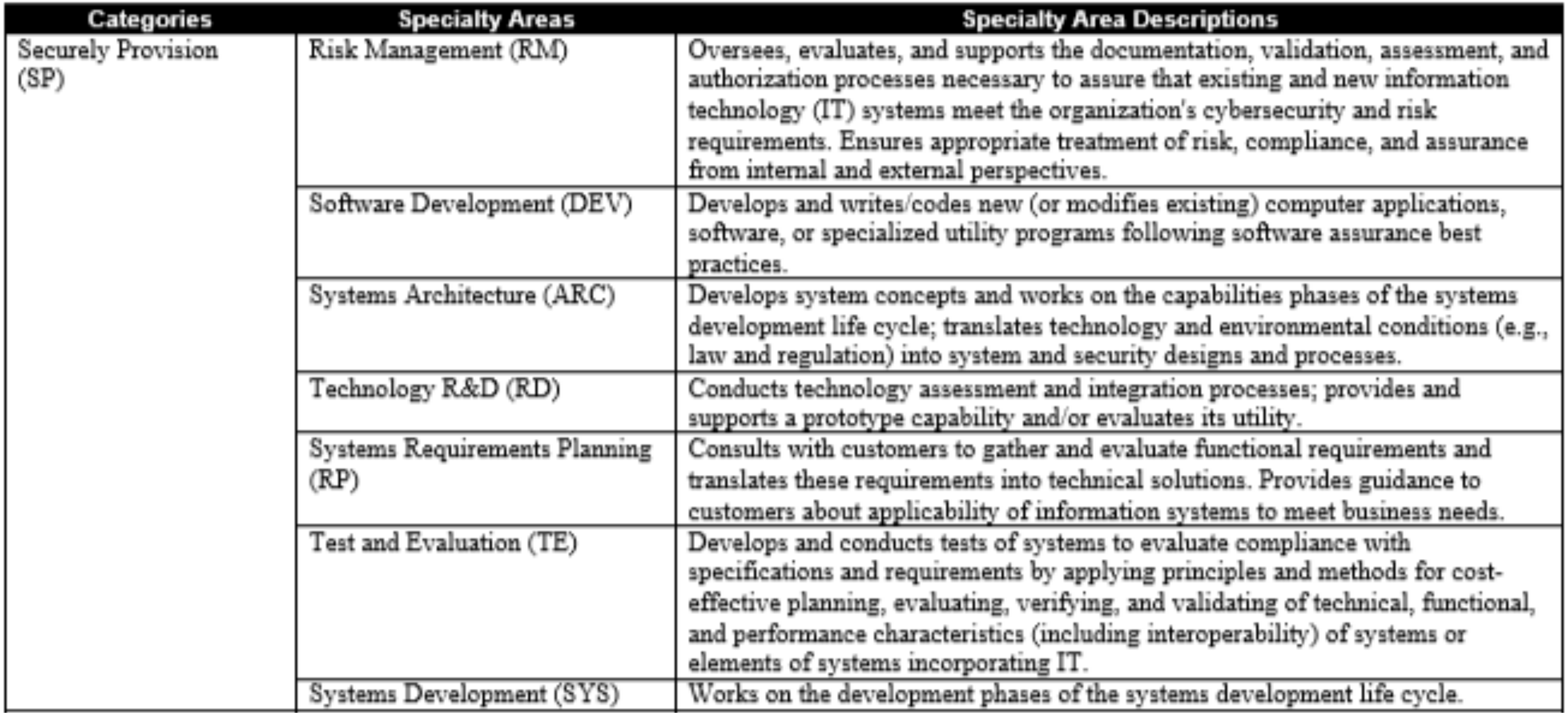


Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective 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.

Specialty Areas

- Specialty Areas are groupings of cybersecurity work
    - 31 Specialty Areas callout out in NCWF version 1.0 and 32 in NCWF version 2.0, 35 in version 3.0
- Each specialty area represents an area of concentrated work, or function, within cybersecurity
    - Previous versions of the NCWF provided broader and less defined Tasks and Knowledge, Skills and Abilities (KSAs)
- SP 800-181 connects Tasks and KSAs with the Work Roles

Specialty Areas

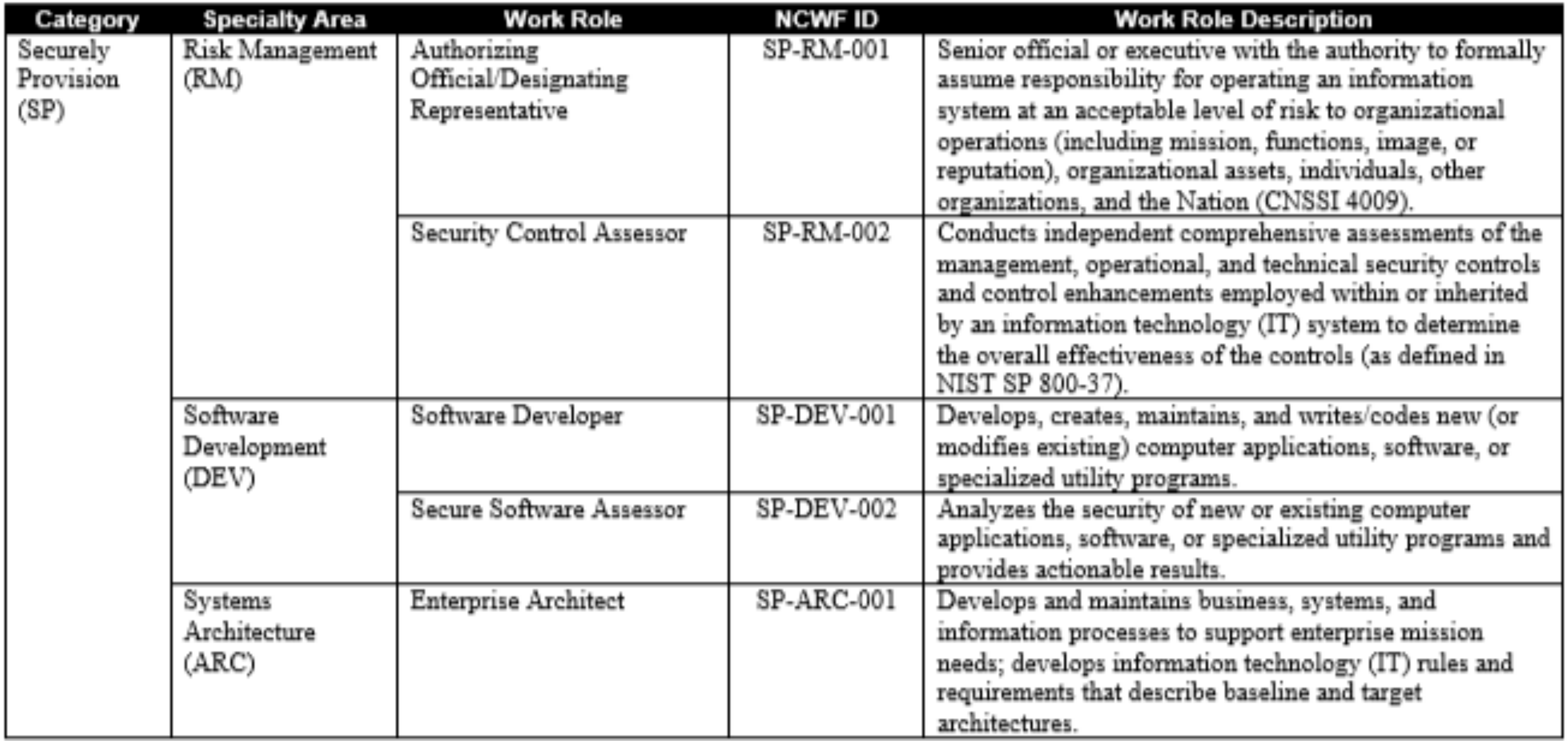


Categories	Specialty Areas	Specialty Area Descriptions
Securely Provision (SP)	Risk Management (RM)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's 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 (RD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning (RP)	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 (TE)	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.

Work Roles

- Work Roles are the most detailed grouping of IT, cybersecurity, or cyber related work
- Roles include lists of KSAs that are required to perform a set of functions or tasks
- Work being performed is described by selecting one or more Work Roles relevant to that job or position
- Work Roles aid in the organization and communication about cybersecurity responsibilities

Work Roles

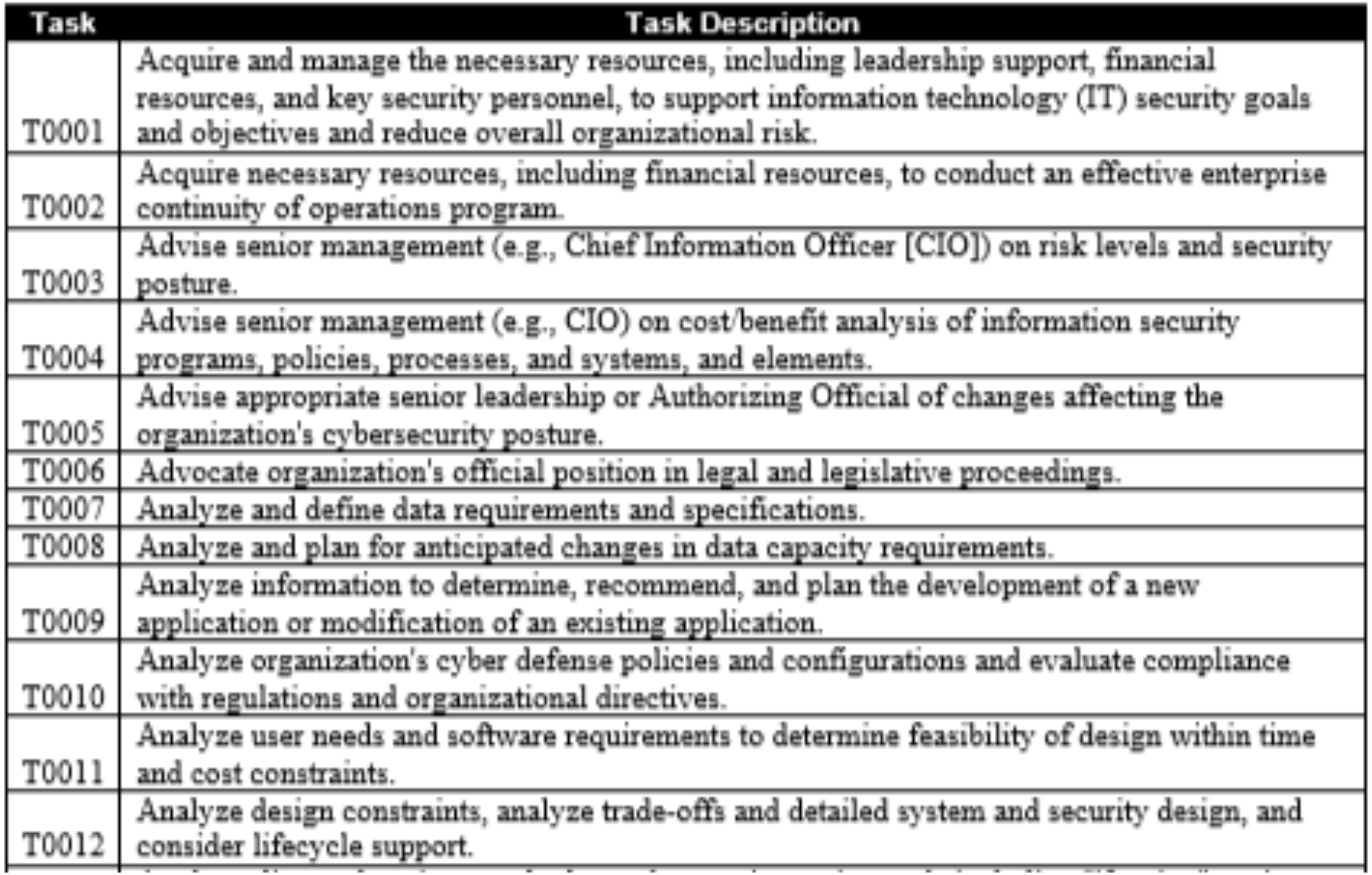


Category	Specialty Area	Work Role	NCWF ID	Work Role Description
Securely Provision (SP)	Risk Management (RM)	Authorizing Official/Designating Representative	SP-RM-001	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable 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-RM-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.

Tasks - KSAs

- Every Work Role requires an individual to perform certain duties, or Tasks which are the type of work that could be assigned
- Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform a job
- SP 800-181 associates KSAs with Work Roles to clearly define the qualifying experience or capabilities needed to successfully perform the tasks

Tasks



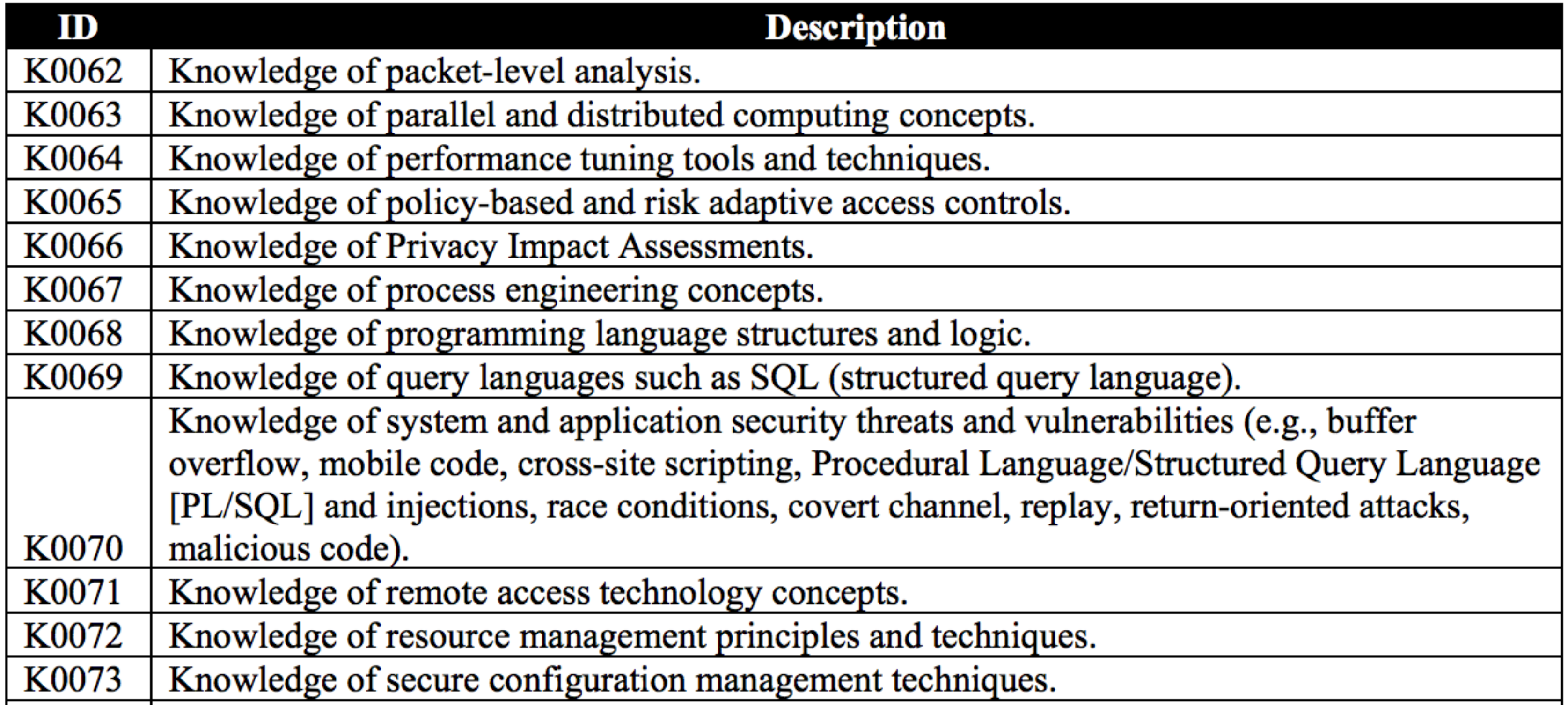
Task	Task Description
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
T0002	Acquire necessary resources, including 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, and 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 lifecycle support.

359 Tasks in SP 800-181

KSAs

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

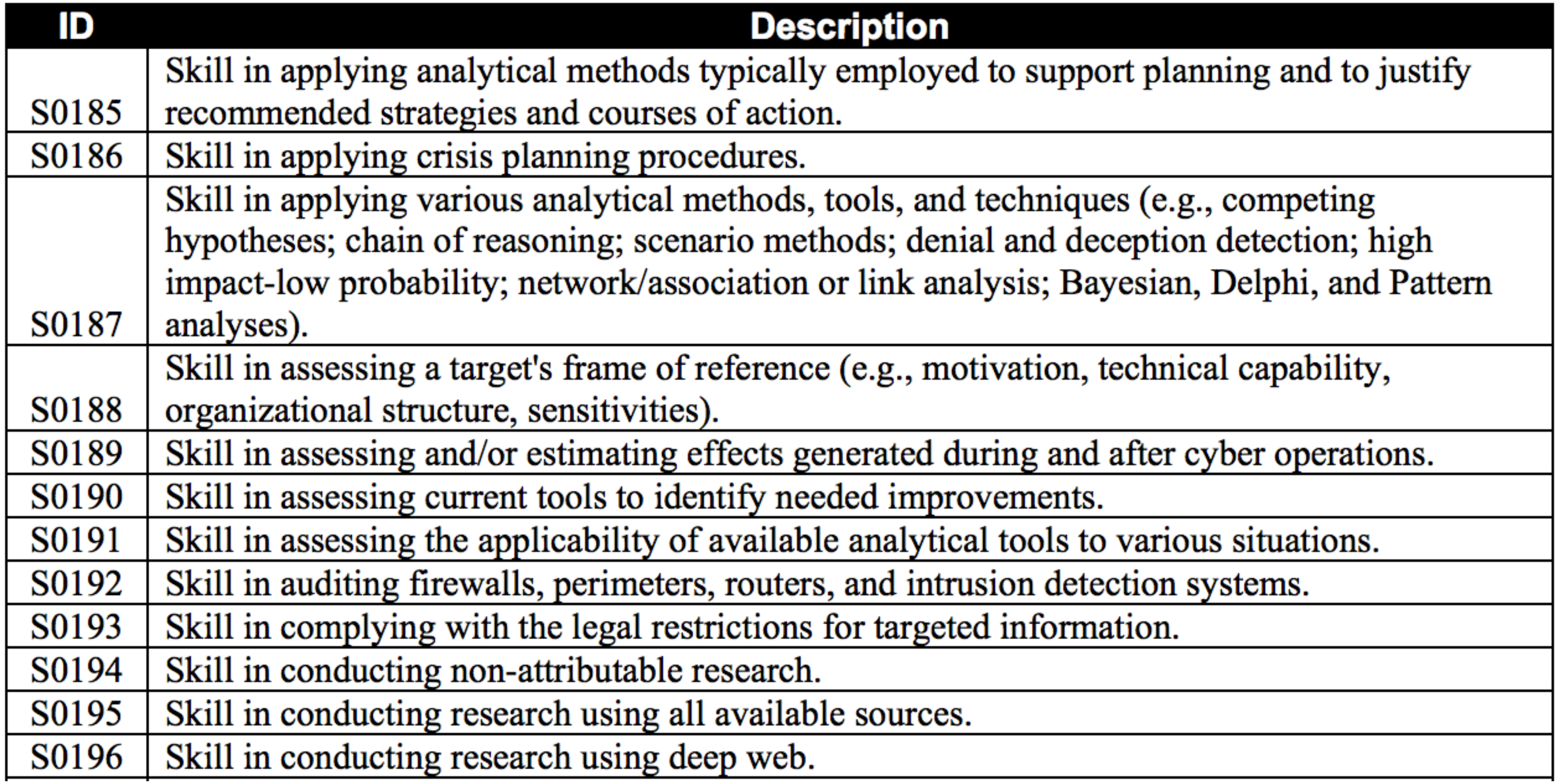
Knowledge



ID	Description
K0062	Knowledge of packet-level analysis.
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.

614 Knowledge elements

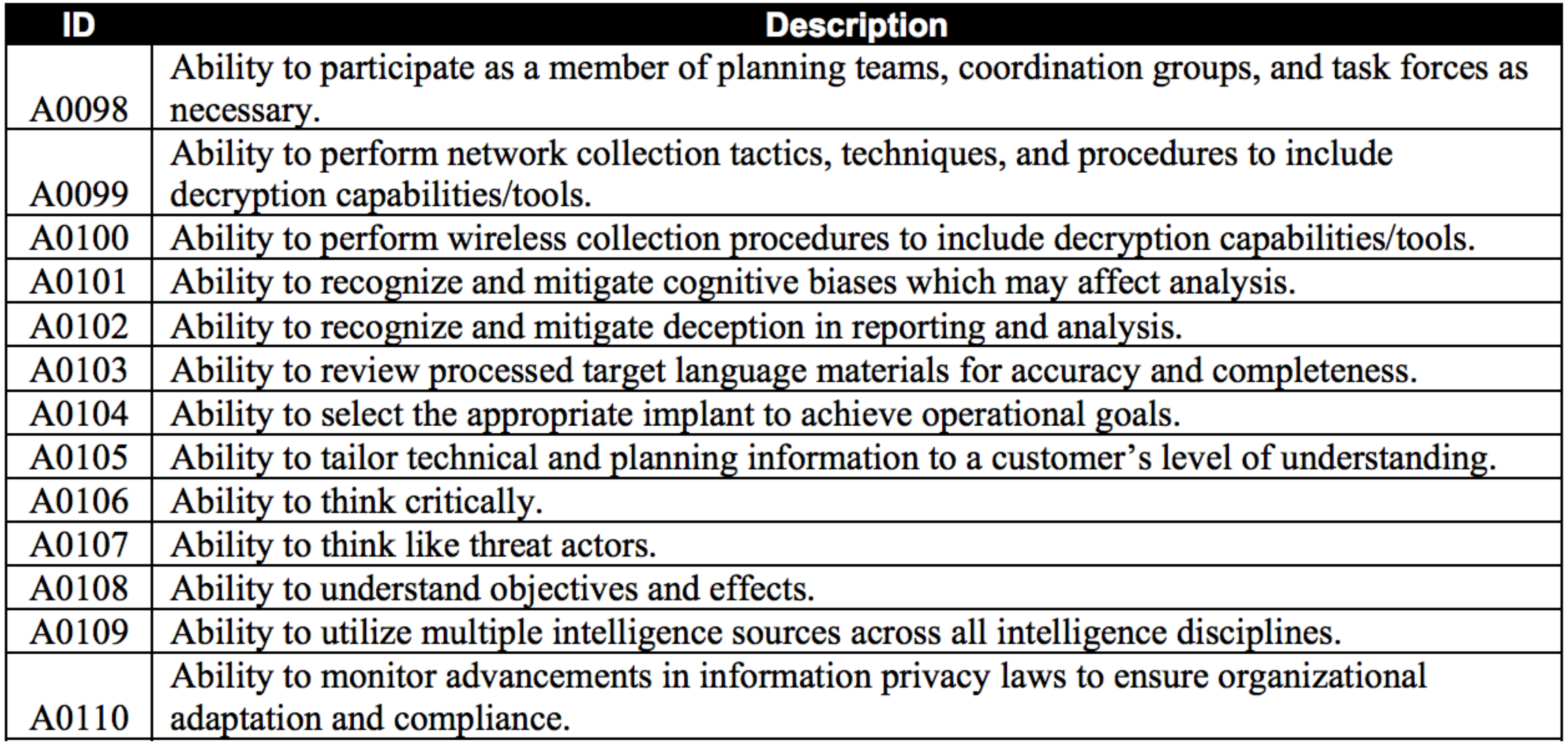
Skills



ID	Description
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.

359 Skills

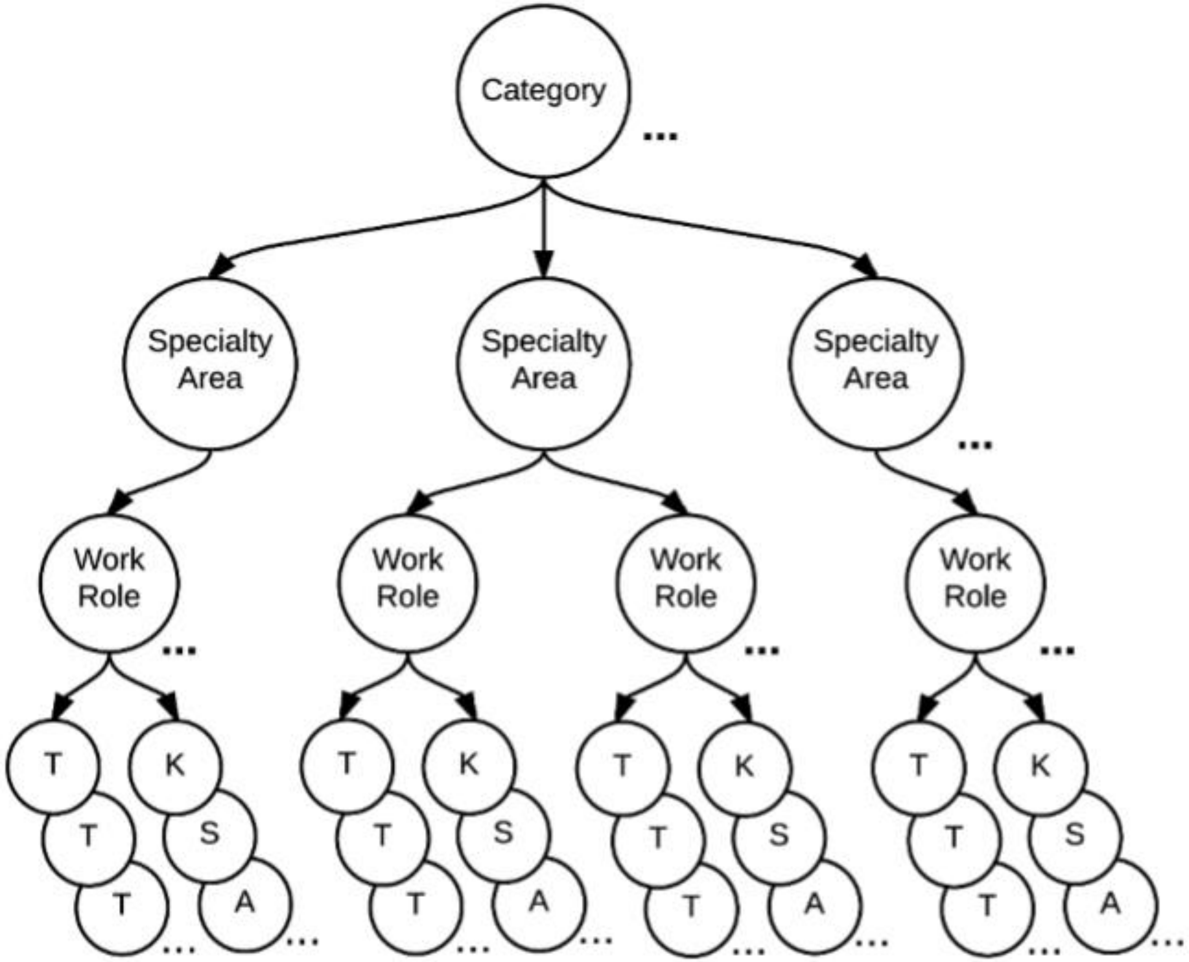
Abilities



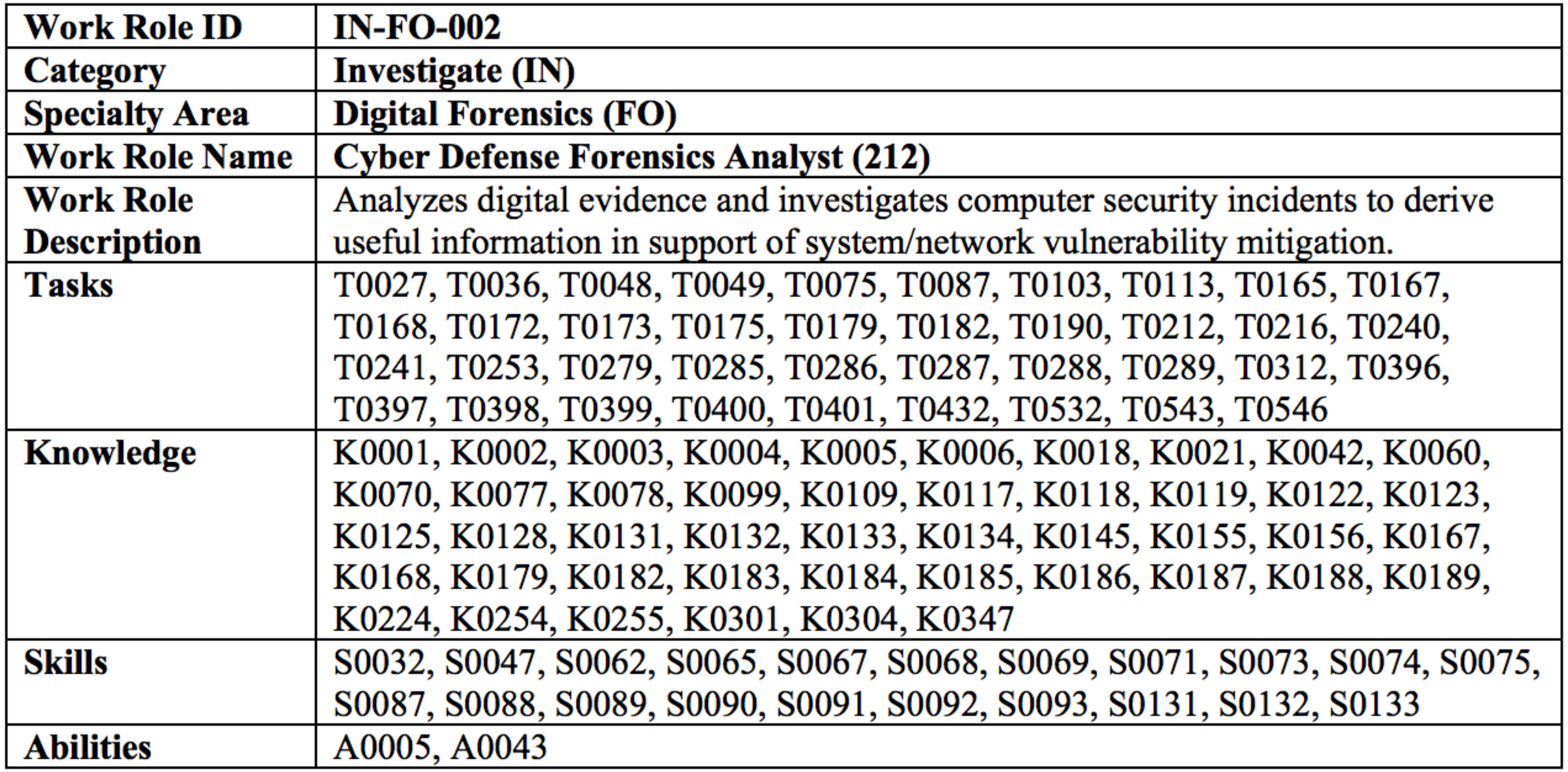
ID	Description
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.
A0099	Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools.
A0100	Ability to perform wireless collection procedures 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.

119 Abilities

Relationships



Work Role Detail Listing



Work Role ID	**IN-FO-002**
Category	**Investigate (IN)**
Specialty Area	**Digital Forensics (FO)**
Work Role Name	**Cyber Defense Forensics Analyst (212)**
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, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0543, T0546
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0099, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347
Skills	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133
Abilities	A0005, A0043

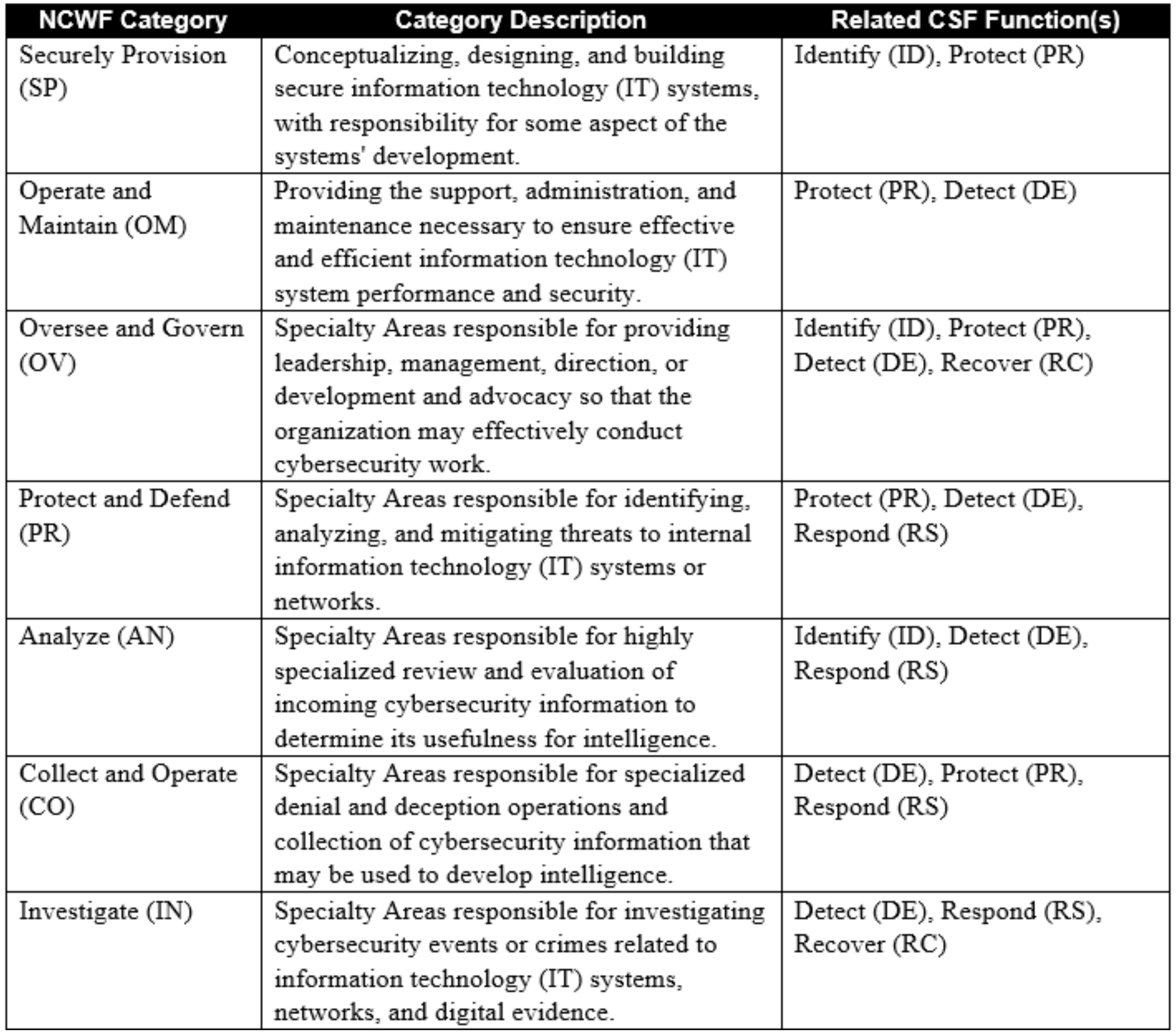
Workforce Mapping Efforts

- Cybersecurity Framework
- Employer/Employee
- Academic Institutions
- Certification Providers

Cybersecurity Framework

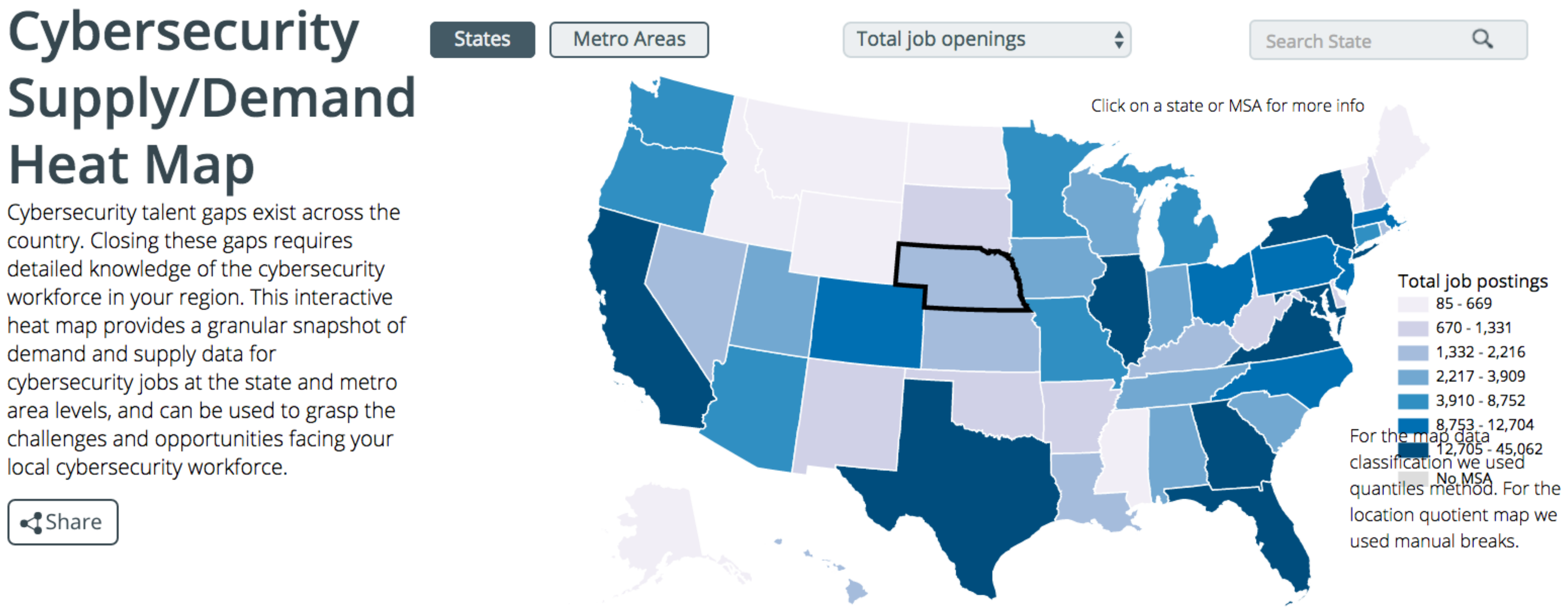
- Released in 2014, the Cybersecurity Framework was developed in response to Executive Order 13636, provides a performance-based and cost-effective approach to help organizations identify, assess, and manage cybersecurity risk
  - Identify (ID) – Develop the organizational understanding to manage cybersecurity 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

NCWF to CSF



NCWF Category	Category Description	Related CSF Function(s)
Securely Provision (SP)	Conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for some aspect of the systems' development.	Identify (ID), Protect (PR)
Operate and Maintain (OM)	Providing 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)	Specialty Areas responsible for providing 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)	Specialty Areas responsible for identifying, analyzing, and mitigating threats to internal information technology (IT) systems or networks.	Protect (PR), Detect (DE), Respond (RS)
Analyze (AN)	Specialty Areas responsible for 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)	Specialty Areas responsible for 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)	Specialty Areas responsible for investigating cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Detect (DE), Respond (RS), Recover (RC)

Cyberseek.org



Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Click on a state or MSA for more info

For the map data classification we used quantiles method. For the location quotient map we used manual breaks.

Nebraska

TOTAL CYBERSECURITY JOB OPENINGS

1,936

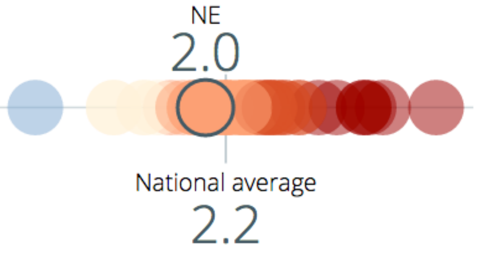
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

3,911

SUPPLY OF CYBERSECURITY WORKERS

Very Low

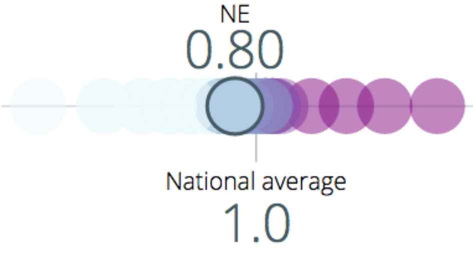
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION

Low

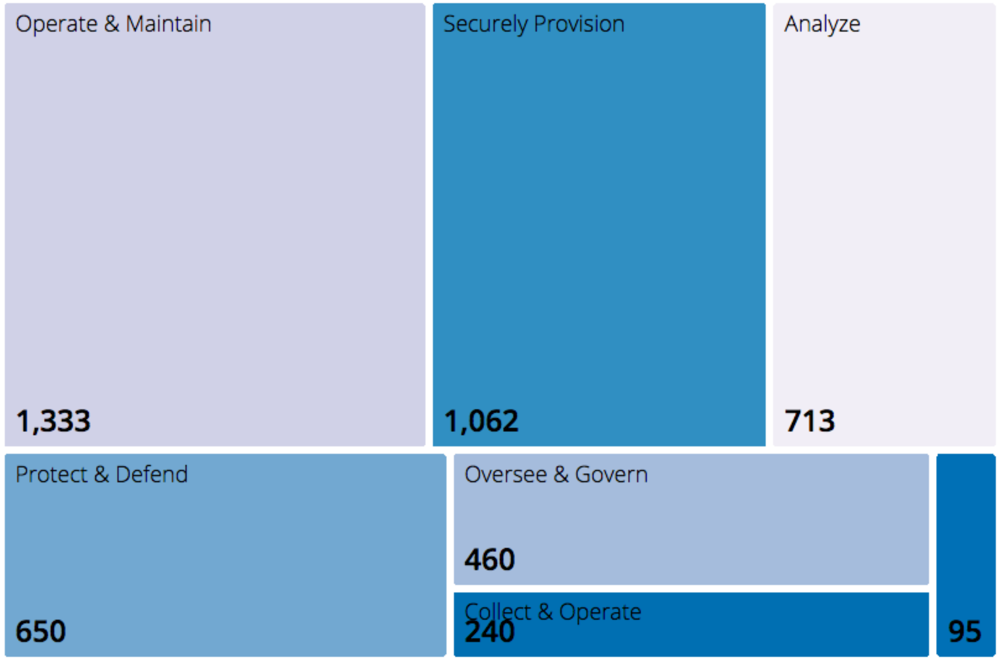
LOCATION QUOTIENT



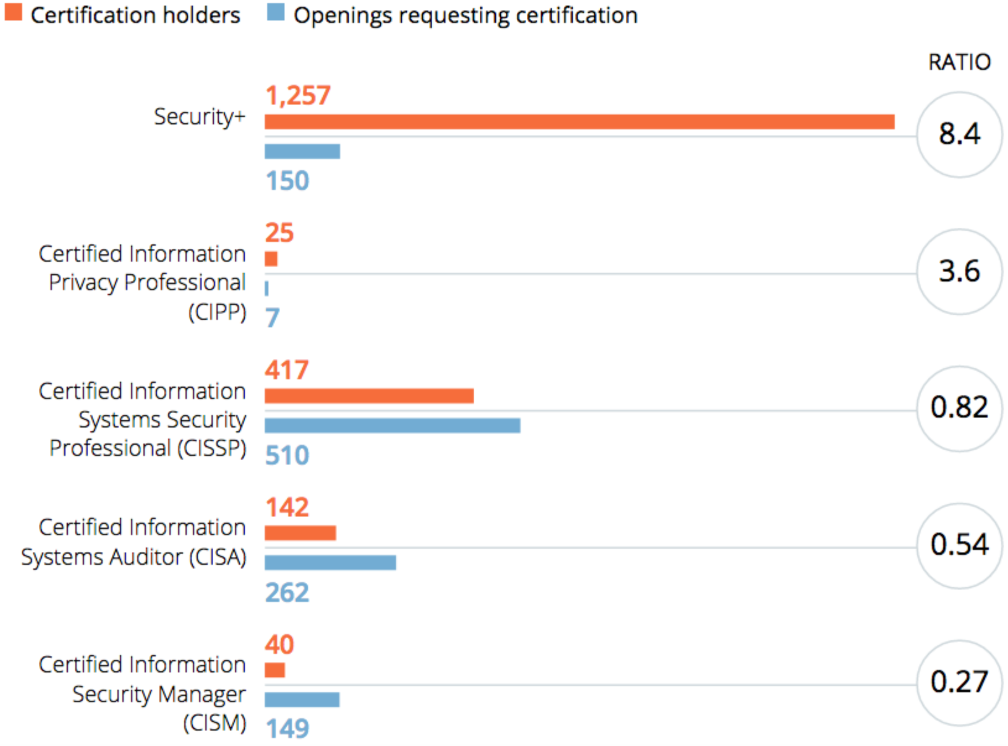
TOP CYBERSECURITY JOB TITLES

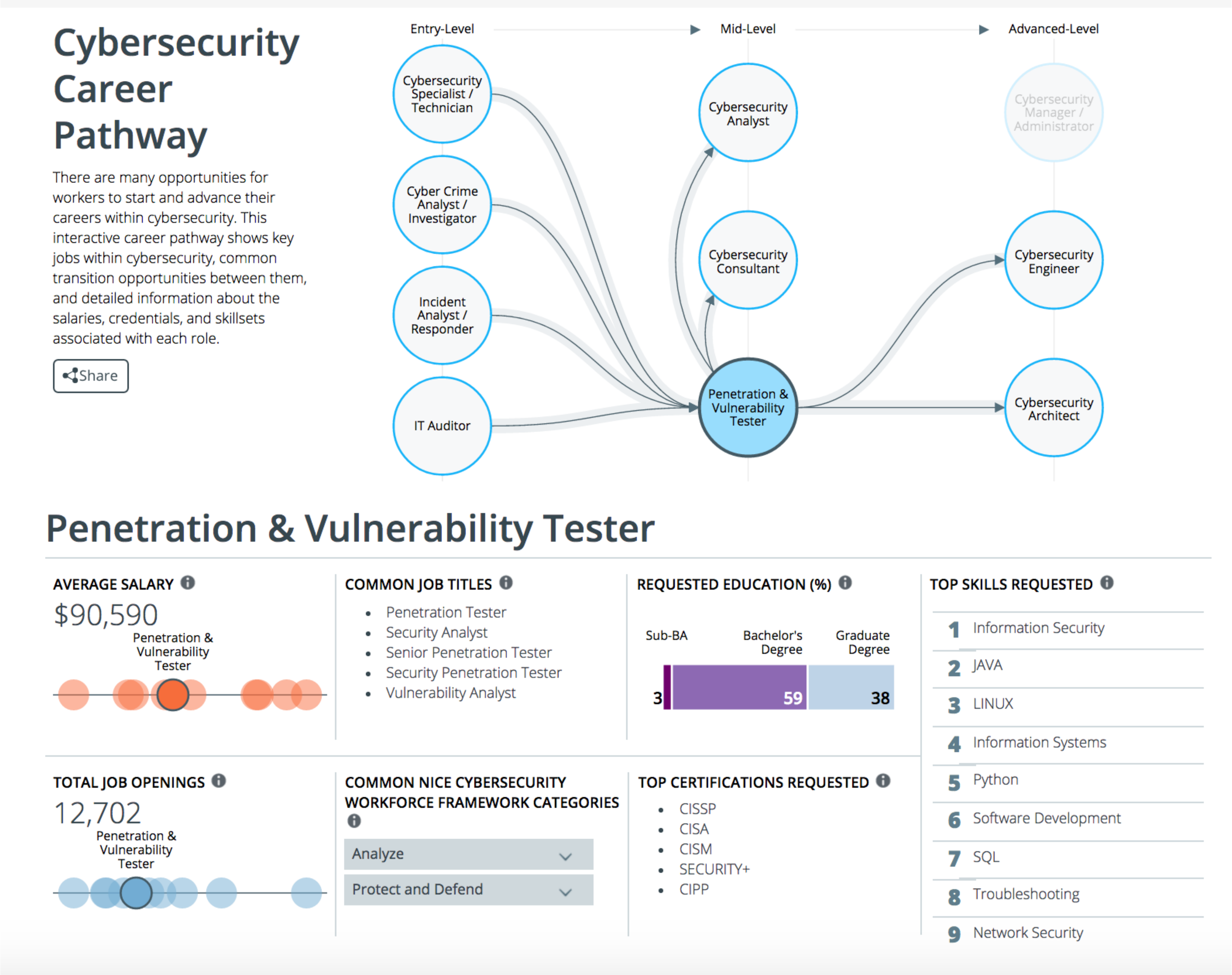
- Cyber Security Analyst / Specialist
- Cyber Security Engineer
- Auditor
- Systems Engineer
- Network Engineer / Architect
- Systems Administrator
- Network Administrator
- Risk Manager / Analyst
- Software Developer / Engineer

POSTINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION





Cybersecurity Career Pathway

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

Share

Entry-Level
Mid-Level
Advanced-Level
Cybersecurity Specialist / Technician
Cyber Crime Analyst / Investigator
Incident Analyst / Responder
IT Auditor
Cybersecurity Analyst
Cybersecurity Consultant
Penetration & Vulnerability Tester
Cybersecurity Manager / Administrator
Cybersecurity Engineer
Cybersecurity Architect

Penetration & Vulnerability Tester

AVERAGE SALARY

$90,590

COMMON JOB TITLES

- Penetration Tester
- Security Analyst
- Senior Penetration Tester
- Security Penetration Tester
- Vulnerability Analyst

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduate Degree
3	59	38

TOP SKILLS REQUESTED

1. Information Security
2. JAVA
3. LINUX
4. Information Systems
5. Python
6. Software Development
7. SQL
8. Troubleshooting
9. Network Security

TOTAL JOB OPENINGS

12,702

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

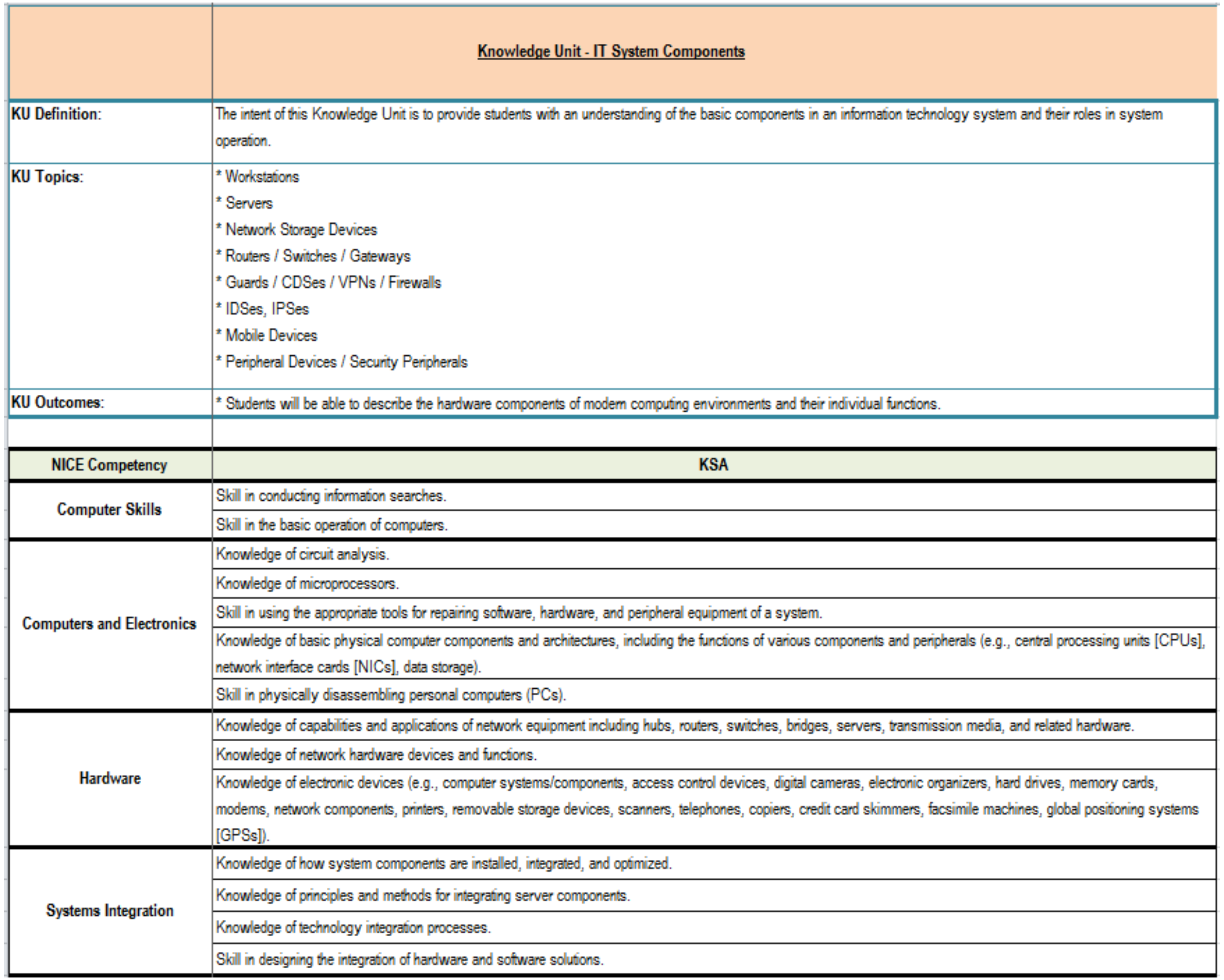
Analyze

Protect and Defend

TOP CERTIFICATIONS REQUESTED

- CISSP
- CISA
- CISM
- SECURITY+
- CIPP

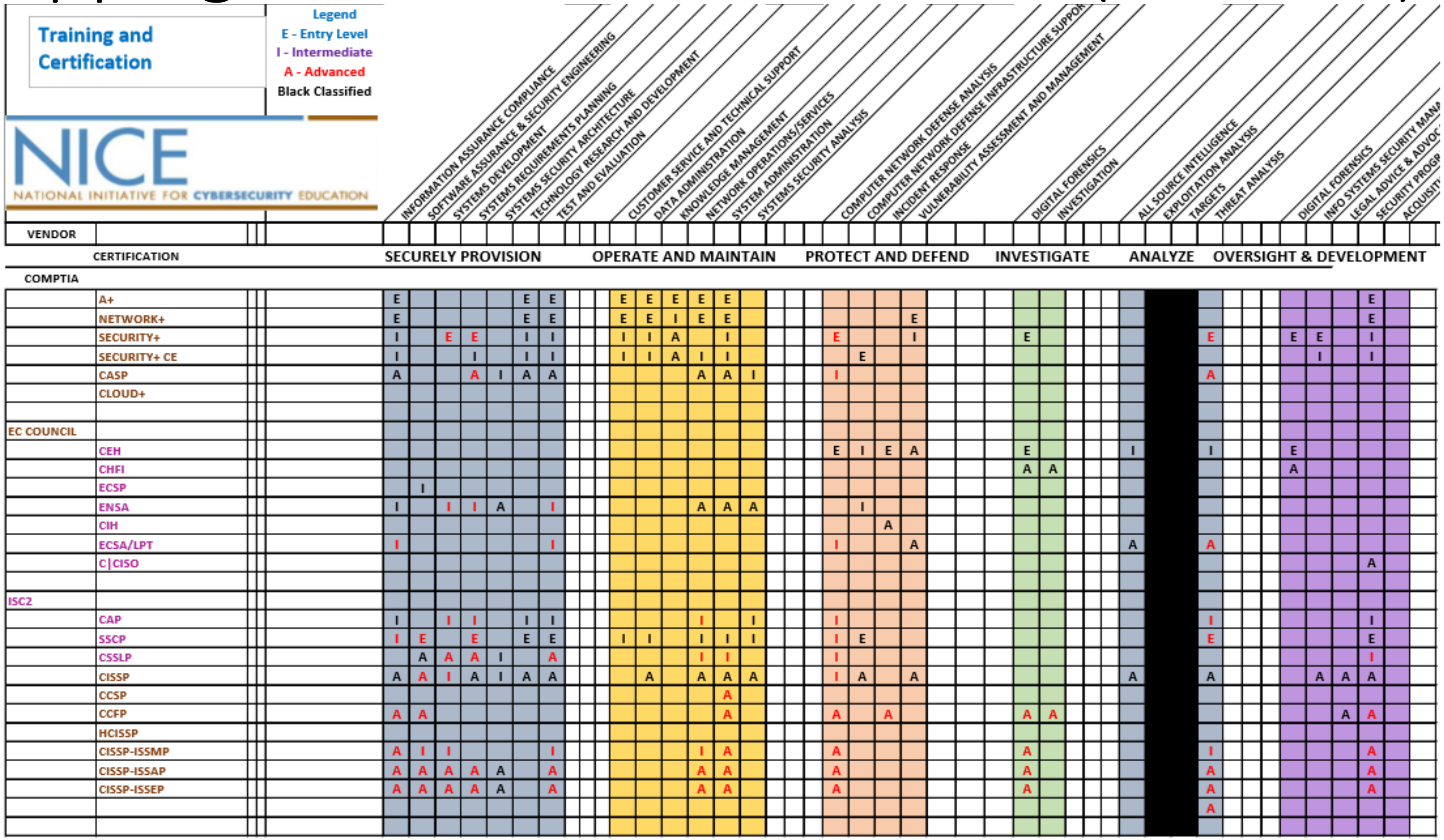
NSA KU’s to NICE KSA’s



	Knowledge Unit - IT System Components
KU Definition:	The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.
KU Topics:	* Workstations * Servers * Network Storage Devices * Routers / Switches / Gateways * Guards / CDSes / VPNs / Firewalls * IDSes, IPSes * Mobile Devices * Peripheral Devices / Security Peripherals
KU Outcomes:	* Students will be able to describe the hardware components of modern computing environments and their individual functions.

NICE Competency	**KSA**
Computer Skills	Skill in conducting information searches.
	Skill in the basic operation of computers.
Computers and Electronics	Knowledge of circuit analysis.
	Knowledge of microprocessors.
	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.
	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage).
	Skill in physically disassembling personal computers (PCs).
Hardware	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
	Knowledge of network hardware devices and functions.
	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]).
Systems Integration	Knowledge of how system components are installed, integrated, and optimized.
	Knowledge of principles and methods for integrating server components.
	Knowledge of technology integration processes.
	Skill in designing the integration of hardware and software solutions.

Mapping to Vendor Certifications (notional)



Training and Certification

Legend
E - Entry Level
I - Intermediate
A - Advanced
Black Classified

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

VENDOR	CERTIFICATION	SECURELY PROVISION							OPERATE AND MAINTAIN						PROTECT AND DEFEND				INVESTIGATE		ANALYZE				OVERSIGHT & DEVELOPMENT				
		INFORMATION ASSURANCE COMPLIANCE	SOFTWARE ASSURANCE & SECURITY ENGINEERING	SYSTEMS DEVELOPMENT	SYSTEMS REQUIREMENTS PLANNING	SYSTEMS SECURITY ARCHITECTURE	TECHNOLOGY RESEARCH AND DEVELOPMENT	TEST AND EVALUATION	CUSTOMER SERVICE AND TECHNICAL SUPPORT	DATA ADMINISTRATION	KNOWLEDGE MANAGEMENT	NETWORK OPERATIONS/SERVICES	SYSTEM ADMINISTRATION	SYSTEMS SECURITY ANALYSIS	COMPUTER NETWORK DEFENSE ANALYSIS	COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPOR	INCIDENT RESPONSE	VULNERABILITY ASSESSMENT AND MANAGEMENT	DIGITAL FORENSICS	INVESTIGATION	ALL SOURCE INTELLIGENCE	EXPLOITATION ANALYSIS	TARGETS	THREAT ANALYSIS	DIGITAL FORENSICS	INFO SYSTEMS SECURITY MANA	LEGAL ADVICE & ADVOC	SECURITY PROGR	ACQUISIT
COMPTIA																													
	A+	E					E	E	E	E	E	E	E															E	
	NETWORK+	E					E	E	E	E	I	E	E					E										E	
	SECURITY+	I		E	E		I	I	I	I	A		I		E			I	E					E	E	E		I	
	SECURITY+ CE	I			I		I	I	I	I	A	I	I			E										I		I	
	CASP	A			A	I	A	A				A	A	I	I									A					
	CLOUD+																												
EC COUNCIL																													
	CEH														E	I	E	A	E		I			I	E				
	CHFI																		A	A					A				
	ECSP		I																										
	ENSA	I		I	I	A		I				A	A	A		I													
	CIH																A												
	ECSA/LPT	I						I							I			A			A			A					
	C|CISO																											A	
ISC2																													
	CAP	I		I	I		I	I				I		I	I									I				I	
	SSCP	I	E		E		E	E	I	I		I	I	I	I	E								E				E	
	CSSLP		A	A	A	I		A				I	I		I													I	
	CISSP	A	A	I	A	I	A	A		A		A	A	A	I	A		A			A			A		A	A	A	
	CCSP												A																
	CCFP	A	A										A		A		A		A	A							A	A	
	HCISSP																												
	CISSP-ISSMP	A	I	I				I				I	A		A				A					I				A	
	CISSP-ISSAP	A	A	A	A	A		A				A	A		A				A					A				A	
	CISSP-ISSEP	A	A	A	A	A		A				A	A		A				A					A				A	
																								A					

Questions

Purpose and Applicability

- Provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work useful to educators, employers, and employees
- Improves communication among organizations to help identify, recruit, and develop cyber talent
- Enables employers to standardize professional development, certifications, and training
- Facilitates a more consistent, comparable, and repeatable approach to select and specify cybersecurity work roles for positions within organizations
- Provides a stable yet flexible catalog of tasks, knowledge skills and abilities for each cybersecurity work role to meet both the current and future needs
- Enables academic institutions to align curricula to the Workforce Framework and teach the knowledge necessary for students to effectively join the workforce