

CTE Program Narrative

NAME OF COLLEGE: Cerro Coso Community College

CONTACT: Dr. Corey Marvin

PHONE NUMBER: 760-375-6201

EMAIL ADDRESS: cmarvin@cerrocoso.edu

DATE: April 27, 2016

DIVISION: CTE

FACULTY: Valerie Karnes

PROGRAM NAME: Cyber Security Technician Certificate of Achievement

REASON FOR APPROVAL REQUEST (Check One):

- New Program Proposal
- Program Revision Proposal (Substantial or TOP Code Changes)
- Locally Approved

TYPE OF DEGREE:

- Certificate of Achievement
- Associate of Arts
- Associate of Science
- Associate of Arts for Transfer
- Associate of Science for Transfer
- Other

TRANSFER APPLICABILITY: Yes No

ATTACHMENTS/INFORMATION REQUIRED:

Labor/Job Market Data and Analysis
Advisory Committee Meeting Minutes
List of Advisory Committee Members
Employer Survey, if applicable

1. Statement of Program Goals and Objectives

Identify the goals and objectives of the program. For CTE programs, the statement must include the main competencies students will have achieved that are required for a specific occupation. The statement must, at a minimum, clearly indicate the specific occupations or fields the program will prepare students to enter and the basic occupational competencies students will acquire.

If the program is selective, describe relevant entry criteria and the selection process for admission to the program. Specify all mandatory fees that students will incur for the program aside from the ordinary course enrollment fee.

Statement of Program Goals and Objectives

The goals of this new certificate are to fill a documented need in the area of cyber security, information security and information assurance of our service area employers. The certificate is designed for students pursuing professional employment in information security for business. This certificate program provides students with skills to enter the job market as information security specialists, information security technicians, information assurance technicians, networking security technicians, and cyber security technicians. Designed for both full and part-time students, this program is appropriate to both those currently employed and those seeking to enter this field. The courses are aligned with industry certificates and students are prepared to take the A+ exam, Net+ exam, Security+ and Server+ exam.

Program Learning Outcomes:

- 1 . Configure, install, diagnose, and support hardware and software issues.
- 2 . Utilize identifying tools and methodologies that hackers use to break into a network computer and defend a computer and local area network against a variety of different types of security attacks using a number of hands-on techniques.
- 3 . Design, analyze, and support computer networks.
- 4 . Apply problem-solving, programming, and application development including the ability to design, test, debug, and implement complex computer programs.
- 5 . Operate servers, storage, and virtualization including implementing and evaluating network security solutions.
- 6 . Read and interpret technical information, as well as communicate with and write clearly for wide ranges of audiences.

2. Catalog Description

Enter exactly as it will appear in the catalog, including program outcomes. The description must also

- *Convey the certificate's goal(s) and objectives*
- *Provide an overview of the knowledge and skills that students who complete the requirements must demonstrate (student learning outcomes)*
- *List all prerequisite skills or enrollment limitations*
- *Mention any risks, such as occupations that are inherently competitive or low-salaried and/or occupational areas where inexperienced graduates are not generally hired.*
- *For CTE programs, the description must list the potential careers students may enter upon completion.*

- *Convey what the student may expect as an outcome*

If applicable, reference accrediting and/or licensing standards. If there is a widely recognized certification provided by a professional association, specify whether the program will fully prepare completers for the recognized professional certification.

The goals of this new certificate are to fill a documented need in the area of cyber security, information security and information assurance of our service area employers. The certificate is designed for students pursuing professional employment in information security for business. This certificate program provides students with skills to enter the job market as information security specialists, information security technicians, information assurance technicians, networking security technicians, and cyber security technicians. Designed for both full and part-time students, this program is appropriate to both those currently employed and those seeking to enter this field. The courses are aligned with industry certificates and students are prepared to take the A+ exam, Net+ exam, Security+ and Server+ exam.

Cyber Security Technician Certificate of Achievement is designed for students pursuing professional employment in information security for business. This certificate program provides students with skills to enter the job market as information assurance technicians, information security analysts, network security professionals and cyber security technicians. Designed for both full-time and part-time students, this program is appropriate to both those currently employed and those seeking to enter the field.

Students exiting this program are prepared to enter the fields of information security, network security, information assurance or cyber security. Students can demonstrate the following student learning outcomes.

- 1 . Configure, install, diagnose, and support hardware and software issues.
- 2 . Utilize identifying tools and methodologies that hackers use to break into a network computer and defend a computer and local area network against a variety of different types of security attacks using a number of hands-on techniques.
- 3 . Design, analyze, and support computer networks.
- 4 . Apply problem-solving, programming, and application development including the ability to design, test, debug, and implement complex computer programs.
- 5 . Operate servers, storage, and virtualization including implementing and evaluating network security solutions.
- 6 . Read and interpret technical information, as well as communicate with and write clearly for wide ranges of audiences.

Students entering this program develop all the skills necessary to be successful are taught in the first course in the career pathway (CSCI C101). Jobs in information security and cyber security are in high demand and pay from \$86,000 (per Labor Market data attached).

3. Program Requirements

- ✓ *The program requirements must be consistent with the catalog description. The number of units, specific course requirements and the sequence of the courses must be coherent, complete and appropriate. Display the program requirements in a table format that includes all courses required for completion of the program (core requirements and required or restricted electives), subtotal of core units, and total program units. For each course, indicate the course department number, course title, and unit value.*

Display of Program Requirements

Core Courses	Title	Units
CSCI C101	Introduction to Computer Information Systems	3
CSCI C142	Information & Communication Technology Essentials	4
CSCI C143	Computer Network Fundamentals	3
CSCI C146	Security+ Fundamentals of Networks	3
CSCI C251	Introduction to Programming Concepts and Methodologies	3
CSCI C190	Introduction to Cyber Security: Ethical Hacking	3
CSCI C193	System and Network Administration	3
CSCI C195	Introduction to Systems Analysis and Design	3
MATH C121	Elementary Probability and Statistics Or MATH C121H Elementary Probability and Statistics – Honors Or	4-5
MATH C130	Finite Mathematics Or	4
MATH C131	Basic Functions and Calculus for Business	4
	Total Core Courses	29-30

In addition to the core courses, the student must take at least 0 units from the following courses:

Elective Courses	Title	Units
	Total Elective Courses	

Total Units Required for Certificate	29-30
---	--------------

Display of Proposed Sequence

First Semester	Units
CSCI C101	3
CSCI C142	4
Total	10

Third Semester	Units
CSCI C190	3
CSCI C193	3
MATH C121/130/131	4-5
Total	10-11

Second Semester	Units
CSCI C143	3
CSCI C146	3
Total	6

Fourth Semester	Units
CSCI C195	3
CSCI C251	3
Total	6

7. Master Planning (Background and Rationale)

Given the stated goals and objectives, address the role the proposed program will fulfill in the college's mission and curriculum offerings. This discussion may include some history of the program proposal origins, a description of the program purpose, and/or the program's relevancy for the region and college.

The proposal must demonstrate a need for the program that meets the stated goals and objectives in the region the college proposes to serve with the certificate. A proposed new certificate must not cause undue competition with an existing program at another college.

If any expenditures for facilities, equipment or library and learning resources are planned, please explain the specific needs in this section.

If the program is to be offered in close cooperation with one or more specific employers, a discussion of the relationship must be provided.

There has been an increasing need in our service area, state and across the country for qualified entry-level personnel to enter the Cyber Security, Information Technology Security, Network Security, and Information Assurance. This need continues to expand as the networks and hackers and hostile groups infiltrate systems in major organizations. The Cyber Security Certificate of Achievement will provide students with a baseline of courses to be immediately employed in Cyber Security, Information Assurance, and Information Security. The employer community within our service area supports the need for this certificate. The employer community within our service area supports the need for this certificate and has requested over one hundred graduates per year. Program development has been driven by the employers in our service area and the national need for technicians in this field.

Most on-site courses at the IWV campus are taught in the Learning Resource Center. There are two computer lab classrooms. One classroom is equipped with 30 student stations and the third is equipped with 29 student stations. All rooms have an instructor station, an overhead projector, and whiteboards. Although iTV rooms are available to allow multiple campuses to participate in a single course, the rooms are not equipped with computer stations, limiting their usefulness for CSCI courses that require hands-on access to technology to achieve the student learning objectives. Increasingly, other disciplines (English, math, engineering, science) are requesting to use the computer classrooms for their own courses. It is expected as the college continues to develop science, technology, engineering, and as the use of computer technology is infused across the curriculum, the demand for these rooms will increase and additional facilities will be required. In addition, if the college pursues a partnership with Cisco to further develop an Information Technology/Cyber Security/Information Assurance program, it will be required to have a dedicated laboratory to be designated as a Cisco certified college.

The college has used VTEA funds to further develop the Computer Information Systems program in the past and it is expected that the new Cyber Security program will also be supported by VTEA funds. A VTEA program plan has already been developed and submitted for funding to fund the needs of an emerging program for 2016-2017. If it determined that the college needs to be a Cisco certified partner for higher level certificates, there will be space required, equipment required and an ongoing equipment cost that could be funded through federal grants for Cyber Security.

The Library and Learning Resource Center are used to support the current program. The library is used to support research for the courses in the program. Five of the Cyber Security program is shared with the Computer Information Systems courses, so there are adequate resources available. The additional three courses for the program may require additional books and materials for the program. The department faculty regularly works with the librarian to acquire books and materials for the area and programs. There have been recent additions to the electronic library resources that will support both the Computer Information Systems and Cyber Security Program. Additionally, several courses in the department are directly supported with Library research instructions tailored to the course by the library staff.

The program was developed and is supported by the Computer Information Systems Advisory Committee and the Cyber Security Sub-committee. An internship program with Jacobs Technology and the Naval Air Warfare Center at China Lake demonstrates the strong commitment of industry to this program. Employers are interviewing and hiring student interns that have completed the first course in the sequence (CSCI C101) with the expectation that the students will complete the Cyber Security Certificate of Achievement and the Cyber Security degree program within three years. This is a direct result of a close relationship with employer needs. The five employers on the Advisory Committee are also considering adopting the Jacobs model of internships.

7. Need for Program

a. Enrollment and Completer Projections

Address and justify the number of projected students or “annual completers” to be awarded the certificate each year after the program is fully established.

The Cyber Security program is a new program that will fill a target need for industry. Employers have indicated a need for 100 employees in this area. In order to full this need, we will need to scale our program offerings to meet this need. We project enrollment in the program to be 150-200 in the four beginning courses. Students will choose between the Computer Information Systems and Cyber Security program following completion of the four core classes. Completer projections are 50-100 per year by 2018.

For those students interested in transfer, the new model cyber security curriculum provides students with a pathway to California State University at San Bernardino in the Information Systems and Technology Bachelor of Science program. All of the courses offered in the CIS degree are accepted for transfer within the UC and CSU systems (source: assist.org) as well as other universities throughout the US.

b. Labor Market Information (LMI)

Summarize the Labor Market Information (LMI) and employment outlook (Including citation for the source of the data) for students exiting the program.

Enter table or chart as a separate attachment.

The attached Labor Market report for Information Security/Cyber Security/Information Assurance shows a regional need for 164 jobs with the 2020 projections to be 200 jobs. This represents a 22% increase in jobs. While this shows demonstrated need, in the Cerro Coso service area there are many known jobs that are not documented because employer's corporate offices are out of state. For example, positions appropriate for IT/CIS/Cyber Security graduates such as those required by aerospace contractors, the Naval Air Warfare Center at China Lake, and even our own Cerro Coso Community College classified IT staff are not captured in this reporting system because the corporate offices are located outside our service area.

The Cyber Security program has documented labor market demand for the degree and certificate. In the Cerro Coso service area there are many known jobs that are not documented because employer's corporate offices are out of state. For example, positions appropriate for Cyber Security graduates such as those required by aerospace contractors, the Naval Air Warfare Center at China Lake, and even our own Cerro Coso Community College classified IT staff are not captured in this reporting system because the corporate offices are located outside our service area.

Employers in the Indian Wells Valley have attended the Advisory Committee meetings over the past several years and have actively engaged in the discussions and development of the new certificate(s) and degree for Computer Information Systems and Cyber Security Technology. At first, we believed that the Information Technology Plus certificate would fill the entire need. Following the CIS Advisory Committee Meeting in November 2015, the employers indicated that they needed a more specific cyber security program (COA and AS) as well as the CIS program. Faculty attended the Information and Communication Technology state conference in January 2016, which outlined the needs and forecast for Cyber Security programs. Additionally, there was an announcement that there was a model program that was fully transferrable to CSU San Bernardino. This new program will share the IT Plus certificate and then students will be able to select the IT pathway or the Cyber pathway.

While the numbers of job opportunities are reflective in the environmental scans attached, two local employers are not captured (Jacobs Technology and the Naval Air Warfare Center at China Lake). These two specific employers have come to the college in the past few months presenting their local hiring requirements. Each employer is estimating a minimum of 40-50 students needed for their organization. Internships and apprenticeship programs have recently been developed to provide a pipeline for employees. Employers are hiring directly out of our first level class with the understanding that students will take the remaining courses to earn their certificate and then their degrees. In December, they hired three students for the internship program and anticipate hiring the fourth in March/April. We are preparing students now to interview in mid to late April. Jacobs plans to hire three to four students per quarter for the internship program.

Environmental scan reports from EMSI, Burning Glass and the Community College Review all project huge need that is only expected to expand. The Cyber Security job postings have grown 91% from 2010-2014 as compared to other IT postings (28%). The duration of the postings in cyber security is 47 days versus 36 days for all other IT jobs. Salaries for Cyber Security are \$6,459 higher than all other IT postings (Cyber Security \$83,934 versus IT \$77,475). Additionally, California ranks first in the nation for the job postings (Burning Glass) and the percentage of growth from 2010-2014 was 75%. There were 28,744 job postings in California from 2010-14.

c. Employer Survey (if applicable)

When strong LMI data is not available, an employer survey may be submitted. Provide a copy of the survey, including the number of those surveyed, number of responses, and a summary of the results. The survey must address the extent to which the proposed degree or certificate will be valued by employers.

Specific CSCI courses have been developed and delivered to meet the short-term and long-term needs of local employers. The CIS Advisory Committee formed a subcommittee for Cyber Security to review the national Homeland Security and National Security Administration. Additionally, the development team of the program includes top experts from NAWC at China Lake, Monarch and AltaOne. The department is responsive to requests for specific training programs and attempts to develop appropriate coursework, as needed, dependent on staffing and budgetary constraints. Informal surveys have been done at the CIS and Cyber Security Advisory Committees and this program is being driven by local, state and national needs.

7. Place of Program in Curriculum/Similar Programs

Review the college's existing program inventory, then address the following questions:

- *Do any active inventory records need to be made inactive or changed in connection with the approval or the proposed program? If yes, please specify.*
- *Does the program replace any existing program(s) on the college's inventory? Provide relevant details if this program is related to the termination or scaling down of another program(s).*
- *What related programs are offered by the college?*

These courses also serve the Computer Information Systems Associate's degree. The Information Technology Plus certificate is the first level of the Computer Information Systems pathway and provides students a first step into the industry. The second level certificate (Cyber Security certificate) has several additional courses that result in another certificate and finally adding General Educational requirements; students will earn an Associate Degree of Science.

There are no other colleges in our service area and the program does not represent unnecessary duplication. The program does not represent unnecessary duplication of training programs and other regional colleges offering a similar program are too far away to impact employer's needs in our service area.

7. Similar Programs at Other Colleges in Service Area

List similar programs offered at other colleges within the Central/Mother Lode Region that may be adversely impacted. Enter 'none' if there are no similar programs.

College	Program
None	

Supporting documentation required

Labor Market Information

In a separate attachment, provide current Labor Market Information showing that jobs are available for program completers within the local service area. Statewide or national LMI may be included as supplementary support but evidence of need in the specific college service area or region is also necessary.

List of Members of Advisory Committee

This list must include advisory committee member names, job titles, and affiliations.

Name	Title	Affiliation
Melissa Oliverez	Manager	Continental Labor
Johnson Daniel	Network Administrator	Coso/Teragen contrastIT
Mary Lorber	Software Architect/Program Mgr	Engility
Sean Callihan	STARS IT/IA Director	Jacobs Engineering
Tom Della Santana	STARS IT/IA/Business Director	Jacobs Engineering
Rich Christenson	Recruiter	Jacobs Engineering
Vaughn Corbridge	VX-9 TIMS PM/Analyst	HTii
Eileen Shibley	CEO	Monarch
Uwe Schmiedel	IT Director	Monarch
Edward Balcer	Head, Weapons & Energetics Technology Assurance Branch	NAVAIR Weapons Division

Keith Bennett	Information Assurance	NAWC China Lake
Tony Vitale	Information Assurance	NAWC China Lake
Margaret Porter	Information Assurance	NAWC China Lake
Autumn Piotrowski	Information Assurance	NAWC China Lake
Mark Henderson	Directed Energy Manager	NAWC China Lake
Linda Homer	Software Programmer	NAWC China Lake
John Paul	Program Manager	New Directions Technology, Inc
Kishor Joshi	CEO	Pertexa
Scott Lougheed	Director	Saalex
Paul McKenzie	Director	Saalex

Recommendation of Advisory Committee (Meeting Minutes)

In a separate attachment, provide minutes of the advisory committee meetings at which the program was discussed and approved, with relevant areas highlighted, as well as a summary of the advisory committee recommendations.

CIS Advisory Committee Meeting

Meeting Date April 9, 2014

Attendees:

- Valerie Karnes: Dean CTE IWV
- April Browne: CIS/CS faculty IWV
- John Bradley: Operations Lead, Navair

Model Curriculum

April went through the courses in the Draft Model Curriculum. It was discussed that this is a Model Curriculum and not a Transfer Curriculum because there are not enough 4 year degrees offered by the CSU's in the CIS area.

Core Classes

1. Information & Communication Technology Essentials C-ID ITIS 110 is equivalent to our current CIS 140 and CIS 141 A+ certification courses.
2. Computer Information Systems C-ID ITIS 120 is equivalent to our current CIS 101 Introduction to Computer Information Systems course. This course has been revised to the C-ID standard already for the Business Transfer degree
3. Introduction to Programming Concepts and Methodologies C-ID ITIS 130 is equivalent to our current CIS 251 Introduction to Visual Basic course
4. Computer Network Fundamentals C-ID ITIS 150 is equivalent to our current CIS 143 Network + course.

Elective Courses (2 courses or 6 units)

1. Introduction to Systems Analysis and Design C-ID ITIS 140 based on conversations with the other CIS instructor Matt Hightower, it was decided that we would not offer this course as an elective. It has been offered in the past and most of the information is covered in the Database course.
2. Introduction to Information Systems Security C-ID ITIS 160 is equivalent to our current CIS 146 Security+ course
3. Introduction to Database Management Systems C-ID ITIS 180 is equivalent to our current CIS 240 Database course
4. Business Communication C-ID BUS 115 is already offered for the Business Transfer degree
5. Systems and Network Administration C-ID ITIS 155 is a course we do not currently offer. This course prepares students for the CompTIA Server+ certification (similar to all of our other certification courses). This leads to our second agenda item a discussion on Operating System certifications. This course may fulfill it based on the proposed textbooks but it isn't entirely clear if it would or not. John Bradley said he received a list of approved courses for that area and would forward this me (received 4/9/2014 and is attached).

This course would be good for students to have because it would move their resumes forward in the process if they are looking for a Systems Administrator (SA) or Computer Security job. It was decided that we should offer this course as an elective in the program even if it won't fulfill the Operating System requirement. This would be a good CEU course for current SA and security personnel.

Math Classes

The math class options were brought up. All of the math courses are already offered at the college. Students must have 1 math class from Statistics which is often the suggestion for transferring. We don't currently have Calculus 1 in the degree and would have to add that as an option for this degree.

Operating System Certification

John said there is still some confusion if applicants MUST have their operating system certification before being hired or if they have 6 months after being hired. Both are referenced in materials he receives. Applicants that meet these requirements are moved forward in the interview process.

Applicants that have some coding (our VB course), Security+ and an operating system certification are having their applications forwarded. There are approximately 5 – 10 IT/SA positions available each year. Some years there are short term projects such as the RAM project 4 years ago and there are many positions available.

Other discussions

Other jobs open to our students are Data Processing jobs. For these entry level jobs, they are looking for applicants with basic computer skills and application skills. It appears that a 12 unit certification covering the Core classes may be a good fit for these jobs.

The full degree (as we investigate the Operating Systems requirement) would be a good fit for Systems Administration and IAO/IAM jobs. NOTE: the IAO/IAM language is changing. John will provide the new structure for these jobs (received 4/9/2014 and attached).

It was brought up that right now we offer a programming pathway in our CIS degree. John did not believe that this was necessary if we offer a Computer Science program. Programmers would take that degree program most likely. It was also discussed that they need some entry level database applications jobs. These are jobs in which applicants would be responsible for upkeep and maintenance of databases such as Access. So a program in which students took all of the Microsoft Office courses, Visual Basic for Applications (a new class), Vizio and Adobe Acrobats forms as well as courses such as PHP MySQL and the CIS Database course would be a good fit. This may be a new certification opportunity to support this area with few new classes. This should be examined further.

Credentialed Operating System Training Courses

TWMS COURSE ID	COURSE TITLE	Category and Level
TP70270_ENG	70-270 INSTALLING, CONFIGURING, AND ADMINISTERING MICROSOFT WINDOWS XP PROFESSIONAL	IAT I, II, III
TP70284_ENG	70-284: IMPLEMENTING AND MANAGING MICROSOFT EXCHANGE SERVER 2003	IAT I, II, III
TP70290_ENG	70-290: MANAGING AND MAINTAINING A MICROSOFT WINDOWS SERVER 2003 ENVIRONMENT	IAT I, II, III
TP70291_ENG	70-291: IMPLEMENTING, MANAGING, AND MAINTAINING A MICROSOFT WINDOWS SERVER 2003 NETWORK INFRASTRUCTURE	IAT I, II, III
TP70294_ENG	70-294: PLANNING, IMPLEMENTING, AND MAINTAINING A MICROSOFT WINDOWS SERVER 2003 ACTIVE DIRECTORY INFRASTRUCTURE	IAT I, II, III
TWMS-505631	70-640: Configuring Windows Server 2008 Active Directory Training	IAT I, II, III
TWMS-505629	70-642: Configuring Windows Server 2008 Network Infrastructure Training	IAT I, II, III
TWMS-505627	70-646: Windows 2008 Server Administrator Training	IAT I, II, III
TP70647_ENG	70-647: WINDOWS SERVER 2008 ENTERPRISE ADMINISTRATOR	IAT I, II, III
TWMS-505630	70-662: Configuring Microsoft Exchange Server 2010 Training	IAT I, II, III
TP70680_ENG	70-680: CONFIGURING WINDOWS 7	IAT I, II, III
TP70685_ENG	70-685: WINDOWS 7: ENTERPRISE DESKTOP SUPPORT TECHNICIAN	IAT I, II, III
TWMS-509394	Automated Digital Networking System (ADNS) F CIN A-101-1125/Navy F School Provided	IAT I, II, III
TWMS-509395	Automated Digital Networking System (ADNS) H CIN A-101-1125/Navy F School Provided	IAT I, II, III
TWMS-509396	Automated Digital Networking System (ADNS) J CIN A-101-1125/Navy F School Provided	IAT I, II, III
TWMS-509397	Automated Digital Networking System (ADNS) K CIN A-101-1125/Navy F School Provided	IAT I, II, III
TWMS-509383	CISCO Certified Entry Network Professional (CCNP): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509382	CISCO Certified Entry Networking Technician (CCENT): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509384	CISCO Certified Network Associate (CCNA): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
J-150-2955	GLOBAL COMMAND AND CONTROL SYSTEM MARITIME SYSTEM ADMINISTRATOR	IAT I, II, III
A-150-0045	GLOBAL COMMAND AND CONTROL SYSTEM-MARITIME (GCCS-M) 4.X SYSTEM ADMINISTRATOR	IAT I, II, III
A-150-3400	GLOBAL COMMAND AND CONTROL-MARITIME(GCCS-M) 4.0.3 SYSTEM ADMINISTRATOR	IAT I, II, III
A-150-3500	GLOBAL COMMAND AND CONTROL-MARITIME(GCCS-M) 4.1 SYSTEM ADMINISTRATOR	IAT I, II, III
W-150-2130	HOST-BASED SECURITY SYSTEM (HBSS) VERSION 4.5	IAT I, II, III
TWMS-509389	Integrated Shipboard Networking System (ISNS) Compose 3.0 Increment 1 CIN A-150-1121/Navy F School Provided	IAT I, II, III
TWMS-509390	Integrated Shipboard Networking System (ISNS) Compose 3.0 Increment 1 CIN A-150-1121/Navy F School Provided	IAT I, II, III
TWMS-509391	Integrated Shipboard Networking System (ISNS) Compose 3.0 Increment 1 MOD 1 (C) CIN W-150-0101/Navy F School Provided	IAT I, II, III
TWMS-509392	Integrated Shipboard Networking System (ISNS) Compose 3.5 (D) CIN W-150-0800/Navy F School Provided	IAT I, II, III
TWMS-509393	Integrated Shipboard Networking System (ISNS) W/Compose 4.0 (D) CIN W-150-0800/Navy F School Provided	IAT I, II, III
EG_70290	MANAGING AND MAINTAINING A MICROSOFT WINDOWS SERVER 2003 ENVIRONMENT (EXAM 70-290) EXPRESS	IAT I, II, III
TWMS-509376	Microsoft Training for Exchange Server 2003 Infrastructure: Skillport/Vendor Provided	IAT I, II, III
TWMS-509377	Microsoft Training for Exchange Server 2007 Infrastructure: Skillport/Vendor Provided	IAT I, II, III
TWMS-509378	Microsoft Training for Exchange Server 2010 Infrastructure: Skillport/Vendor Provided	IAT I, II, III
TWMS-509379	Microsoft Training for Server 2003 Active Director: Skillport/Vendor Provided	IAT I, II, III
TWMS-509373	Microsoft Training for Server 2003 Network Infrastructure: Skillport/Vendor Provided	IAT I, II, III
TWMS-509380	Microsoft Training for Server 2008 Active Director: Skillport/Vendor Provided	IAT I, II, III
TWMS-509374	Microsoft Training for Server 2008 Network Infrastructure: Skillport/Vendor Provided	IAT I, II, III
TWMS-509375	Microsoft Training for Windows 7 Network Infrastructure: Skillport/Vendor Provided	IAT I, II, III
A-531-0021	NAVY TACTICAL COMMAND SUPPORT SYSTEM (NTCSS) II MANAGER	IAT I, II, III
TWMS-509398	Red Hat Certified System Administrator (RHCSA): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509403	Red Hat Certified Architect (RHCA): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509402	Red Hat Certified DataCenter Specialist (RHCDs): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509399	Red Hat Certified Engineer (RHCE): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509401	Red Hat Certified Security Specialist (RHCSs): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509400	Red Hat Certified Virtualization Administrator (RHCVa): Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509381	UNIX: Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509386	VM DataCenter Virtualization: Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509387	VM Desktop Virtualization: Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509388	VM VFabric: Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III
TWMS-509385	VMWare Certified Professional Infrastructure: Carnegie-Mellon/Skillport/Vendor Provided	IAT I, II, III

**Risk Management Framework (RMF) Changes in Terms
DIACAP -> RMF**

Old Term	New Term
<ul style="list-style-type: none"> • Certification and Accreditation (C&A) 	<ul style="list-style-type: none"> • Risk Management Framework (RMF)
<ul style="list-style-type: none"> • Certification 	<ul style="list-style-type: none"> • Assessment or • Security Control Assessment
<ul style="list-style-type: none"> • Accreditation 	<ul style="list-style-type: none"> • Authorization
<ul style="list-style-type: none"> • Requirements 	<ul style="list-style-type: none"> • Controls
<ul style="list-style-type: none"> • Protection Level <ul style="list-style-type: none"> - PL1/PL2 - PL3 - PL4/PL5 	<ul style="list-style-type: none"> • Accessibility <ul style="list-style-type: none"> - Baseline - Baseline + Accessibility Overlay - Baseline + CDS Overlay
<ul style="list-style-type: none"> • Level of Concern 	<ul style="list-style-type: none"> • Impact Level
<ul style="list-style-type: none"> • Security Requirements Traceability Matrix (SRTM) 	<ul style="list-style-type: none"> • Security <i>Controls</i> Traceability Matrix (SCTM)

**Risk Management Framework (RMF) Changes in Terms
DIACAP -> RMF**

Old Term	New Term
<ul style="list-style-type: none"> • System Security Authorization Agreement (SSAA) • System Security Plan (SSP) 	<ul style="list-style-type: none"> • System Security Plan (SSP)
<ul style="list-style-type: none"> • Certification Test and Evaluation (CT&E) • Security Test and Evaluation (ST&E) Report 	<ul style="list-style-type: none"> • Security Assessment Report (SAR)
<ul style="list-style-type: none"> • Designated Accrediting Authority (DAA) 	<ul style="list-style-type: none"> • Authorizing Official (AO) • Delegated AO (DAO)
<ul style="list-style-type: none"> • Certifier • Certification Authority • Service Certifying Organization (SCO) Information System Security Professional (ISSP) 	<ul style="list-style-type: none"> • Security Control Assessor (SCA)

**Risk Management Framework (RMF) Changes in Terms
DIACAP -> RMF**

Old Term	New Term
<ul style="list-style-type: none"> • Chief Information Assurance Officer (CIAO) 	<ul style="list-style-type: none"> • Chief Information Security Officer (CISO)/ Senior Information Security Officer (SISO)
<ul style="list-style-type: none"> • No equivalent 	<ul style="list-style-type: none"> • Risk Executive (function) (REf)
<ul style="list-style-type: none"> • No equivalent 	<ul style="list-style-type: none"> • Common Control Provider (CCP)
<ul style="list-style-type: none"> • No equivalent 	<ul style="list-style-type: none"> • Overlay (e.g. Accessibility, CDS, Standalone, etc.)
<ul style="list-style-type: none"> • Information Assurance Manager (IAM) 	<ul style="list-style-type: none"> • Information System Security Manager (ISSM)
<ul style="list-style-type: none"> • Information Assurance Officer (IAO) 	<ul style="list-style-type: none"> • Information System Security Officer (ISSO)

**Risk Management Framework (RMF) Changes in Terms
DIACAP -> RMF**

Old Term	New Term
<ul style="list-style-type: none"> • Program Manager 	<ul style="list-style-type: none"> • Information System Owner (ISO)
<ul style="list-style-type: none"> • Information System Security Engineer (ISSE) 	<ul style="list-style-type: none"> • ISSE • Information Assurance Systems Architect and Engineer (IASAE)
<ul style="list-style-type: none"> • Master SSP (MSSP) 	<ul style="list-style-type: none"> • Information Assurance Standard Operating Procedures (IA SOP)
<ul style="list-style-type: none"> • Guest System 	<ul style="list-style-type: none"> • External Information System
<ul style="list-style-type: none"> • Interim Approval to Operate (IATO) 	<ul style="list-style-type: none"> • Authorization to Operate (ATO) with a Plan of Actions and Milestones (POA&M)

Computer Information Systems Advisory Committee Meeting
Minutes
November 20, 2014

Members Present:

Name	Title	Company
Chris Harper	IT Infrastructure Manager	AltaOne
Tim Dawson	CEO	Approach Robotics
Kara Tolbert	Continuing Education Manger	Cerro Coso Community College
Valerie Karnes	Professor, CIS	Cerro Coso Community College
Frank Timpone	Professor, Business	Cerro Coso Community College
Karen O'Connor	Professor, BOT/Department Faculty Chair	Cerro Coso Community College
Lori Acton	Council Member	City of Ridgecrest
Melissa Olivarez	Operations Coordinator	Continental Labor
Daniel Johnson	Network & Controls Supervisor	Coso Operating Company
Sean Callahn	IT Director	Jacobs
Rich Christensen	Recruiter	Jacobs
Eileen Shibley	CEO	Monarch
Margaret Porter	Information Specialist	NAVAIR
Scott Fairfield	IT Specialist	NAVAIR
Linda Homer	Computer Scientist	NAVAIR
Kishor Joshi	Manager	Pertexa
Katherine Hu	Sr. Chemist/Environmental Lab Director	Searles Valley Mineral

The meeting was called to order by Valerie Karnes and the members present introduced themselves, who they worked for and their role in the organization. Several members were absent due to travel and/or work schedules. Minutes will be sent out following the meeting.

Minutes of the April 2014 meeting were reviewed and approved.

The committee purpose agenda was reviewed and employers raised the topic of internships/work experience and job shadowing as a need for most of the organizations. Discussion regarding our work experience courses, potential barriers to student completion and issues with security clearances for those working for the base. Advantages and benefits for students and employers in offering internships and work experience were also discussed. Students would benefit from real world experiences, which would enhance their education that could be noted on a resume. In addition, internships/work experiences could result in aiding in completion and job placement. Several attendees noted that they had internships while in school and that they not only enhanced their educational background, but also resulted in placements.

As Cerro Coso Community College work experience courses are not currently being offered, at this point there is no avenue for credit to be offered to students. A suggestion of offering a Work Experience certificate (new certificate) was brought forward as this would not change the current programs at the college, but will offer students a supplemental certificate that would be valued by employers. Valerie will check with the Counseling department and the CTE Dean to inquire about bringing these courses back and in the form of a certificate.

The Committee moved next to the Computer Information Systems program certificates that were brought forward for review.

The Data Analyst Certificate (12 units) certificate proposed the following courses below:

- ✓ BSAD 220 Principles of Project Management (3 units)
- ✓ BSAD 220 Problem Solving, Decision Making, and Computer Applications in Business (3 units)
- ✓ CSCI 251 Introduction to Visual Basic Programming (3 units)
- ✓ CSCI 270 Introduction to Database Design and Management (3 units)

The purpose of this certificate is to prepare students for positions in data collection, processing, and analysis and to provide a foundation for future training in big data analysis. The certificate would be offered online and includes four courses and could be completed in one year. The committee reviewed the certificate and approved it. The only suggestion was to have a SQL course. They indicated that there is a need and they would hire these students. One person from China Lake said that it would fit in the Configuration Management/ Data Management group at the base. They said they need an understanding of SQL but not Microsoft specific. They also said that the SQL could be in another course. Valerie will check with Matt Hightower about the content of CSCI C270 (Introduction to Database Design and Management) and inquire if SQL is included in the topics and assignments in this course.

The Information Technology Certificate (13 units) was reviewed next as a basic Information Technology certificate that would serve organizations hiring for various positions as noted in the purpose below.

The courses identified for this certificate are:

- ✓ CSCI C101: Introduction to Computer Information Systems (3 units)
- ✓ CSCI C140/141 A+ Essentials (4 units)
- ✓ CSCI C143: Network + and Fundamentals of Networking (3 units)
- ✓ CSCI C146: Security + Fundamentals (3 units)

The purpose of this certificate is to prepare students for entry-level positions in computer repair, networking, cyber security and general information systems jobs. The certificate would be offered online and includes four courses (13 units) and can be completed in one year. The committee endorsed

this certificate and said they would hire students with this type of certificate. It was noted that it would be good for students retraining with a desire to go into another field (IT). This proposed certificate would fit the need for students entering the Information Assurance positions (cyber security), basic help desk, entry-level network positions and general computer technicians. NAVAIR requires Security + certification prior to hiring, so this certificate fits their needs. Coso Operating company is currently hiring and A+ is a requirement and the addition of Security + would be a good thing to have for incoming employees. Sean Callahan (Jacobs) said the certificate is “perfect’ for what they need at Jacobs.

Discussion regarding the value of hands-on laboratories was discussed and the committee expressed that additional hands-on laboratories would be valuable to the students and the employers. It was suggested that we have students note the hands-on laboratories in their resumes so employers would know that they did labs physically and not virtually. We discussed the optional tutoring sessions that had been proposed through the Annual Unit Plan process as well as the updating of curriculum that Valerie Karnes, Matt Hightower and Chris Harper will be doing in the spring term. They were fully supportive of this as an option.

After the review of the certificate, the committee reviewed the CIS Model Curriculum and the committee supported the degree pathway as well. Questions arose about the need for an Operating Systems certification. Currently NAVAIR uses SkillPort/SkillSoft which is self paced program for incoming employees. They didn’t feel that we needed to add this to either the certificate or the degree program.

The Certification Testing Center at the college was brought up as a service for employers. They stated that this was a crucial service to the employers, students and community. They stated that the college needs to advertise this center more broadly so that potential candidates locally would know that they are able to take their exams on Friday at the college. Perhaps some advertising would be helpful.

Throughout the conversations regarding the CIS certificates and programs, employers noted that the ability of students to be computer literate and have MS Office experience was a basic skill that is required for any employment. Karen shared the Business Office Technology teaches these components and employers stated that the skills are an important basic skill that will lead to employment. Without these basic computer skills and MS Office knowledge, students would not be employable.

The question of CEU requirements for employees to keep their certifications current was raised. There is a need for those holding certifications to take 17 CEU a year (50 units over a three year program). Kara Tolbert from the Office of Continuing Education at the college brought up that the college could offer supplemental not for credit training to meet the needs of employers. She also talked about meeting the needs for customized training. Jacobs Technology and others will meet with Kara separately to discuss specific needs of the employers. Kara also talked about rolling out seminars and

other types of trainings to industry in the valley. There was a lot of interest in these types of professional services to the valley. Many of the employers were not aware that the college had this type of service and/or ability to provide customized education not for credit. Advertisement of these services and offering to the community needs to be expanded.

Karen O'Connor provided an update about the Computer Science AS-T and the challenge with the additional three units that caused the program to be rejected by the state. Employers asked if we can have multiple classes with various units or if there was another "creative" method we can use. Karen stated that we are working with the Science and Math departments to come up with a solution. She inquired about the need for this computer science transfer program and the employers unanimously supported the need for this program in our valley to support the mission of the Naval Air Warfare Center at China Lake, local contractors, new companies bringing up manufacturing and high technological businesses in Ridgecrest. Other businesses in the valley will also need those with computer science skill levels as technology continues to increase. Employers will be submitting letters of support for the continuation of the pursuit of an AS-T in Computer Science so the college can provide evidence to the State of California of the need for this transfer program and their support.

Other needs employers presented included the need for students competent in manufacturing processes including fiberglass, cybernetics, AutoCad, ProEngineering and SolidWorks software packages. Additional needs include students having a combination of computer skills and medical background (Medical Terminology and Physiology) , Chemistry background for laboratory positions at Searles Valley Minerals. Linux (Red Hat Enterprise edition) operating system is an emerging need that needs to be incorporated into our classes in CIS.

The next meeting date will be either in late spring or in the fall depending on the needs of industry and the progression of the new curriculum in the spring term.

ACTION ITEMS

- ✓ Valerie Karnes will check with the Counseling department and the CTE Dean to inquire about bringing Work Experiences courses back and explore the possibility of creating an additional certificate that would provide value to the students and employers. It would not impact current programs.
- ✓ Valerie Karnes will check with Matt Hightower about the content of CSCI C270 (Introduction to Database Design and Management) and inquire if SQL is included in the topics and assignments in this course.
- ✓ Valerie Karnes will complete the Advisory Minutes and send out on Monday, November 24, 2014 for review.
- ✓ Kara Tolbert will meet with Sean Callahan to follow up on the CEU needs for Jacobs's employees.

- ✓ Kara Tolbert will contact other employers about their needs for continuing education and community services for employers
- ✓ Employers will send letters of support for the Associate of Science degree for Transfer (AS-T) in Computer Science to Valerie Karnes and Karen O'Connor.

CIS Advisory Committee Members 2015-16

First Name	Last Name	Company Name	Program	Email	Phone
Harper	Christopher	AltaOne	CIS	chharper@cerrocoso.edu	
Tim	Dawson	Approach Engineering	Team Lead, Pertexa	dawson.superscale@gmail.com	
Damien	Jacotin	Burroughs High School	Project Lead the Way	djacotin@ssusd.org	
Suzanne	Ama	CCCC	Web Design	sama@cerrocoso.edu	
Jarrod	Bowen	CCCC	Admin of Justice Facutly	jarod.bowen@cerrocoso.edu	
Matt	Hightower	CCCC	CIS & Business	mhightower@cerrocoso.edu	
Mike	McNair	CCCC	CTE Dean	mike.mcnair@cerrocoso.edu	
Karen	O'Connor	CCCC	BIT Chair	koconnor@cerrocoso.edu	
Frank	Timpone	CCCC	Business	frank.timpone@cerrocoso.edu	
Kara	Tolbert	CCCC	Contract & Community Education	kara.tolbert@cerrocoso.edu	
Ashlin	Mattos	CCCC	Job Devlopment Specialist	ashlin.mattos@cerrocoso.edu	760-384-6128
Paula	Suorez	CCCCC	Director of Counseling	pasuorez@cerrocoso.edu	
Melissa	Oliverrez	Continental Labor	Staffing	ridgecrest@clsri.com	760-446-3525
Johnson	Daniel	Coso/Teragen contrastIT	CIS	daniel@contrastIT.net	760-301-5317
Mary	Lorber	Engility	Software Systems Engineer	mary.lorber.ctr@navy.mil	(760) 939-0875
Gary	Tomlin	Engility	Program Manager - ESS Contract	Gary.Tomlin@Engilitycorp.com	760-375-0390 X405
Vaughn	Corbridge	Htii	Aerospace, NAWC	vcorbridge@htii.com	760-939-8334
Nestor	Cora	Intrepid IT Solutions, LLC	Computer Repair/Networking	Nestor@intrepidits.com	760-382-7793
Sean	Callihan	Jacobs Engineering	CIS-CS	Sean.Callahan@jacobs.com	
Rich	Christenson	Jacobs Engineering	CIS-CS	rich.christensen@nsg.jacobs.com	
Tom	Della Santina	Jacobs Engineering	Aerospace, NAWC	thomas.dellasantina@nsg.jacobs.com	760-446-7670
Eileen	Shibley	Monarch	CEO	eileen.shibley@monarchmakers.com	
Katherine	Hu	Monarch/Searles Valley Mineral	Director of Business Development	katherine.hu@monarchmakers.com	(760) 377-7286
Margaret	Porter	NAVAIR	CyberSecurity	margaret.porter@navy.mil	760-939-3335
Alan	Van Nevel	NAVAIR	College Outreach	alan.vannevel@navy.mil	
Autumn	Piotrowski	NAVAIR Pending	Information Assurane	ak.petro0727@gmail.com	
Mark	Henderson	NAVAIR Weapons Division	Engineering - Computer Science	mark.henderson@navy.mil	
Linda	Homer	NAVAIR Weapons Division	Advanced Systems Development Office - Code 47K20D	Linda.Homer@navy.mil	760-939-6581
Wendy	Raglin	NAWC	Apprentice Training Coordinator	wendy.raglin@navy.mil	760-428-3927
John	Paul	NDTI	Director, High Desert Operations	john.paul@ndti.net	760-384-2444
Lori	Acton	Pertexa	Call Center/Medical Scribing/RoboDoc	lori@pertexa.com	661-301-5397
Kishor	Joshi	Pertexa	Robotics	Kishor@Pertexa.com	520-204-5957
Tim	Bode	Pertexa	Robotics		
Scott	Lougheed	Saalex	LSRS Program Manager	scott.lougheed@saalex.com	760-384-4209

**ESCC Area
Business and Information Technology
Advisory Committee Meeting
Spring 2014 (May 1, 2014)
Minutes**

Attendees: Suzie Ama, Deanna Campbell, Julie Faber, Joanie Hanson, Matt Hightower, Gina Jones

1. Introductions

2. Information and Communication Technology Model Curriculum

The group reviewed the proposed Information and Communication Technology model curriculum from the state. There was discussion about not having to implement it and having some flexibility in courses if we did. Comments in favor included cutting down the number of electives in the program and that the Java and PHP are specialty courses that, in practice, when the skills are needed in this area, are contracted out. There was also discussion regarding problem solving training. It was agreed that the program looked good, that there is a place for it, and that it provides a good foundation for on-the-job training.

3. Web Professional Program

Suzie presented the Web Professional program certification mapping for Jacobs training needs. Julie expressed the applied need to have more open-source CMS training (specifically WordPress) and that integrating social networking into the training would serve the program well. Suzie discussed the courses that provide some of that training. Julie also suggested that students obtain more depth in PHP training than they are currently obtaining from DMA C213. There was discussion about the rapid changes to the profession and the lack of need for a bachelor's degree to be employable in the local communities.

4. SAM 2013

There was discussion about the use of SAM in the applications courses. It was agreed to defer this to Karen and the BSOT program.

5. Business Leaders Observations and Recommendations

These were incorporated into the above discussions.

6. Adjournment

The meeting adjourned at 2:00PM.

**ESCC Area
Business and Information Technology
Advisory Committee Meeting
Spring 2015 (April 30, 2015)
via Video Conference, 1:00 – 1:55
Minutes**

Attendees: Deanna Campbell (Bishop), Chris Carmichael (Mammoth), Julie Faber (Bishop), Gina Jones (Bishop), Matt Hightower (Bishop), Karen O'Connor (IWV)

1. Introductions & Updates

The group welcomed the addition of Chris Carmichael (of Carmichael Business Technologies) to the committee. Chris described his business and the services that they offer locally and internationally.

2. Personnel Changes

Matt described Valerie Karnes' transition from Dean of CTE to faculty and the hiring of Mike McNair to fill the Dean's position.

3. Program Changes & Updates

○ **This Year**

▪ **Computer Science Deactivation**

Matt and Karen described the need to place the Computer Science program into a "deactivated" state due to the AS-T program's non-approval by the State. The non-approval was based on too many units in the program, which was attributed to higher than average units in the required Math and Physics courses. Karen pointed out that many schools in the state are in the same situation and that she has been asked to add the courses in the program to the schedule for those students that are currently in program.

▪ **Data Analyst I Certificate of Achievement**

The Data Analyst I program was approved by CIC this year. It will go to the Regional Consortium and then, if approved there, to the State for approval. The purpose of the program is prepare students for entry-level positions in the Data Analysis, Data Science, Big Data fields. Comments from the committee described the program as "perfect for remote workers in the ESCC" and added that it would be good for employees of government agencies and hospitals within the ESCC area and many other employers in the South County.

- **Web Fundamentals Certificate of Achievement**

The committee reviewed the Web Fundamentals Certificate of Achievement that was due for its second reading at CIC the following day (since approved). Due to other commitments, Suzie Ama could not attend the meeting but provided this description of the program for the committee.

The active Web Professional A.S and Certificate provide students with advanced and varied skills in web design and development. However, it is a high unit program, and we have identified a need for a mid-way academic milestone that effectively provides students with entry level skills in web design and development. More specifically, the Web Fundamentals Certificate will qualify students for jobs that entail maintenance and update of web sites (both static HTML and content management systems). They will be able to develop new web sites, and install and configure content management systems. And they will be able to create custom graphics and graphic user interfaces for the creation of new sites or the redesign of existing sites. Students will also have acquired experience working in teams and learned to communicate effectively with others.

Members of the committee were in favor of the certificate. There were some questions and suggestions for the future. There was a question about the use of Dreamweaver and the lack of identifiable specific topics in mobile applications and popular content management systems (CMS). It was suggested that one of Dreamweaver's purpose was that it was being used as an HTML debugging tool and that mobile applications and CMS use were integrated throughout the program.

- **Next Year**

- **CIS AS Degree and Certificate of Achievement**

As discussed at the last (5/1/14) ESCC Business and Information Technology Advisory Committee meeting, the CIS AS degree and Certificate of Achievement are being redesigned to follow the State's Model Curriculum. The redesign is in the queue for CIC for the beginning of next year.

- **Information Technology Plus Certificate of Achievement**

As part of the redesign of the CIS program, a new certificate is being developed. This certificate will have CIS 101, 142, 143, and 146 as the required courses. The committee was very enthusiastic about this certificate and viewed it being useful for employers in the service area. The outcome skills were identified as being essential and very “hireable” and the ability to have it offered online was viewed as a tremendous asset.

4. Student Club – Millionaires in the Making

Frank Timpone created a student club for Business students at the IWV campus. The club currently has 15 students, has officers, and is meeting for the second time this semester to finalize the creation process. The club’s name is “Millionaires in the Making”. The committee was enthusiastic about this as well and looks forward to hear more about it as it grows.

5. Adjournment

The meeting adjourned at 1:53PM.

Department of Business and Information Technology Advisory Committee: Fall 2014

Organization	Name	Contact Information
Bishop Chamber of Commerce Representative	Julie Faber Owner, Mountain Studio	760-872-1045 julie@mntstudio.com
Inyo County Superintendent of Schools Representative	Sophie Kenn Coordinator, ROP	760-873-3262 x. 411 sophie_kenn@inyo.k12.ca.us
Mammoth Lakes Chamber of Commerce Representative	Billy Gogesch Consultant Pupfish Design	650-257-0910 billyg@pupfishdesign.com
Mono County Superintendent of Schools Representative	Joe Griego Director, Information Technology	760-934-0031 jgriego@monocoe.org
Owens Valley Career Development Center Representative	Gina Jones Director	gjones@ovcdc.com 760-873-5107 2574 Diaz Lane Bishop, CA 93514 760-873-5107
Mammoth Mountain Ski Area Representative	Randy Broderick Director, Information Systems	760-934 -0688 rbroderick@mammoth-mtn.com
Bishop Area Representative at Large	Joanie Hanson Career Counselor	jhanson@ovcdc.com
Mammoth Lakes Representative at Large	Vickie Taton	vtaton@cerrocoso.edu
ESCC Representative	Deanna Campbell	dcampbel@cerrocoso.edu Director, ESCC 760-872-1565
Cerro Coso Community College, Ridgecrest	Karen O'Connor, Professor Faculty Chair	koconnor@cerrocoso.edu 760-384-6172
Cerro Coso Community College, Bishop	Matt Hightower, Professor	Bishop: 760-873-5312 Mammoth 760-924-1600
Cerro Coso Community College, Ridgecrest	April Browne, Instructor	april.browne@cerrocoso.edu 760-384-6171
Cerro Coso Community College, Ridgecrest	Frank Timpone, Assistant Professor	frank.timpone@cerrocoso.edu 760-384-6149
Cerro Coso Community College	Valerie Karnes, Dean Career Technical Education	vkarnes@cerrocoso.edu

**Computer Information Systems Advisory Committee Meeting
Minutes
November 19, 2015**

Members Present:

Name	Title	Company
Gerald Baker	NAWC, JT3 Department Manager	NAWC
Megan Callahan	Student	Cerro Coso Community College
Sean Callahan	IT Director	Jacobs
Mark Henderson	R&D Material Branch Head	NAWCWD
Linda Homer	Computer Scientist	NAVAIR
Valerie Karnes	Professor, CIS	Cerro Coso Community College
Amy Kennedy	Counseling Department	Cerro Coso Community College
Scott Lougheed	Program Manager	Saalex
Ashlin Mattos	Job Development Specialist	Cerro Coso Community College
Paul McKenzie	IA, System Administrator	Saalex
Karen O'Connor	Professor, BOT/Department Faculty Chair	Cerro Coso Community College
Melissa Olivarez	Operations Coordinator	Continental Labor
John Paul	Director	NDTI
Uwe Schmiedel	Director of Engineering	Monarch
Kara Tolbert	Continuing Education Manger	Cerro Coso Community College
Angel Zamarron	Pathways Program Coordinator	NAWC

Introductions

Valerie Karnes called the meeting to order and the members present introduced themselves, who they worked for and their role in the organization. Several members were absent due to travel and/or work schedules. Minutes will be sent out following the meeting.

A certificate of Appreciation was awarded to Sean Callahan of Jacobs who has served faithfully on the committee and has been instrumental in getting the first internship program started. He is moving to another job in January and will be a missed member of the Advisory Committee.

Minutes of the November 2015 meeting were reviewed and approved with no changes.

Committee Purpose and Overview

The purpose of the committee purpose and overview were reviewed. Employer advise and guidance to our programs is a critical component to the success of our programs.

Computer Information Systems/Business Information Worker Programs

The new Computer Information Systems program revised from the last meeting a year ago was reviewed and the committee was notified that the program work has been done and gone through the local college process and will be presented to the Kern Community College District Board of Directors in December. From there, it will go to the California Community College Chancellor's Office for state approval. We hope that March or April will approve the program in order to promote the program prior to registration for the summer and fall terms.

Karen O'Connor presented the new statewide program for Business Information Worker (BIW) and shared the components of our current Office Technology program.

The group discussed the value of hand-on training in the CIS program and/or a fully online program would be adequate. For the NAWC IT Apprenticeship program, Angel expressed the online program fits the needs of their workers, as they are required to work full time during the day. John Paul stated that the online flexibility was good for their workforce. After lengthy discussion, there was consensus in the value of hands-on experiences for the workforce and the hybrid model of having theory taught online with several required weekend (Flex Friday/Saturday) on campus would fit the needs of the employers and employees. Further discussion and needs for the volume of employees that would be needed in this area in the future suggests that one online section and perhaps one hybrid section would be needed to fill the online community and the IWW employers. Valerie will talk to administration about the possibility of running one hybrid section of CSCI C142, CSCI C143 and CSCI C146 in the course of a year to test the success of that model. The employers indicated that they would have the following needs for students in this pathway per year (Jacobs 30-40 employees per year, NAWC Apprenticeship Program 40-50 per year, Saalex 15 in the next six months with a 15% replacement rate each year, Continental Labor 6-10 per year and Monarch 1 per year). Other employers had to leave the meeting early or were not able to attend due to other commitments. Valerie will email and request their needs for annual employees. With over 100 potential placements per year, the college needs to expand the offerings to meet the employment needs in the Indian Wells Valley. From conversations at the meeting, this need is expected to increase each year. Employers are scrambling to hire in this area and sometimes end up hiring each other's employees to meet the needs. This is not a preferred method and they would like to have a pool to select future employees.

Karen O'Connor outlined the needs of college as far as any expansion to the course offerings and explained that if we offer the program on the campus, we need to know that there are sufficient students that would enroll. She asked about the best way for us to get the information to the employers and they indicated an email blast would be best.

Employers were asked if they would support the weekend labs and contribute to scenarios to prepare students to enter the job market. They would support and assist in the labs. The new Computer Information Systems Student Club will be meeting tomorrow to form and the labs could provide our current students with these experiences until a hybrid class could be offered. This will require a space at the college and equipment for both the student club and the future of an expanded program. Sean Callahan will send a configuration of what is needed to set up a network for these types of experiences.

Internships/Apprenticeship Programs

Sean Callahan outlines for the group the intermittent student employment program that he has championed at Jacobs. This employment program interviews top students in the CSCI C101 class that are on track to major in CIS and provides intermittent training and employment during the student college experience. During the time that they are not in class, they would go through a training program at Jacobs in Information Assurance, apply for a security clearance and be mentored for six months. As they complete their Security Plus class and certification, the students would be eligible for full time hire depending upon their performance as an intern.

Angel outlined the new NAWC Information Technology Apprenticeship program where students would work full time and take up to six units to continue their education. As the program is still in development, some of the details are yet to be worked out.

Other employers may be interested in developing similar internship/apprenticeship program and will work with Valerie and Ashlin.

Customized Training

Kara Tolbert outlined the customized training and reviewed with the committee the options that are available to them including non-credit professional development training, ETP funding and options for training. Kara offered to meet with them to outline the specific options for their organization. One offering that was discussed was the IT boot camps (A+, Net+ and Security+). The need for the PearsonVue training Center is also an important component that is needed by the base and the employers. Cerro Coso Community College lost its proctor due to an employee sudden death.

Industry needs - Cyber Security Certificate/Degree

The final discussion was about the new Cyber Security courses that are now being offered through C-ID at the college and the question about if the college needs a higher-level program than the Information Technology Plus certificate and Computer Information Systems degree. Do we need both programs?

The group reviewed the components and agreed that Cerro Coso Community College needs to develop not only a certificate, but a new Cyber Security Associate of Science degree and keep the Computer

Information Systems degree program as well. The programs would have the same first 4 classes (CSCI C101, 142, 143 and 146), but then would spin off into different directions.

The Computer Information Systems degree would serve the needs of computer operators, computer repair, computer networking and entry level to information assurance. It is important to keep this program, as it would fit the needs for IT professionals with a need for some security. There are also needs of Cyber Security that need a some IT content.

The Cyber Security program would serve the higher-level functions including cyber hacking, information security, computer forensics, and network defense. The Cyber Security program would meet the needs of their incumbent workforce for continual education. Employers stated that if a student completes a degree, they will be promoted and have an increase in salary. In the CIS and Cyber Security fields, continual education is crucial and employment is expected to continue to grow and expand. Paul will send Valerie the latest information on what would be required for the higher level program components and she will research the classes that will need to be developed and present it to the administration at the college. There will also be a need for dedicated classroom and additional faculty with expertise in these areas.

The meeting was adjourned at 1:10 pm.

Occupation Overview

EMSI Q3 2015 Data Set

February 2016

3000 College of Heights Blvd
Ridgecrest, California 93555
760.384.6258

Parameters

Occupations

Code	Description
15-1122	Information Security Analysts

Regions

Code	Description
6027	Inyo County, CA
6029	Kern County, CA
6051	Mono County, CA
6071	San Bernardino County, CA
6107	Tulare County, CA

Timeframe

2015 - 2020

Datarun

2015.3 - QCEW Employees

Information Security Analysts in 5 Counties

Information Security Analysts (SOC 15-1122):

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses. Excludes "Computer Network Architects" (15-1143).

Sample of Reported Job Titles:

Computer Security Specialist

Information Systems Security Officer

Security Analyst

Information Security Manager

Systems Analyst

Systems Administrator

Security Specialist

Security Director

Programmer Analyst

PC Analyst (Personal Computer Analyst)

Related O*NET Occupation:

Information Security Analysts (15-1122.00)

Occupation Summary for Information Security Analysts

<p>164 Jobs (2015) 77% below National average</p>	<p>+22.0% % Change (2015-2020) Nation: +16.4%</p>	<p>\$44.48/hr Median Hourly Earnings Nation: \$42.74/hr</p>
---	---	--

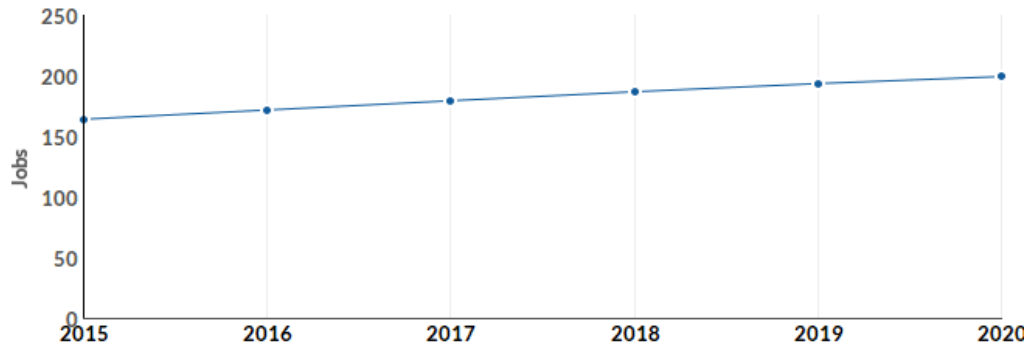
Growth for Information Security Analysts (15-1122)

164
2015 Jobs

200
2020 Jobs

36
Change (2015-2020)

22.0%
% Change (2015-2020)

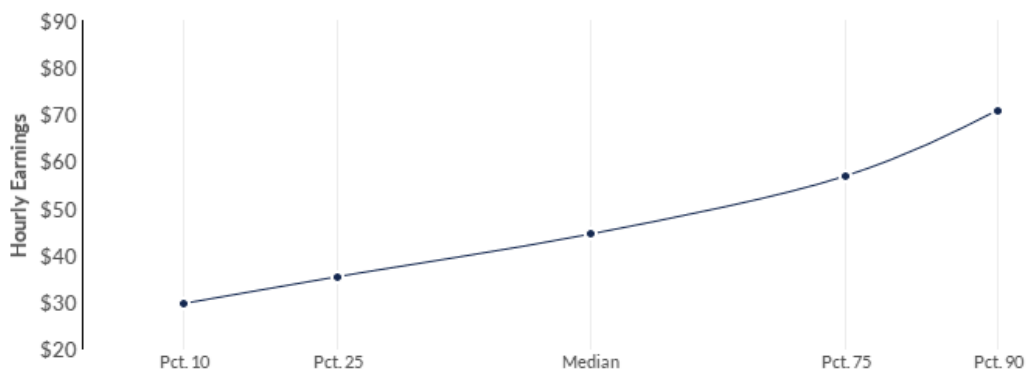


Percentile Earnings for Information Security Analysts (15-1122)

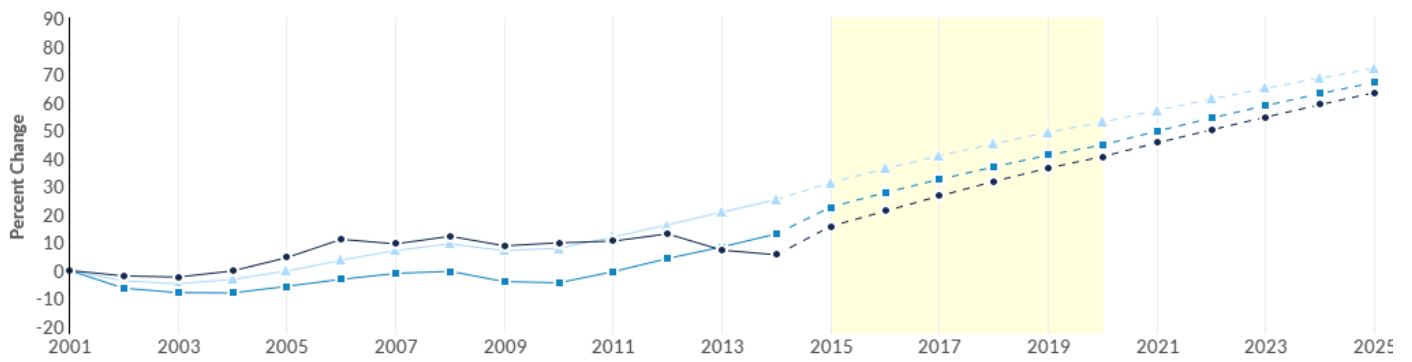
\$35.34/hr
25th Percentile Earnings

\$44.48/hr
Median Earnings

\$56.82/hr
75th Percentile Earnings

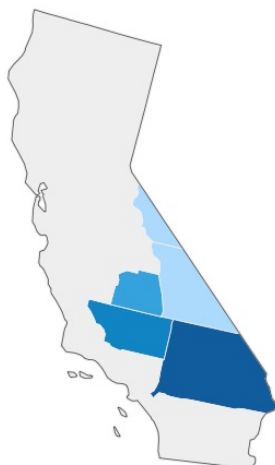


Regional Trends



Region	2015 Jobs	2020 Jobs	Change	% Change
● Region	164	200	36	22.0%
■ State	8,688	10,258	1,570	18.1%
▲ Nation	84,774	98,689	13,915	16.4%

Regional Breakdown



County	2020 Jobs
San Bernardino County, CA	110
Kern County, CA	67
Tulare County, CA	19
Inyo County, CA	<10
Mono County, CA	<10

Job Postings Summary

65

Unique Postings (Dec 2015)
262 Total Postings

4 : 1

Posting Intensity (Dec 2015)



There were 262 total job postings for *Information Security Analysts* in December 2015, of which 65 were unique. These numbers give us a Posting Intensity of 4-to-1, meaning that for every 4 postings there is 1 unique job posting.

This is close to the Posting Intensity for all other occupations and companies in the region (4-to-1), indicating they are putting average effort toward hiring this position.

Occupation Gender Breakdown



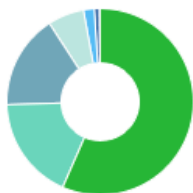
Gender	2015 Jobs	2015 Percent
● Males	123	75.0%
● Females	41	25.0%

Occupation Age Breakdown



Age	2015 Jobs	2015 Percent
14-18	0	0.1%
19-24	5	3.3%
25-34	45	27.2%
35-44	47	28.6%
45-54	34	20.7%
55-64	27	16.5%
65+	6	3.6%

Occupation Race/Ethnicity Breakdown



Race/Ethnicity	2015 Jobs	2015 Percent
White	93	56.6%
Hispanic or Latino	29	17.9%
Asian	27	16.4%
Black or African American	10	6.3%
Two or More Races	3	1.9%
American Indian or Alaska Native	1	0.8%
Native Hawaiian or Other Pacific Islander	0	0.2%

National Educational Attainment



Education Level	2015 Percent
Less than high school diploma	0.6%
High school diploma or equivalent	6.4%
Some college, no degree	22.0%
Associate's degree	14.4%
Bachelor's degree	34.0%
Master's degree	21.0%
Doctoral or professional degree	1.6%

Occupational Programs

11

Programs (2014)

503

Completions (2014)

17

Openings (2014)

CIP Code	Program	Completions (2014)
11.0901	Computer Systems Networking and Telecommunications	135
11.0103	Information Technology	127
11.0701	Computer Science	68
11.1002	System, Networking, and LAN/WAN Management/Manager	67
11.1003	Computer and Information Systems Security/Information Assurance	31

Industries Employing Information Security Analysts

Industry	Occupation Jobs in Industry (2015)	% of Occupation in Industry (2015)	% of Total Jobs in Industry (2015)
Other Computer Related Services	15	9.2%	0.6%
Corporate, Subsidiary, and Regional Managing Offices	13	7.9%	0.1%
Custom Computer Programming Services	<10	4.2%	0.6%
Local Government, Excluding Education and Hospitals	<10	4.0%	0.0%
Computer Systems Design Services	<10	3.9%	0.7%

Appendix A - Data Sources and Calculations

Location Quotient

Location quotient (LQ) is a way of quantifying how concentrated a particular industry, cluster, occupation, or demographic group is in a region as compared to the nation. It can reveal what makes a particular region unique in comparison to the national average.

Occupation Data

EMSI occupation employment data are based on final EMSI industry data and final EMSI staffing patterns. Wage estimates are based on Occupational Employment Statistics (QCEW and Non-QCEW Employees classes of worker) and the American Community Survey (Self-Employed and Extended Proprietors). Occupational wage estimates also affected by county-level EMSI earnings by industry.

Completers Data

The completers data in this report is taken directly from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

Institution Data

The institution data in this report is taken directly from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

Industry Data

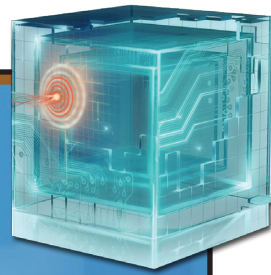
EMSI industry data have various sources depending on the class of worker. (1) For QCEW Employees, EMSI primarily uses the QCEW (Quarterly Census of Employment and Wages), with supplemental estimates from County Business Patterns and Current Employment Statistics. (2) Non-QCEW employees data are based on a number of sources including QCEW, Current Employment Statistics, County Business Patterns, BEA State and Local Personal Income reports, the National Industry-Occupation Employment Matrix (NIOEM), the American Community Survey, and Railroad Retirement Board statistics. (3) Self-Employed and Extended Proprietor classes of worker data are primarily based on the American Community Survey, Nonemployer Statistics, and BEA State and Local Personal Income Reports. Projections for QCEW and Non-QCEW Employees are informed by NIOEM and long-term industry projections published by individual states.

Staffing Patterns Data

The staffing pattern data in this report are compiled from several sources using a specialized process. For QCEW and Non-QCEW Employees classes of worker, sources include Occupational Employment Statistics, the National Industry-Occupation Employment Matrix, and the American Community Survey. For the Self-Employed and Extended Proprietors classes of worker, the primary source is the American Community Survey, with a small amount of information from Occupational Employment Statistics.

State Data Sources

This report uses state data from the following agencies: California Labor Market Information Department



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a diverse, qualified cybersecurity workforce is vital to our nation's security and prosperity.

[\[full text version\]](#)

DEFINING CYBERSECURITY

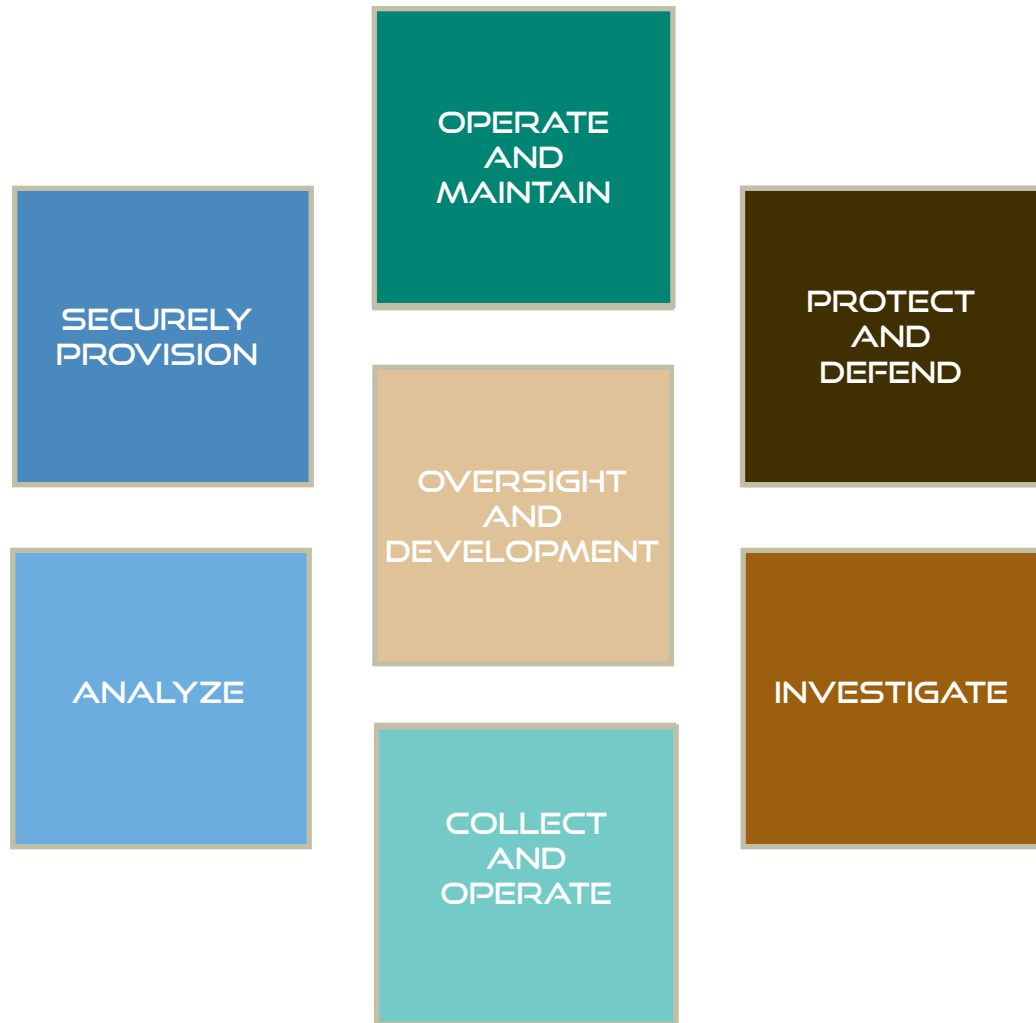
Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.

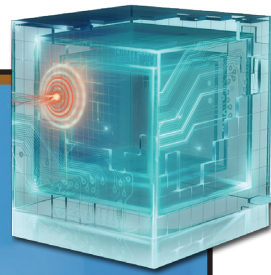
[\[full text version\]](#)

THE CALL TO ACTION

Only in the universal adoption of the *National Cybersecurity Workforce Framework* can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.

[\[full text version\]](#)





THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce is vital to our nation's security and prosperity.

Today, there is little consistency throughout the federal government and the nation in terms of how cybersecurity work is defined or described (e.g., there is significant variation in occupations, job titles, position descriptions, and the Office of Personnel Management [OPM] series). This absence of a common language to describe and understand cybersecurity work and requirements hinders our nation's ability to establish a baseline of capabilities, identify skills gaps, ensure an adequate pipeline of future talent, and continuously develop a highly-qualified cybersecurity workforce. Consequently, establishing and using a common lexicon, taxonomy, and other data standards for cybersecurity work and requirements is not merely desirable, it is vital.

The compelling need for enhanced public and private cybersecurity capabilities and a more enlightened public has been documented repeatedly over the last twenty years. Unfortunately, many of these issues have persisted over time and, by virtue of not improving, have become more acute. A National Research Council report lamented this problem in 2002:

The unfortunate reality is that relative to the magnitude of the threat, our ability and willingness to deal with threats have, on balance, changed for the worse, making many of the analyses, findings, and recommendations of these reports all the more relevant, timely, and applicable today. (National Research Council Computer Science and Telecommunications Board, 2002).

These challenges are exacerbated by the unique aspects of cybersecurity work. For example, the cybersecurity workforce must keep up with emerging risks, threats, vulnerabilities, and associated technologies that may require more rapid skill and knowledge acquisition than other functional areas. In fact, this requirement makes a compelling case for the need for innovative, robust private-public partnerships, and the capacity for cybersecurity talent to move more easily between public and private sector jobs and in and out of academia to maintain and develop skills and advance the collective knowledge base for future capabilities.

In recognition of the criticality of these issues, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The workforce aspect of the CNCI was specifically emphasized and reinforced in 2010 when President Obama established the National Initiative for Cybersecurity Education (NICE), which was formerly CNCI Initiative 8. The NICE is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Its goals are to encourage and help increase cybersecurity awareness and competence across the nation and to build an agile, highly skilled cybersecurity workforce capable of responding to a dynamic and rapidly evolving array of threats.

More information about the National Initiative for Cybersecurity Education can be found at <http://csrc.nist.gov/nice/>. This document is available online at <http://csrc.nist.gov/nice/framework/>

INTRODUCTION

DEFINING THE CYBERSECURITY WORKFORCE

THE CALL TO ACTION

Home

Using This Document

Sample Job Titles

Securely Provision

Operate and Maintain

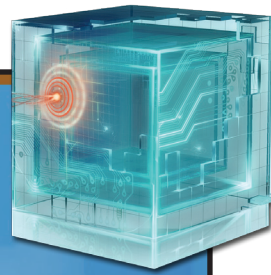
Protect and Defend

Investigate

Collect and Operate

Analyze

Oversight and Development



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

DEFINING THE CYBERSECURITY WORKFORCE

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The NICE, in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* (“the Framework”) to provide a common understanding of and lexicon for cybersecurity work.

The *National Cybersecurity Workforce Framework* establishes the common taxonomy and lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The Framework is intended to be applied in the public, private, and academic sectors. Use of the Framework does not require that organizations change organizational or occupational structures. In fact, the Framework was developed because requiring such changes would be costly, impractical, ineffective, and inefficient.

The Framework is agnostic to the particulars of a given organization and is overarching by design so that it can be overlaid onto any existing occupational structure to facilitate achieving an agile, highly-qualified cybersecurity workforce.

The Framework consists of thirty-one specialty areas organized into seven categories. These categories, serving as an overarching structure for the Framework, group related specialty areas together. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided.

This interactive document provides the Framework in its entirety.

The seven categories and a description of the types of specialty areas included in each are below

SECURELY PROVISION - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

OPERATE AND MAINTAIN - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

PROTECT AND DEFEND - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

INVESTIGATE - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

COLLECT AND OPERATE - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

ANALYZE - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

OVERSIGHT AND DEVELOPMENT - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

INTRODUCTION

DEFINING THE CYBERSECURITY WORKFORCE

THE CALL TO ACTION

Home

Using This Document

Sample Job Titles

Securely Provision

Operate and Maintain

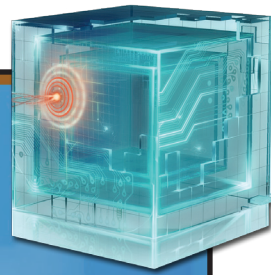
Protect and Defend

Investigate

Collect and Operate

Analyze

Oversight and Development



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

THE CALL TO ACTION

Only in the universal adoption of the National Cybersecurity Workforce Framework can we ensure our nation’s enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework’s lexicon (labels and definitions) as soon as possible.

The Framework is at the core of this vital capability as it enables all organizations to describe their cybersecurity work and workforces with an unprecedented level of consistency, detail, and quality. It is only with this understanding that organizations can analyze and explain the factors and dynamics that influence the workforce and work requirements. This in turn supports maturing to a predictive model that will anticipate requirements, gaps, needs, and other critical strategic and operational workforce issues.

For example, initially an organization may only know the attrition rates for a segment of the cybersecurity population. As it collects and analyzes the data and other information consistent with the Framework, it will mature in its understanding of cybersecurity retention issues, be able to identify root causes, know the extent of the potential impact of the attrition, and take appropriate action to prevent continued attrition. Finally, the desired end state is to predict workforce retention issues in advance and take actions to preempt them.

This approach is depicted in the figure below.



To achieve these goals, the Framework’s specified labels and definitions should be used when describing the corresponding work or workers; otherwise the inability to truly understand the cybersecurity workforce will persist and the nation will be unnecessarily vulnerable to risk.

While fidelity to the Framework labels and definitions is essential, the Framework is flexible by design and is intended to accommodate existing organizational structures. **The key is describing similar cybersecurity work, work requirements, and related skills using this common lexicon.**

Once organizations standardize their cybersecurity workforce information according to the Framework, the following initiatives can proceed in a meaningful, coherent, and cost-effective way across all sectors of the economy:

Collect and Analyze Data	Capture cybersecurity workforce and training data to understand capabilities and needs.
Recruit and Retain	Incentivize the hiring and retention of highly skilled and adaptive professionals needed for a secure digital nation.
Educate, Train, and Develop	Expand the pipeline for and deliberately develop an unrivaled cybersecurity workforce.
Engage	Educate and energize all cybersecurity workforces and the American public to strengthen the nation’s front lines of cybersecurity.

INTRODUCTION

DEFINING THE CYBERSECURITY WORKFORCE

THE CALL TO ACTION

Home

Using This Document

Sample Job Titles

Securely Provision

Operate and Maintain

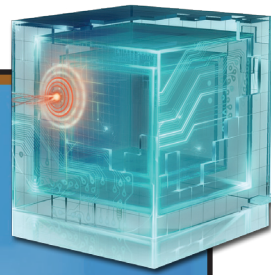
Protect and Defend

Investigate

Collect and Operate

Analyze

Oversight and Development



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES

The Framework is designed to be useful across all cybersecurity functions and organizations. The following list of sample job titles may be helpful as organizations adopt and prepare to use the Framework. It is important to note that this list is illustrative only and represents job titles that are frequently aligned with the indicated specialty area. A similar determination in any organization should be made based on a review of the work performed and the Framework.

The sample job titles are organized by specialty area in each category. Please note that no sample job titles are provided for the “Analyze” and “Collect and Operate” specialty areas in this document due to the unique and highly specialized nature of that work.

Securely Provision - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

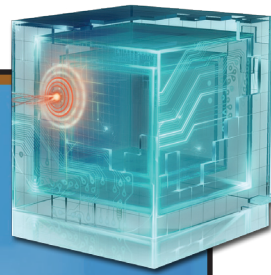
Information Assurance (IA) Compliance - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization’s information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

- Accreditor
- Auditor
- Authorizing Official Designated Representative
- Certification Agent
- Certifying Official
- Compliance Manager
- Designated Accrediting Authority
- Information Assurance (IA) Auditor
- Information Assurance (IA) Compliance Analyst/Manager
- Information Assurance (IA) Manager
- Information Assurance (IA) Officer
- Portfolio Manager
- Quality Assurance (QA) Specialist
- Risk/Vulnerability Analyst
- Security Control Assessor
- Systems Analyst
- Validator

Software Assurance and Security Engineering - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

- Analyst Programmer
- Computer Programmer
- Configuration Manager
- Database Developer/Engineer/Architect
- Information Assurance (IA) Engineer
- Information Assurance (IA) Software Developer
- Information Assurance (IA) Software Engineer
- Research & Development Engineer
- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

Systems Security Architecture - Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

- Information Assurance (IA) Architect
- Information Security Architect
- Information Systems Security Engineer
- Network Security Analyst
- Research & Development Engineer
- Security Architect
- Security Engineer
- Security Solutions Architect
- Systems Engineer
- Systems Security Analyst

Technology Research and Development - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

- Capabilities and Development Specialist
- Chief Engineer
- Research & Development Engineer

Systems Requirements Planning - 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.

- Business Analyst
- Business Process Analyst
- Computer Systems Analyst
- Human Factors Engineer
- Requirements Analyst
- Solutions Architect
- Systems Consultant
- Systems Engineer

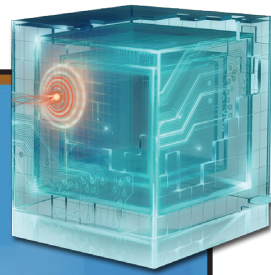
Test and Evaluation - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).

- Application Security Tester
- Information Systems Security Engineer
- Quality Assurance (QA) Tester
- Research & Development Engineer
- Research & Development Research Engineer
- Security Systems Engineer
- Software Quality Assurance (QA) Engineer
- Software Quality Engineer
- Systems Engineer
- Testing and Evaluation Specialist

Systems Development - Works on the development phases of the systems development lifecycle.

- Firewall Engineer
- Information Assurance (IA) Developer
- Information Assurance (IA) Engineer
- Information Assurance (IA) Software Engineer
- Information Systems Security Engineer
- Program Developer
- Security Engineer
- Systems Engineer
- Systems Security Engineer

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

Operate and Maintain - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Data Administration - Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

- Content Staging Specialist
- Data Architect
- Data Custodian
- Data Manager
- Data Warehouse Specialist
- Database Administrator
- Database Developer
- Database Engineer/Architect
- Information Dissemination Manager
- Systems Operations Personnel

Knowledge Management - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

- Business Analyst
- Business Intelligence Manager
- Content Administrator
- Document Steward
- Freedom of Information Act Official
- Information Manager
- Information Owner
- Information Resources Manager

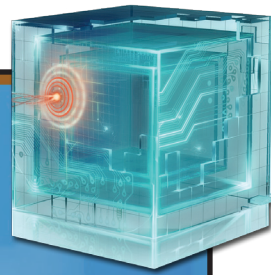
Customer Service and Technical Support - Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

- Computer Support Specialist
- Customer Support
- Help Desk Representative
- Service Desk Operator
- Systems Administrator
- Technical Support Specialist
- User Support Specialist

Network Services - 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.

- Cabling Technician
- Converged Network Engineer
- Network Administrator
- Network Analyst
- Network Designer
- Network Engineer
- Network Systems and Data Communications Analyst
- Network Systems Engineer
- Systems Engineer
- Telecommunications Engineer/Personnel/Specialist

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

System Administration - Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

- Local Area Network (LAN) Administrator
- Platform Specialist
- Security Administrator
- Server Administrator
- System Operations Personnel
- Systems Administrator
- Website Administrator

Systems Security Analysis - Conducts the integration/testing, operations, and maintenance of systems security.

- Information Assurance (IA) Operational Engineer
- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager
- Information Security Specialist
- Information Systems Security Engineer
- Information Systems Security Manager (ISSM)
- Platform Specialist
- Security Administrator
- Security Analyst
- Security Control Assessor
- Security Engineer

Protect and Defend - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

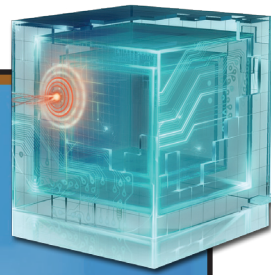
Computer Network Defense (CND) Analysis - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

- Computer Network Defense (CND) Analyst (Cryptologic)
- Cybersecurity Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- Security Analyst
- Security Operator
- Sensor Analyst

Incident Response - Responds to crisis 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.

- Computer Crime Investigator
- Incident Handler
- Incident Responder
- Incident Response Analyst
- Incident Response Coordinator
- Intrusion Analyst

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

Computer Network Defense (CND) Infrastructure Support - Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

- Information Systems Security Engineer
- Intrusion Detection System (IDS) Administrator
- Intrusion Detection System (IDS) Engineer
- Intrusion Detection System (IDS) Technician
- Network Administrator
- Network Analyst
- Network Security Engineer
- Network Security Specialist
- Security Analyst
- Security Engineer
- Security Specialist
- Systems Security Engineer

Vulnerability Assessment and Management - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

- Blue Team Technician
- Certified TEMPEST¹ Professional
- Certified TEMPEST¹ Technical Authority
- Close Access Technician
- Computer Network Defense (CND) Auditor
- Compliance Manager
- Ethical Hacker
- Governance Manager
- Information Security Engineer
- Internal Enterprise Auditor
- Penetration Tester
- Red Team Technician
- Reverse Engineer
- Risk/Vulnerability Analyst
- Technical Surveillance Countermeasures Technician
- Vulnerability Manager

Investigate - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

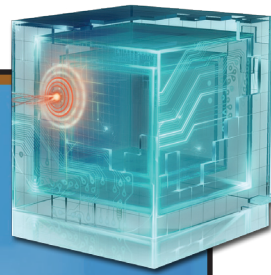
Digital Forensics - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

- Computer Forensic Analyst
- Computer Network Defense (CND) Forensic Analyst
- Digital Forensic Examiner
- Digital Media Collector
- Forensic Analyst
- Forensic Analyst (Cryptologic)
- Forensic Technician
- Network Forensic Examiner

Investigation - 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.

- Computer Crime Investigator
- Special Agent

¹ TEMPEST is a codename and not an acronym



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SAMPLE JOB TITLES (CONTINUED)

Oversight and Development - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Education and Training - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

- Cyber Trainer
- Information Security Trainer
- Security Training Coordinator

Information Systems Security Operations (Information Systems Security Officer [ISSO]) - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

- Contracting Officer (CO)
- Contracting Officer Technical Representative (COTR)
- Information Assurance (IA) Manager
- Information Assurance (IA) Program Manager
- Information Assurance (IA) Security Officer
- Information Security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Information Systems Security Operator

Legal Advice and Advocacy - 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.

- Legal Advisor/Staff Judge Advocate (SJA)
- Paralegal

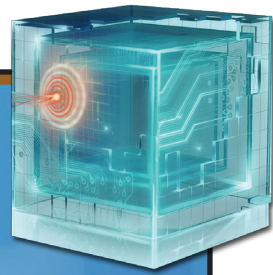
Security Program Management (Chief Information Security Officer [CISO]) - Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

- Chief Information Security Officer (CISO)
- Common Control Provider
- Cyber Security Officer
- Enterprise Security Officer
- Facility Security Officer
- Information Systems Security Manager (ISSM)
- Information Technology (IT) Director
- Principal Security Architect
- Risk Executive
- Security Domain Specialist
- Senior Agency Information Security (SAIS) Officer

Strategic Planning and Policy Development - Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

- Chief Information Officer (CIO)
- Command Information Officer
- Information Security Policy Analyst
- Information Security Policy Manager
- Policy Writer and Strategist

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

USING THIS DOCUMENT

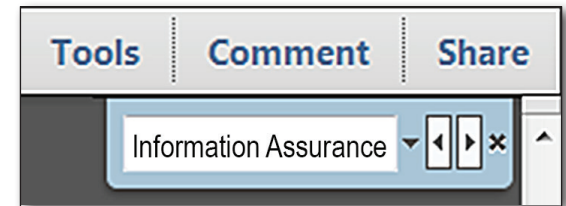
Navigating the Framework

To navigate to a particular Framework category from the Home page, click on one of the seven large category boxes or the smaller tabs at the bottom of the page. Tabs appear on every page, allowing you to easily navigate the Framework.

Once inside a Framework category, select a specific specialty area to explore it further. Selecting a specialty area will display a detailed view of that specialty area including associated tasks and KSAs. You can switch between the specialty area tasks or KSAs at any time by selecting the “Task” or “KSA” tab at the top of the list.

Searching the Framework

To search for a particular word or term, press “CTRL+F” and type the word or term in the “Find” box of the Adobe® Reader menu bar (typically in the upper right corner of the screen). Then press “Enter.” The small down arrow to the right of the “Find” box gives options for refining a search. The small left and right arrows search backwards and forwards in the document.



SECURELY PROVISION

Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, i.e., responsible for some aspect of systems development.

Information Assurance (IA) Compliance

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Software Assurance and Security Engineering

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Systems Security Architecture

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Technology Research and Development

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

Systems Requirements Planning

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.

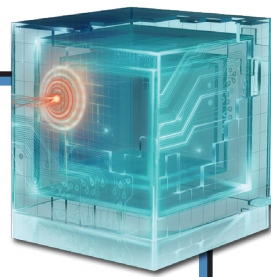
Test and Evaluation

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 information technology (IT).

Systems Development

Works on the development phases of the systems development lifecycle.

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



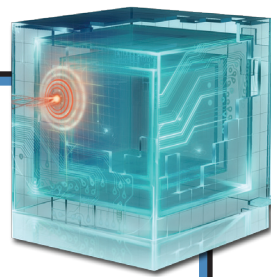
SECURELY PROVISION

INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization’s information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK	KSA
ID	Statement
537	Develop methods to monitor and measure risk, compliance, and assurance efforts
548	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level
566	Draft statements of preliminary or residual security risks for system operation
691	Maintain information systems assurance and accreditation materials
696	Manage and approve Accreditation Packages (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 15026-2)
710	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements
772	Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks
775	Plan and conduct security authorization reviews and assurance case development for initial installation of software applications, systems, and networks
798	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant information assurance (IA) compliances
827	Recommend new or revised security, resilience, and dependability measures based on the results of reviews
836	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network
878	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations
879	Verify that the software application/network/system accreditation and assurance documentation is current
936	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers)
937	Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



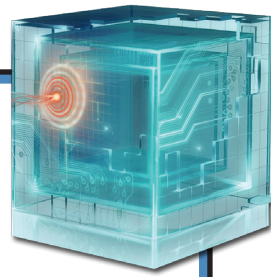
SECURELY PROVISION

INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization’s information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK	KSA	
ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
77	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	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
121	Knowledge of structured analysis principles and methods	Logical Systems Design
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
143	Knowledge of the organization’s enterprise information technology (IT) goals and objectives	Enterprise Architecture
183	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	Information Assurance
203	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	Information Technology Performance Assessment
942	Knowledge of the organization's core business/mission processes	Organizational Awareness

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



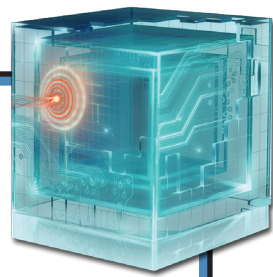
SECURELY PROVISION

INFORMATION ASSURANCE (IA) COMPLIANCE

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization’s information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

TASK		KSA
ID	Statement	Competency
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

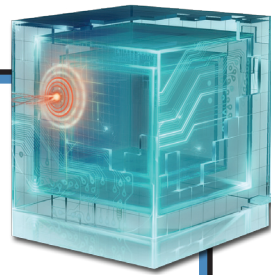
SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK ID	KSA	Statement
408		Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application
414		Analyze user needs and software requirements to determine feasibility of design within time and cost constraints
417		Apply coding and testing standards, apply security testing tools (including "fuzzing" static-analysis code scanning tools), and conduct code reviews
418		Apply secure code documentation
432		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
446		Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program
459		Conduct trial runs of programs and software applications to be sure they will produce the desired information and that the instructions are correct
461		Confer with systems analysts, engineers, programmers, and others to design applications and to obtain information on project limitations and capabilities, performance requirements, and interfaces
465		Develop threat model based on customer interviews and requirements
467		Consult with engineering staff to evaluate interface between hardware and software
477		Correct errors by making appropriate changes and rechecking the program to ensure that the desired results are produced
506		Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design
515		Develop and direct software system testing and validation procedures, programming, and documentation
543		Develop secure code and error messages
602		Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

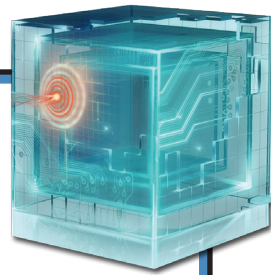
SOFTWARE ASSURANCE
AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK	KSA
ID	Statement
634	Identify basic common coding flaws at a high level
644	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development
645	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
709	Modify existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance
756	Perform integrated quality assurance testing for security functionality and resiliency from attacks
764	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities
770	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change
785	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
826	Recognize security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing
865	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
969	Perform penetration testing as required for new or updated applications
970	Apply defensive functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities of supply chain vulnerabilities
971	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements
972	Determine and document critical numbers of software patches or the extent of releases that would leave software vulnerable

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

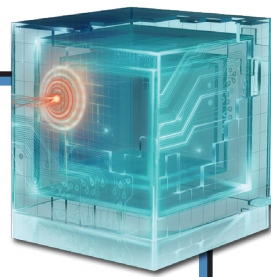
SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK		KSA
ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
20	Knowledge of complex data structures	Object Technology
23	Knowledge of computer programming principles such as object-oriented design	Object Technology
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
43	Knowledge of embedded systems	Embedded Computers
56	Knowledge of information assurance (IA) principles and methods that apply to software development	Information Assurance
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
74	Knowledge of low-level computer languages (e.g., assembly languages)	Computer Languages
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
102	Knowledge of programming language structures and logic	Computer Languages

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance		Software Assurance and Security Engineering		Systems Security Architecture		Technology Research and Development		Systems Requirements Planning		Test and Evaluation		Systems Development	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development				



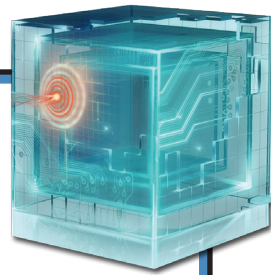
SECURELY PROVISION

SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK		KSA
ID	Statement	Competency
109	Knowledge of secure configuration management techniques	Configuration Management
116	Knowledge of software debugging principles	Software Development
117	Knowledge of software design tools, methods, and techniques	Software Development
118	Knowledge of software development models (e.g., waterfall model, spiral model)	Software Engineering
119	Knowledge of software engineering	Software Engineering
121	Knowledge of structured analysis principles and methods	Logical Systems Design
123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
149	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol (SOAP), and web service description language	Web Technology
168	Skill in conducting software debugging	Software Development
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation
174	Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams	Software Testing and Evaluation
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
185	Skill in developing applications that can log errors, exceptions, and application faults and logging	Software Development

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

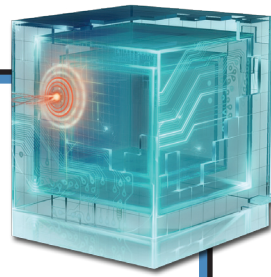
SOFTWARE ASSURANCE
AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK	KSA	
ID	Statement	Competency
191	Skill in developing and applying security system access controls	Identity Management
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
238	Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) in a modern programming language (e.g., Java, C++)	Computer Languages
904	Knowledge of interpreted and compiled computer languages	Computer Languages
905	Knowledge of secure coding techniques	Computer Languages
968	Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization)	Information Systems/Network Security
973	Skill in using code analysis tools to eradicate bugs	Software Development
974	Ability to tailor code analysis for application-specific concerns	Software Testing and Evaluation
975	Skill in integrating black box security testing tools into quality assurance process of software releases	Quality Assurance
976	Knowledge of software quality assurance process	Software Engineering
978	Knowledge of root cause analysis for incidents	Incident Management
979	Knowledge of supply chain risk management processes and practices	Risk Management
980	Skill in performing root cause analysis for incidents	Incident Management
1020	Skill in secure test plan design (i.e., unit, integration, system, acceptance)	Systems Testing and Evaluation

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



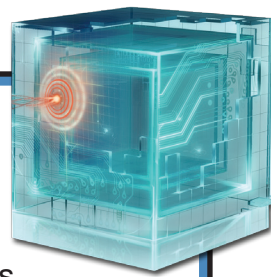
SECURELY PROVISION

SOFTWARE ASSURANCE AND SECURITY ENGINEERING

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

TASK		KSA
ID	Statement	Competency
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1071	Knowledge of secure software deployment methodologies, tools, and practices	Software Engineering
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

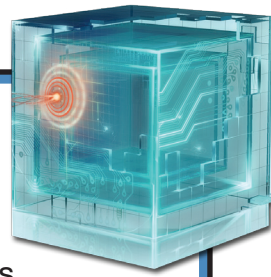
SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK	KSA
ID	Statement
413	Analyze user needs and requirements to plan system architecture
437	Collaborate with system developers and users to select appropriate design solutions or ensure the compatibility of system components
483	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event
484	Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements, to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recovery/restoration
502	Design system architecture or system components required to meet user needs
534	Develop information assurance (IA) designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET)
561	Document and address organization's information security, information assurance (IA) architecture, and systems security engineering requirements throughout the acquisition lifecycle
563	Document design specifications, installation instructions, and other system-related information
568	Employ secure configuration management processes
569	Ensure all definition and architecture activities (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials) are properly documented and updated as necessary
579	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's information assurance (IA) architecture guidelines
601	Evaluate current or emerging technologies to consider factors such as cost, security, compatibility, or usability
603	Evaluate interface between hardware and software and operational and performance requirements of overall system
631	Identify and prioritize critical business functions in collaboration with organizational stakeholders
646	Identify the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



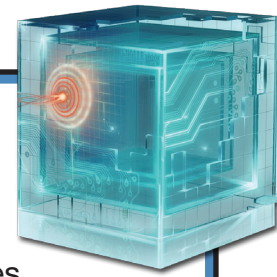
SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK	KSA
ID	Statement
765	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan
780	Plan system implementation to ensure that all system components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware)
797	Provide advice on project costs, design concepts, or design changes
807	Provide input on security requirements to be included in statements of work and other appropriate procurement documents
809	Provide input to the Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
849	Specify power supply and heating, ventilation, and air conditioning (HVAC) requirements and configuration based on system performance expectations and design specifications
864	Translate proposed technical solutions into technical specifications
994	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment
995	Document and manage an enterprise technical risk register, prioritizing and managing technical risks throughout the system lifecycle
996	Assess and design key management functions (as related to information assurance [IA])

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



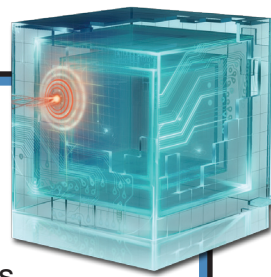
SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK		KSA
ID	Statement	Competency
8	Knowledge of access authentication methods	Identity Management
21	Knowledge of computer algorithms	Mathematical Reasoning
22	Knowledge of computer networking fundamentals	Infrastructure Design
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
43	Knowledge of embedded systems	Embedded Computers
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

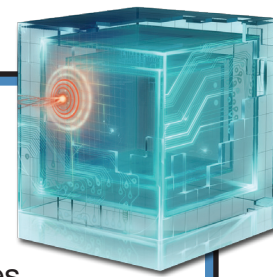
SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK	KSA	
ID	Statement	Competency
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
65	Knowledge of information theory	Mathematical Reasoning
68	Knowledge of information technology (IT) architectural concepts and frameworks	Information Technology Architecture
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



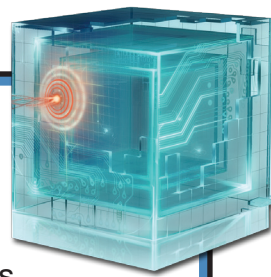
SECURELY PROVISION

SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK		KSA
ID	Statement	Competency
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
111	Knowledge of security system design tools, methods, and techniques	Information Systems/Network Security
113	Knowledge of server and client operating systems	Operating Systems
119	Knowledge of software engineering	Software Engineering
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
132	Knowledge of technology integration processes	Systems Integration
133	Knowledge of telecommunications concepts	Telecommunications
141	Knowledge of the enterprise information technology (IT) architecture	Information Technology Architecture
143	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
180	Skill in designing the integration of hardware and software solutions	Systems Integration

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

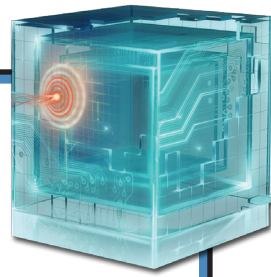
SYSTEMS SECURITY ARCHITECTURE

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

TASK	KSA	
ID	Statement	Competency
183	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	Information Assurance
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
904	Knowledge of interpreted and compiled computer languages	Computer Languages
993	Knowledge of 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])	Enterprise Architecture
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development

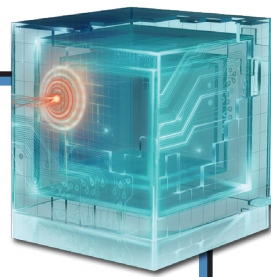


SECURELY PROVISION

TECHNOLOGY RESEARCH AND DEVELOPMENT

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

TASK	KSA
ID	Statement
455	Conduct continuous analysis to identify network and system vulnerabilities
520	Develop and implement data mining and data warehousing programs
925	Research current technology to understand capabilities of required system or network
927	Research and evaluate all available technologies and standards to meet customer requirements
934	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements
1076	Collaborate with stakeholders to identify and/or develop appropriate solutions technology
1077	Design and develop new tools/technologies
1078	Troubleshoot prototype design and process issues throughout the product design, development, and post-launch phases
1079	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate cyberspace vulnerabilities
1080	Identify and/or develop reverse engineering tools to detect cyberspace vulnerabilities



SECURELY PROVISION

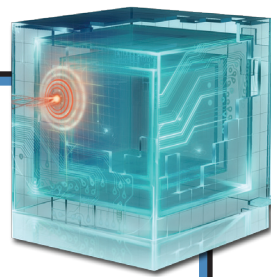
TECHNOLOGY RESEARCH AND DEVELOPMENT

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

TASK	KSA	
ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
10	Knowledge of application vulnerabilities	Vulnerabilities Assessment
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware	Hardware
27	Knowledge of cryptology	Cryptography
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
132	Knowledge of technology integration processes	Systems Integration
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

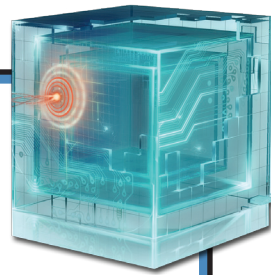
TECHNOLOGY RESEARCH AND DEVELOPMENT

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

TASK	KSA	
ID	Statement	Competency
180	Skill in designing the integration of hardware and software solutions	Systems Integration
238	Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) in a modern programming language (e.g., Java, C++)	Computer Languages
321	Knowledge of products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky) and how differences affect exploitation/vulnerabilities	Technology Awareness
371	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [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)	Operating Systems
905	Knowledge of secure coding techniques	Computer Languages
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1042	Ability to apply network programming towards client/server model	Requirements Analysis
1044	Skill in identifying forensic footprints	Computer Forensics
1047	Skill in writing kernel level applications	Software Development
1052	Knowledge of Global Systems for Mobile Communications (GSM) architecture	Telecommunications

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



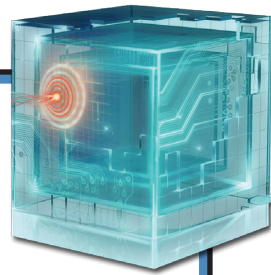
SECURELY PROVISION

TECHNOLOGY RESEARCH AND DEVELOPMENT

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

TASK		KSA
ID	Statement	Competency
1054	Knowledge of hardware reverse engineering techniques	Vulnerabilities Assessment
1055	Knowledge of middleware	Software Development
1056	Knowledge of operations security	Public Safety and Security
1059	Knowledge of networking protocols	Infrastructure Design
1061	Knowledge of the lifecycle process	Systems Life Cycle
1062	Knowledge of software reverse engineering techniques	Vulnerabilities Assessment
1063	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications)	Operating Systems
1064	Knowledge of Extensible Markup Language (XML) schemas	Infrastructure Design
1066	Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (penetration and testing)	Vulnerabilities Assessment
1067	Skill in utilizing network analysis tools to identify software communications vulnerabilities	Vulnerabilities Assessment
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



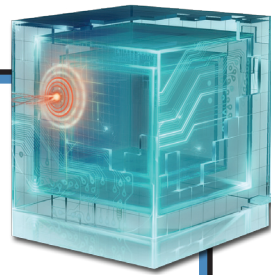
SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

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.

TASK ID	KSA	Statement
458		Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications
466		Consult with customers to evaluate functional requirements
476		Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions
487		Define project scope and objectives based on customer requirements
511		Develop an enterprise system security context, a preliminary system security concept of operations, and define baseline system security requirements in accordance with applicable information assurance (IA) requirements
517		Develop and document requirements, capabilities, and constraints for design procedures and processes
528		Develop cost estimates for future new or modified system(s)
669		Integrate and align information security and/or information assurance (IA) policies to ensure system analysis meets security requirements
700		Manage information technology (IT) projects to ensure that developed solutions meet customer requirements
726		Oversee and make recommendations regarding configuration management
760		Perform needs analysis to determine opportunities for new and improved business process solutions
789		Prepare use cases to justify the need for specific information technology (IT) solutions
863		Translate functional requirements into technical solutions
1003		Develop and document supply chain risks for critical system elements, as appropriate

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



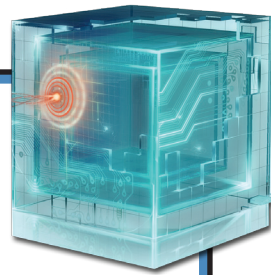
SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

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.

TASK		KSA
ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
16	Knowledge of capabilities and requirements analysis	Requirements Analysis
22	Knowledge of computer networking fundamentals	Infrastructure Design
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
27	Knowledge of cryptology	Cryptography
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
64	Knowledge of information security systems engineering principles	Information Systems/Network Security
65	Knowledge of information theory	Mathematical Reasoning

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



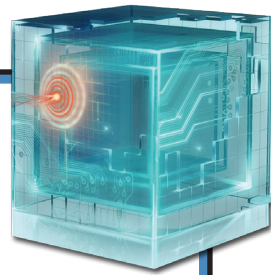
SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

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.

TASK		KSA
ID	Statement	Competency
68	Knowledge of information technology (IT) architectural concepts and frameworks	Information Technology Architecture
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
101	Knowledge of process engineering concepts	Logical Systems Design
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



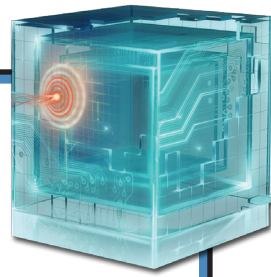
SECURELY PROVISION

SYSTEMS REQUIREMENTS PLANNING

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.

TASK		KSA
ID	Statement	Competency
110	Knowledge of security management	Information Assurance
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
143	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
144	Knowledge of the systems engineering process	Systems Life Cycle
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
156	Skill in applying confidentiality, integrity, and availability principles	Information Assurance
158	Skill in applying organization-specific systems analysis principles and techniques	Systems Testing and Evaluation
162	Skill in conducting capabilities and requirements analysis	Requirements Analysis
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
229	Skill in using incident handling methodologies	Incident Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

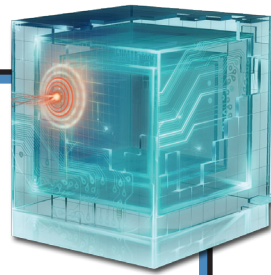
SYSTEMS REQUIREMENTS PLANNING

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.

TASK		KSA
ID	Statement	Competency
911	Ability to interpret and translate customer requirements into operational cyber actions	Requirements Analysis
1002	Skill in conducting audits or reviews of technical systems	Information Technology Performance Assessment
1004	Knowledge of critical information technology (IT) procurement requirements	Contracting/Procurement
1005	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)	Contracting/Procurement
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development

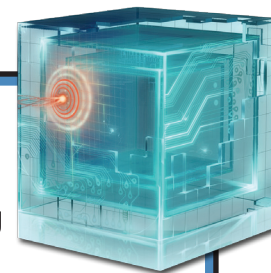


SECURELY PROVISION

TEST AND EVALUATION

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 information technology (IT).

TASK	KSA
ID	Statement
412	Analyze the results of end-to-end testing (e.g., software, hardware, transport, seams, interfaces)
508	Determine level of assurance of developed capabilities based on test results
550	Develop test plans to address specifications and requirements
694	Make recommendations based on test results
747	Perform conformance testing to assess whether a system complies with defined specifications or standards
748	Perform developmental testing on systems being concurrently developed
757	Perform interoperability testing on systems exchanging electronic information with systems of other organizations
761	Perform operational testing to evaluate systems in the operational environment
773	Perform validation testing to ensure that requirements meet proposed specifications or standards and that correct specifications or standards are available
858	Test and verify hardware and support peripherals to ensure that they meet specifications and requirements by recording and analyzing test data
951	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated
1006	Create auditable evidence of security measures



SECURELY PROVISION

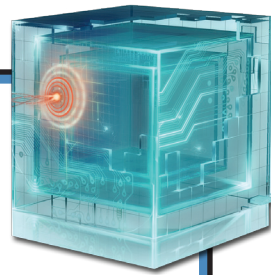
TEST AND EVALUATION

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 information technology (IT).

TASK	KSA	
ID	Statement	Competency
22	Knowledge of computer networking fundamentals	Infrastructure Design
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
83	Knowledge of network hardware devices and functions	Hardware
127	Knowledge of systems administration concepts	Operating Systems
144	Knowledge of the systems engineering process	Systems Life Cycle
169	Skill in conducting test events	Systems Testing and Evaluation
176	Skill in designing a data analysis structure (i.e., the types of data the test must generate and how to analyze those data)	Systems Testing and Evaluation
182	Skill in determining an appropriate level of test rigor for a given system	Systems Testing and Evaluation
190	Skill in developing operations-based testing scenarios	Systems Testing and Evaluation
220	Skill in systems integration testing	Systems Testing and Evaluation
239	Skill in writing test plans	Systems Testing and Evaluation
904	Knowledge of interpreted and compiled computer languages	Computer Languages

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

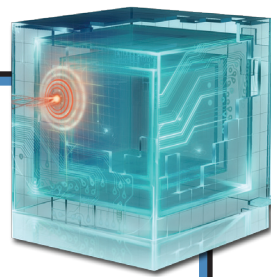
TEST AND EVALUATION

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 information technology (IT).

TASK		KSA
ID	Statement	Competency
950	Skill in evaluating test plans for applicability and completeness	Systems Testing and Evaluation
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

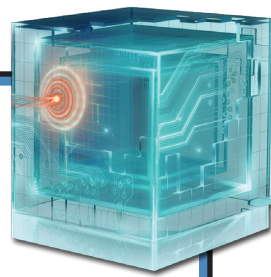
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA
ID	Statement
416	Analyze design constraints, trade-offs, and detailed system and security designs to identify necessary lifecycle support
419	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications
425	Assess the effectiveness of information protection measures utilized by system(s)
426	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile
431	Build, test, and modify product prototypes using working or theoretical models
457	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII)
494	Design and develop information assurance (IA) or IA-enabled products
495	Design and develop secure interface specifications between interconnected systems
496	Design, develop, integrate, and update system security measures (including policies and requirements) that provide confidentiality, integrity, availability, authentication, and non-repudiation
500	Design hardware, operating systems, and software applications to adequately address information assurance (IA) security requirements
501	Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data
503	Design to minimum security requirements to ensure requirements are met for all systems and/or applications
516	Develop and direct system testing and validation procedures and documentation
527	Develop architectures or system components consistent with technical specifications
530	Develop detailed security design documentation for component and interface specifications to support system design and development
531	Develop disaster recovery and continuity of operations plans for systems under development, and ensure testing prior to systems entering a production environment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

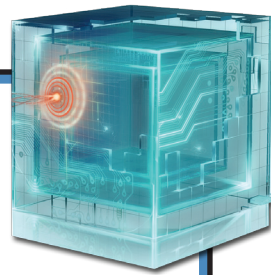
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA
ID	Statement
542	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed
547	Develop specific information assurance (IA) countermeasures and risk mitigation strategies for systems and/or applications
626	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements
630	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)
632	Identify and prioritize essential system functions or sub-systems, as may be necessary to support essential capabilities or business functions; in the event of system failure or system recovery, observe and adhere to overall system requirements for continuity and availability
648	Identify, assess, and recommend information assurance (IA) or IA-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements
659	Implement security designs for new or existing system(s)
662	Incorporate information assurance (IA) vulnerability solutions into system designs (e.g., IA vulnerability alerts)
737	Perform an information security risk assessment and design security countermeasures to mitigate identified risks
766	Perform security reviews and identify security gaps in security architecture
770	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change
803	Provide guidelines for implementing developed systems to customers or installation teams
808	Provide input to implementation plans and standard operating procedures
809	Provide input to the Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



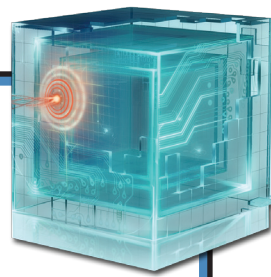
SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA
ID	Statement
850	Store, retrieve, and manipulate data for analysis of system capabilities and requirements
856	Provide support to security/certification test and evaluation activities
860	Trace all system security requirements to design components
874	Utilize models and simulations to analyze or predict system performance under different operating conditions
877	Verify stability, interoperability, portability, or scalability of system architecture
997	Design and develop key management functions (as related to information assurance [IA])
998	Analyze user needs and requirements to plan and conduct system security development
999	Develop information assurance (IA) 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 [SCI])
1000	Ensure that security design and information assurance (IA) development activities are properly documented, providing a functional description of security implementation, and updated as necessary

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



SECURELY PROVISION

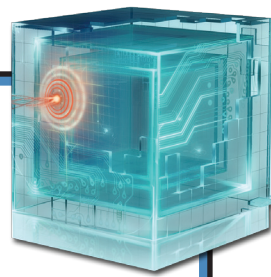
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA	
ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
8	Knowledge of access authentication methods	Identity Management
21	Knowledge of computer algorithms	Mathematical Reasoning
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
27	Knowledge of cryptology	Cryptography
34	Knowledge of database systems	Database Management Systems
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
43	Knowledge of embedded systems	Embedded Computers
46	Knowledge of fault tolerance	Information Assurance
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
64	Knowledge of information security systems engineering principles	Information Systems/Network Security
65	Knowledge of information theory	Mathematical Reasoning

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

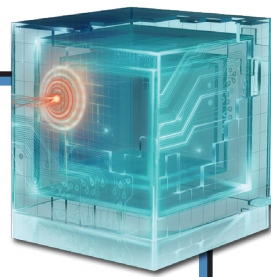
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK		KSA
ID	Statement	Competency
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management	Infrastructure Design
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
101	Knowledge of process engineering concepts	Logical Systems Design

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

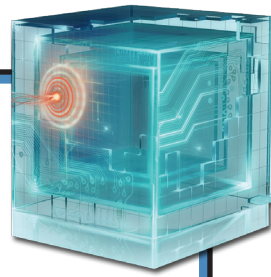
SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA	
ID	Statement	Competency
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
118	Knowledge of software development models (e.g., waterfall model, spiral model)	Software Engineering
119	Knowledge of software engineering	Software Engineering
121	Knowledge of structured analysis principles and methods	Logical Systems Design
124	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools	Logical Systems Design
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
173	Skill in creating policies that reflect system security objectives	Information Systems Security Certification
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
179	Skill in designing security controls based on information assurance (IA) principles and tenets	Information Assurance
180	Skill in designing the integration of hardware and software solutions	Systems Integration
191	Skill in developing and applying security system access controls	Identity Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



SECURELY PROVISION

SYSTEMS DEVELOPMENT

Works on the development phases of the systems development lifecycle.

TASK	KSA	
ID	Statement	Competency
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
199	Skill in evaluating the adequacy of security designs	Vulnerabilities Assessment
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
904	Knowledge of interpreted and compiled computer languages	Computer Languages
1002	Skill in conducting audits or reviews of technical systems	Information Technology Performance Assessment
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

OPERATE AND MAINTAIN

Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Data Administration

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Customer Service and Technical Support

Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Network Services

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.

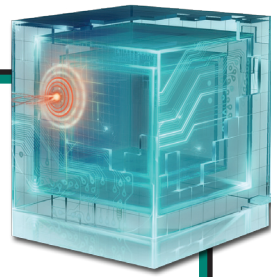
System Administration

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Systems Security Analysis

Conducts the integration/testing, operations, and maintenance of systems security.

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



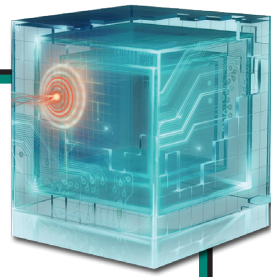
OPERATE AND MAINTAIN

DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

TASK	KSA
ID	Statement
400	Analyze and define data requirements and specifications
401	Analyze and plan for anticipated changes in data capacity requirements
498	Design and implement database systems
520	Develop and implement data mining and data warehousing programs
529	Develop data standards, policies, and procedures
664	Install and configure database management systems software
684	Maintain database management systems software
688	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing
690	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required
702	Manage the compilation, cataloging, caching, distribution, and retrieval of data
712	Monitor and maintain databases to ensure optimal performance
740	Perform backup and recovery of databases to ensure data integrity
796	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements
815	Provide recommendations on new database technologies and architectures

Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	System Security Analysis				
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



OPERATE AND MAINTAIN

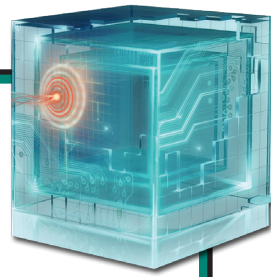
DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

TASK	KSA	
ID	Statement	Competency
28	Knowledge of data administration and data standardization policies and standards	Data Management
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
31	Knowledge of data mining and data warehousing principles	Data Management
32	Knowledge of database management systems, query languages, table relationships, and views	Database Management Systems
35	Knowledge of digital rights management	Encryption
44	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
90	Knowledge of operating systems	Operating Systems
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
104	Knowledge of query languages such as Structured Query Language (SQL)	Database Management Systems
120	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
137	Knowledge of the characteristics of physical and virtual data storage media	Data Management
152	Skill in allocating storage capacity in the design of data management systems	Database Administration
166	Skill in conducting queries and developing algorithms to analyze data structures	Database Management Systems
178	Skill in designing databases	Database Administration
186	Skill in developing data dictionaries	Data Management
187	Skill in developing data models	Modeling and Simulation

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	System Security Analysis				
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



OPERATE AND MAINTAIN

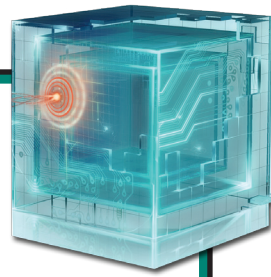
DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

TASK		KSA
ID	Statement	Competency
188	Skill in developing data repositories	Data Management
201	Skill in generating queries and reports	Database Management Systems
208	Skill in maintaining databases	Database Management Systems
213	Skill in optimizing database performance	Database Administration
910	Knowledge of database theory	Data Management
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	System Security Analysis				
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development

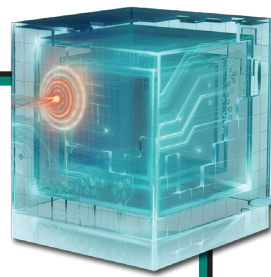


OPERATE AND MAINTAIN

KNOWLEDGE MANAGEMENT

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

TASK	KSA
ID	Statement
394	Administer the indexing/cataloguing, storage, and access of organizational documents
464	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users
505	Design, build, implement, and maintain a knowledge management system that provides end-users access to the organization's intellectual capital
513	Develop an understanding of the needs and requirements of information end-users
519	Develop and implement control procedures into the testing and development of core information technology (IT) based knowledge management systems
721	Monitor the usage of knowledge management assets
777	Plan and manage the delivery of knowledge management projects
794	Promote knowledge sharing through an organization's operational processes and systems by strengthening links between knowledge sharing and information technology (IT) systems
814	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information



OPERATE AND MAINTAIN

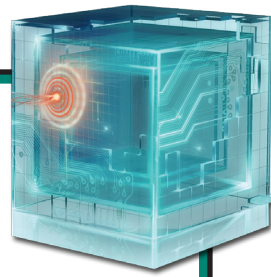
KNOWLEDGE MANAGEMENT

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

TASK	KSA	
ID	Statement	Competency
5	Ability to match the appropriate knowledge repository technology for a given application or environment	Knowledge Management
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
77	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	Information Systems/Network Security
134	Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs)	Technology Awareness
135	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines)	Data Management
136	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint)	Technology Awareness
163	Skill in conducting information searches	Computer Skills
164	Skill in conducting knowledge mapping (i.e., map of knowledge repositories)	Knowledge Management
223	Skill in the measuring and reporting of intellectual capital	Knowledge Management
230	Skill in using knowledge management technologies	Knowledge Management
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
907	Skill in data mining techniques	Data Management
910	Knowledge of database theory	Data Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



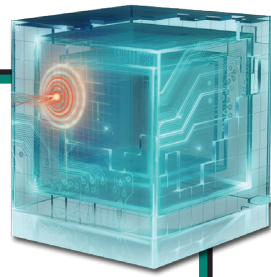
OPERATE AND MAINTAIN

KNOWLEDGE MANAGEMENT

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

TASK		KSA
ID	Statement	Competency
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

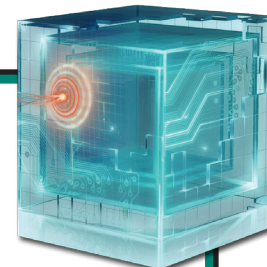


OPERATE AND MAINTAIN

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

TASK		KSA
ID	Statement	
428	Assist in the execution of disaster recovery and continuity of operations plans	
554	Diagnose and resolve customer reported system incidents	
639	Identify end-user requirements for software and hardware	
665	Install and configure hardware, software, and peripheral equipment for system users	
695	Manage accounts, network rights, and access to systems and equipment	
698	Manage inventory of information technology (IT) resources	
714	Monitor client-level computer system performance	
813	Provide recommendations for possible improvements and upgrades	
830	Report emerging trend findings	
859	Test computer system performance	
866	Troubleshoot system hardware and software	



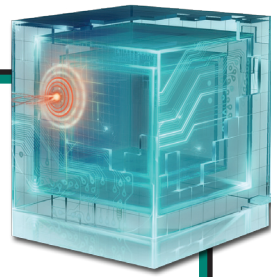
OPERATE AND MAINTAIN

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

TASK	KSA	
ID	Statement	Competency
7	Knowledge of “knowledge base” capabilities for identifying the solutions to less common and more complex system problems	Knowledge Management
33	Knowledge of database procedures used for documenting and querying reported incidents	Incident Management
37	Knowledge of disaster recovery and continuity of operations plans	Incident Management
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
127	Knowledge of systems administration concepts	Operating Systems
142	Knowledge of the operations and processes for diagnosing common or recurring system problems	Systems Life Cycle
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly	Systems Life Cycle
165	Skill in conducting open source research for troubleshooting novel client-level problems	Knowledge Management
204	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation	Systems Life Cycle
221	Skill in testing and configuring network workstations and peripherals	Network Management
222	Skill in the basic operation of computers	Computer Skills
235	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system	Computers and Electronics
264	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)	Computers and Electronics

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



OPERATE AND MAINTAIN

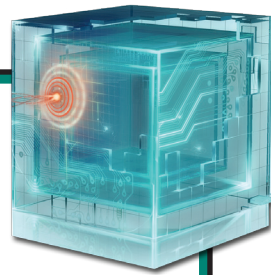
CUSTOMER SERVICE AND TECHNICAL SUPPORT

Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

TASK		KSA
ID	Statement	Competency
281	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])	Hardware
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



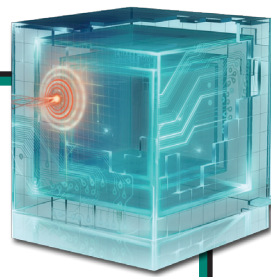
OPERATE AND MAINTAIN

NETWORK SERVICES

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.

TASK	KSA
ID	Statement
462	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling)
522	Develop and implement network backup and recovery procedures
555	Diagnose network connectivity problems
617	Expand or modify network infrastructure to serve new purposes or improve work flow
656	Implement new system design procedures, test procedures, and quality standards
666	Install and maintain network infrastructure device operating system software (e.g., Internetwork Operating System [IOS], firmware)
667	Install or replace network hubs, routers, and switches
673	Integrate new systems into existing network architecture
718	Monitor network capacity and performance
736	Patch network vulnerabilities to ensure information is safeguarded against outside parties
802	Provide feedback on network requirements, including network architecture and infrastructure
829	Repair network connectivity problems
857	Test and maintain network infrastructure including software and hardware devices

Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	System Security Analysis				
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



OPERATE AND MAINTAIN

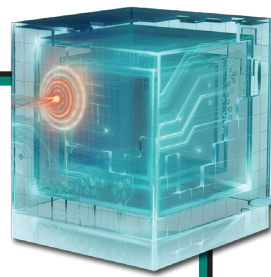
NETWORK SERVICES

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.

TASK		KSA	
ID	Statement		Competency
12	Knowledge of communication methods, principles, and concepts (e.g., cryptography, dual hubs, time multiplexers) that support the network infrastructure		Infrastructure Design
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware		Hardware
41	Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways		Infrastructure Design
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data		Information Assurance
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)		Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management		Infrastructure Design
76	Knowledge of measures or indicators of system performance and availability		Information Technology Performance Assessment
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])		Infrastructure Design
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])		Infrastructure Design
106	Knowledge of remote access technology concepts		Information Technology Architecture
112	Knowledge of server administration and systems engineering theories, concepts, and methods		Systems Life Cycle
133	Knowledge of telecommunications concepts		Telecommunications

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

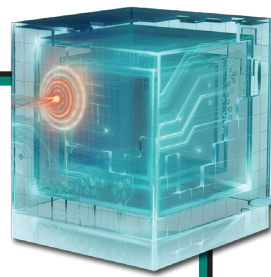
NETWORK SERVICES

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.

TASK	KSA	
ID	Statement	Competency
148	Knowledge of Virtual Private Network (VPN) security	Encryption
154	Skill in analyzing network traffic capacity and performance characteristics	Capacity Management
193	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans	Information Assurance
198	Skill in establishing a routing schema	Infrastructure Design
205	Skill in implementing, maintaining, and improving established network security practices	Information Systems/Network Security
207	"Skill in installing, configuring, and troubleshooting Local Area Network (LAN) and	
231	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)	Network Management
234	Skill in using sub-netting tools	Infrastructure Design
261	Knowledge of basic concepts, terminology, and operations of a wide range of communications media (e.g., computer and telephone networks, satellite, fiber, wireless)	Telecommunications
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup)	Infrastructure Design
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN])	Telecommunications
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)	Operating Systems
891	Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers)	Configuration Management
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

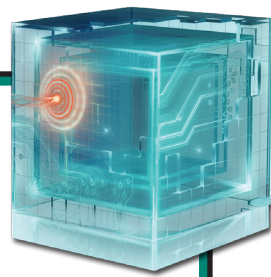
NETWORK SERVICES

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.

TASK	KSA		
ID	Statement	Competency	
900	Knowledge of web filtering technologies	Web Technology	
901	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, Voice over Internet Protocol [VoIP], Instant Messenger [IM], web forums, direct video broadcasts)	Network Management	
902	"Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fidelity [Wi-Fi],		
903	Knowledge of Wireless Fidelity (Wi-Fi)	Network Management	
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management	
989	Knowledge of Voice over Internet Protocol (VoIP)	Telecommunications	
990	Knowledge of the common attack vectors on the network layer	Computer Network Defense	
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security	
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security	
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management	
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications	

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



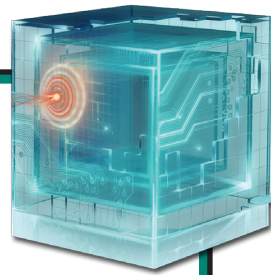
OPERATE AND MAINTAIN

SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

TASK	KSA
ID	Statement
434	Check server availability, functionality, integrity, and efficiency
452	Conduct functional and connectivity testing to ensure continuing operability
456	Conduct periodic server maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing
499	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs
518	Develop and document systems administration standard operating procedures
521	Develop and implement local network usage policies and procedures
668	Install server fixes, updates, and enhancements
683	Maintain baseline system security according to organizational policies
695	Manage accounts, network rights, and access to systems and equipment
701	Manage server resources including performance, capacity, availability, serviceability, and recoverability
713	Monitor and maintain server configuration
728	Oversee installation, implementation, configuration, and support of network components
763	Perform repairs on faulty server hardware
776	Plan and coordinate the installation of new or modified hardware, operating systems, and other baseline software
781	Plan, execute, and verify data redundancy and system recovery procedures
811	Provide ongoing optimization and problem-solving support
835	Resolve hardware/software interface and interoperability problems

Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	System Security Analysis				
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



OPERATE AND MAINTAIN

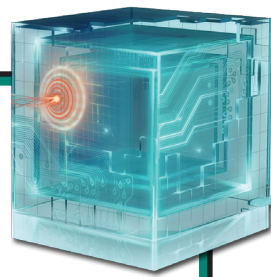
SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

TASK		KSA	
ID	Statement		Competency
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)		Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management		Infrastructure Design
76	Knowledge of measures or indicators of system performance and availability		Information Technology Performance Assessment
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])		Infrastructure Design
89	Knowledge of new technological developments in server administration		Technology Awareness
96	Knowledge of performance tuning tools and techniques		Information Technology Performance Assessment
99	Knowledge of principles and methods for integrating server components		Systems Integration
112	Knowledge of server administration and systems engineering theories, concepts, and methods		Systems Life Cycle
113	Knowledge of server and client operating systems		Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques		Computer Forensics
127	Knowledge of systems administration concepts		Operating Systems
141	Knowledge of the enterprise information technology (IT) architecture		Information Technology Architecture
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly		Systems Life Cycle
148	Knowledge of Virtual Private Network (VPN) security		Encryption

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

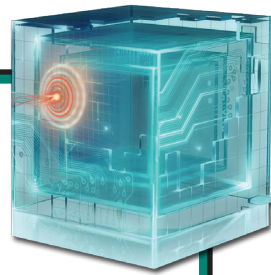
SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

TASK	KSA	
ID	Statement	Competency
167	Skill in conducting server planning, management, and maintenance	Network Management
170	Skill in configuring and optimizing software	Software Engineering
171	Skill in correcting physical and technical problems which impact server performance	Network Management
194	Skill in diagnosing connectivity problems	Network Management
195	Skill in diagnosing failed servers	Network Management
202	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems	Information Technology Performance Assessment
206	Skill in installing computer and server upgrades	Systems Life Cycle
209	Skill in maintaining directory services	Identity Management
211	Skill in monitoring and optimizing server performance	Information Technology Performance Assessment
216	Skill in recovering failed servers	Incident Management
219	Skill in system administration for Unix/Linux operating systems	Operating Systems
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)	Operating Systems
287	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT])	Operating Systems
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)	Computer Languages
344	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems
386	Skill in using virtual machines	Operating Systems

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



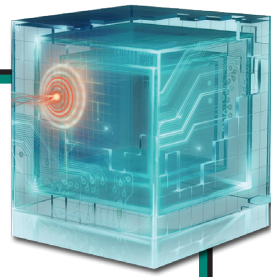
OPERATE AND MAINTAIN

SYSTEM ADMINISTRATION

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

TASK		KSA	
ID	Statement	Competency	
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)	Configuration Management	
986	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)	Identity Management	
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security	
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security	
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security	
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications	

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



OPERATE AND MAINTAIN

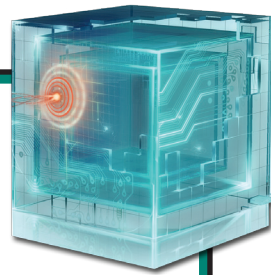
SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

TASK	KSA
ID	Statement
419	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications
420	Apply security policies to meet security objectives of the system
421	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements
525	Develop and test system fail-over or system operations transfer to an alternate site based on system availability requirements
559	Discover organizational trends with regard to the security posture of systems
571	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary
572	Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment
576	Ensure information assurance-enabled products or other compensating security control technologies reduce identified risk to an acceptable level
593	Establish adequate access controls based on principles of least privilege and need-to-know
616	Exercise the system disaster recovery and continuity of operations plans
652	Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines
653	Implement security designs and approaches to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed
660	Implement specific information assurance (IA) countermeasures for systems and/or applications
661	Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation
670	Integrate and/or implement Cross-Domain Solutions (CDS) in a secure environment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

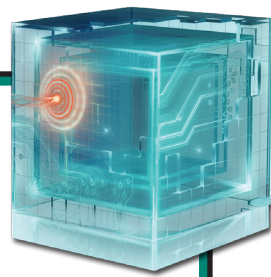
SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

TASK	KSA
ID	Statement
671	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
708	Mitigate/correct security deficiencies identified during security/certification testing, or identify risk acceptance for the appropriate senior leader or authorized representative
717	Monitor information protection assurance mechanisms related to system implementation and testing practices
729	Oversee minimum security requirements are in place for all applications
754	Perform information assurance (IA) testing of developed applications and/or systems
767	Perform security reviews and identify security gaps in security architecture, resulting in recommendations for inclusion into the risk mitigation strategy
782	Plan and recommend modifications or adjustments based on exercise results or system environment
795	Properly document all systems security implementation, operations, and maintenance activities and update as necessary
806	Provide information assurance (IA) guidance to leadership
809	Provide input to the Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
876	Verify and update security documentation reflecting the application/system security design features
880	Work with others to resolve computer security incidents and vulnerability compliance
938	Ensure Recovery and Continuity plans are executable in the system operational environment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

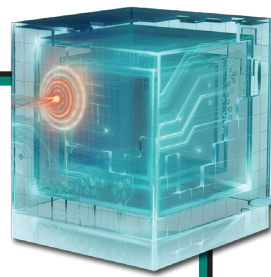
SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

TASK		KSA	
ID	Statement	Competency	
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment	
18	Knowledge of circuit analysis	Computers and Electronics	
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography	
27	Knowledge of cryptology	Cryptography	
34	Knowledge of database systems	Database Management Systems	
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering	
43	Knowledge of embedded systems	Embedded Computers	
46	Knowledge of fault tolerance	Information Assurance	
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration	
52	Knowledge of human-computer interaction principles	Human Factors	
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security	
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance	
65	Knowledge of information theory	Mathematical Reasoning	
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security	

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

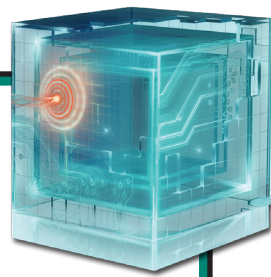
SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

TASK	KSA	
ID	Statement	Competency
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
111	Knowledge of security system design tools, methods, and techniques	Information Systems/Network Security
119	Knowledge of software engineering	Software Engineering
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
133	Knowledge of telecommunications concepts	Telecommunications
144	Knowledge of the systems engineering process	Systems Life Cycle
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		



OPERATE AND MAINTAIN

SYSTEMS SECURITY ANALYSIS

Conducts the integration/testing, operations, and maintenance of systems security.

TASK		KSA
ID	Statement	Competency
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
179	Skill in designing security controls based on information assurance (IA) principles and tenets	Information Assurance
183	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	Information Assurance
191	Skill in developing and applying security system access controls	Identity Management
199	Skill in evaluating the adequacy of security designs	Vulnerabilities Assessment
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Data Administration		Knowledge Management		Customer Service and Technical Support		Network Services		System Administration		System Security Analysis	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development		

PROTECT AND DEFEND

Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

Computer Network Defense (CND) Analysis

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Incident Response

Responds to crisis 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.

Computer Network Defense (CND) Infrastructure Support

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

Vulnerability Assessment and Management

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 non-operational situations.

Computer Network
Defense (CND) Analysis

Incident
Response

Computer Network Defense (CND)
Infrastructure Support

Vulnerability Assessment
and Management

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

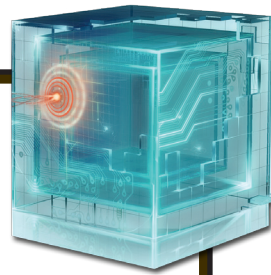
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



PROTECT AND DEFEND

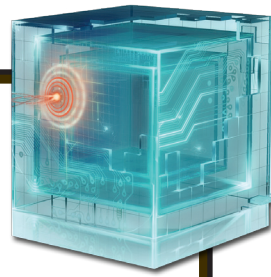
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA
ID	Statement
427	Develop content for computer network defense (CND) tools
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
472	Coordinate with enterprise-wide computer network defense (CND) staff to validate network alerts
716	Monitor external data sources (e.g., computer network defense [CND] vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the enterprise
723	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
745	Perform computer network defense (CND) trend analysis and reporting
750	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
800	Provide daily summary reports of network events and activity relevant to computer network defense (CND) practices
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
956	Provide timely detection, identification, and alerts of possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents and events from benign activities
958	Use computer network defense (CND) tools for continual monitoring and analysis of system activity to identify malicious activity
959	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, and effects on system and information
961	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis		Incident Response		Computer Network Defense (CND) Infrastructure Support		Vulnerability Assessment and Management			
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA
ID	Statement
1010	Determine appropriate course of action in response to identified and analyzed anomalous network activity
1102	Conduct tests of information assurance (IA) safeguards in accordance with established test plans and procedures
1103	Determine tactics, techniques, and procedures (TTPs) for intrusion sets
1104	Examine network topologies to understand data flows through the network
1105	Recommend computing environment vulnerability corrections
1107	Identify and analyze anomalies in network traffic using metadata
1108	Conduct research, analysis, and correlation across a wide variety of all source data sets (e.g., indications and warnings)
1109	Validate Intrusion Detection System (IDS) alerts against network traffic using packet analysis tools
1110	Triage malware
1111	Identify applications and operating systems of a network device based on network traffic
1112	Reconstruct a malicious attack or activity based on network traffic
1113	Identify network mapping and operating system fingerprinting activities

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network
Defense (CND) Analysis

Incident
Response

Computer Network Defense (CND)
Infrastructure Support

Vulnerability Assessment
and Management

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

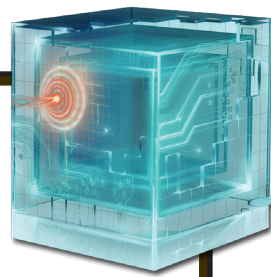
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



PROTECT AND DEFEND

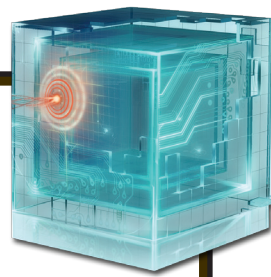
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA	
ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
27	Knowledge of cryptology	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
59	Knowledge of Intrusion Detection System (IDS) tools and applications	Computer Network Defense
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
66	Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies	Computer Network Defense
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis		Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management		
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



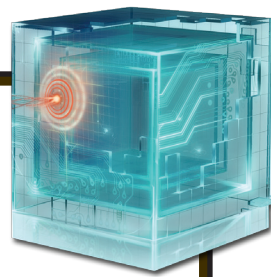
PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA	
ID	Statement	Competency
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
102	Knowledge of programming language structures and logic	Computer Languages
105	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)	Vulnerabilities Assessment
110	Knowledge of security management	Information Assurance
115	Knowledge of content development	Computer Network Defense
138	Knowledge of the computer network defense (CND) service provider reporting structure and processes within one's own organization	Information Systems/Network Security
148	Knowledge of Virtual Private Network (VPN) security	Encryption
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
165	Skill in conducting open source research for troubleshooting novel client-level problems	Knowledge Management
175	Skill in developing and deploying signatures	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



PROTECT AND DEFEND

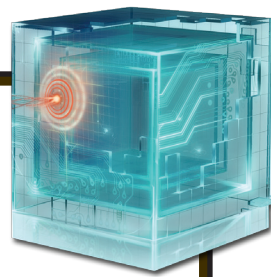
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA	
ID	Statement	Competency
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
212	Skill in network mapping and recreating network topologies	Infrastructure Design
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	Vulnerabilities Assessment
229	Skill in using incident handling methodologies	Incident Management
233	Skill in using protocol analyzers	Vulnerabilities Assessment
234	Skill in using sub-netting tools	Infrastructure Design
270	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities)	Computer Network Defense
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup)	Infrastructure Design
277	Knowledge of defense-in-depth principles and network security architecture	Computer Network Defense
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN])	Telecommunications
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)	Operating Systems
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)	Computer Languages
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)	Operating Systems
353	Skill in collecting data from a variety of computer network defense resources	Computer Network Defense

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis		Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management		
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



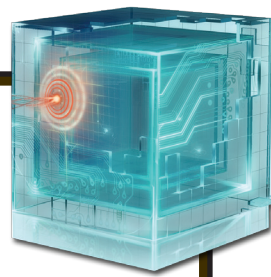
PROTECT AND DEFEND

COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK		KSA
ID	Statement	Competency
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
912	Knowledge of collection management processes, capabilities, and limitations	Configuration Management
915	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection	Information Systems/Network Security
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management
990	Knowledge of the common attack vectors on the network layer	Computer Network Defense
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1007	Skill in data reduction	Data Management
1008	Knowledge of how to troubleshoot basic systems and identify operating systems-related issues	Operating Systems
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



PROTECT AND DEFEND

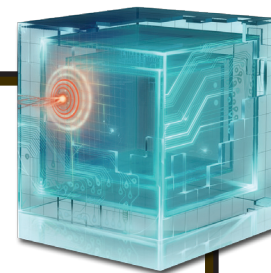
COMPUTER NETWORK DEFENSE (CND) ANALYSIS

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

TASK	KSA	
ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1114	Knowledge of encryption methodologies	Cryptography
1115	Skill in reading Hexadecimal data	Computer Languages
1116	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)	Computer Languages
1117	Skill in utilizing virtual networks for testing	Operating Systems
1118	Skill in reading and interpreting signatures (e.g., Snort)	Information Systems/Network Security
1119	Knowledge of signature implementation impact	Information Systems/Network Security
1120	Ability to interpret and incorporate data from multiple tool sources	Data Management
1121	Knowledge of Windows/Unix ports and services	Operating Systems

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

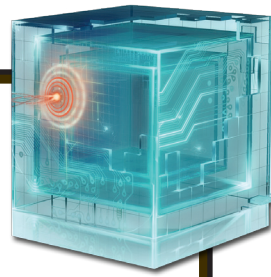
INCIDENT RESPONSE

Responds to crisis 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.

TASK	KSA
ID	Statement
470	Coordinate with and provide expert technical support to enterprise-wide computer network defense (CND) technicians to resolve CND incidents
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
716	Monitor external data sources (e.g., computer network defense [CND] vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the enterprise
738	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
741	Perform command and control functions in response to incidents
743	Perform computer network defense (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time computer network defense (CND) incident handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
861	Track and document computer network defense (CND) incidents from initial detection through final resolution
882	Write and publish computer network defense (CND) guidance and reports on incident findings to appropriate constituencies
961	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



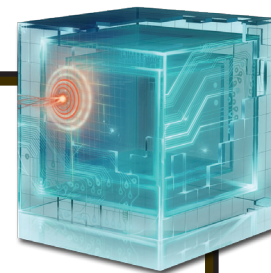
PROTECT AND DEFEND

INCIDENT RESPONSE

Responds to crisis 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.

TASK		KSA
ID	Statement	
1030	Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise	
1031	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required	

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



PROTECT AND DEFEND

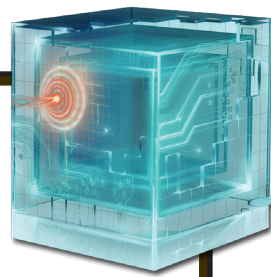
INCIDENT RESPONSE

Responds to crisis 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.

TASK	KSA	
ID	Statement	Competency
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
50	Knowledge of how network services and protocols interact to provide network communications	Infrastructure Design
60	Knowledge of incident categories, incident responses, and timelines for responses	Incident Management
61	Knowledge of incident response and handling methodologies	Incident Management
66	Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies	Computer Network Defense
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
105	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)	Vulnerabilities Assessment
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
153	Skill in handling malware	Computer Network Defense
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



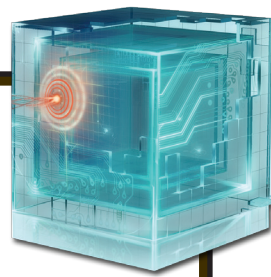
PROTECT AND DEFEND

INCIDENT RESPONSE

Responds to crisis 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.

TASK	KSA	
ID	Statement	Competency
893	Skill in securing network communications	Information Assurance
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense
897	Skill in performing damage assessments	Information Assurance
923	Knowledge of security event correlation tools	Information Systems/Network Security
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1029	Knowledge of malware analysis concepts and methodology	Computer Network Defense
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

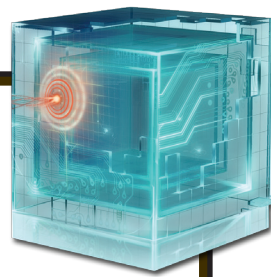


PROTECT AND DEFEND

**COMPUTER NETWORK DEFENSE (CND)
INFRASTRUCTURE SUPPORT**

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

TASK		KSA
ID	Statement	
393	Administer computer network defense (CND) test bed(s), and test and evaluate new CND applications, rules/signatures, access controls, and configurations of CND service provider managed platforms	
471	Coordinate with Computer Network Defense (CND) Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized computer network defense (CND) applications	
481	Create, edit, and manage changes to network access control lists on specialized computer network defense (CND) systems (e.g., firewalls and intrusion prevention systems)	
643	Identify potential conflicts with implementation of any computer network defense (CND) tools within the CND service provider area of responsibility (e.g., tool/signature testing and optimization)	
654	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for specialized computer network defense (CND) systems within the enterprise, and document and maintain records for them	
769	Perform system administration on specialized computer network defense (CND) applications and systems (e.g., anti-virus, audit/remediation) or Virtual Private Network [VPN] devices, to include installation, configuration, maintenance, and backup/restoration	
960	Assist in identifying, prioritizing, and coordinating the protection of critical computer network defense (CND) infrastructure and key resources	



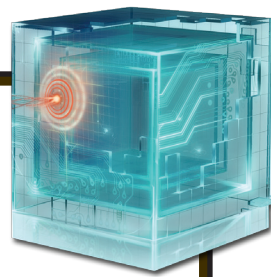
PROTECT AND DEFEND

**COMPUTER NETWORK DEFENSE (CND)
INFRASTRUCTURE SUPPORT**

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

TASK	KSA	
ID	Statement	Competency
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
59	Knowledge of Intrusion Detection System (IDS) tools and applications	Computer Network Defense
61	Knowledge of incident response and handling methodologies	Incident Management
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
105	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)	Vulnerabilities Assessment
146	Knowledge of the types of Intrusion Detection System (IDS) hardware and software	Computer Network Defense
148	Knowledge of Virtual Private Network (VPN) security	Encryption

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



PROTECT AND DEFEND

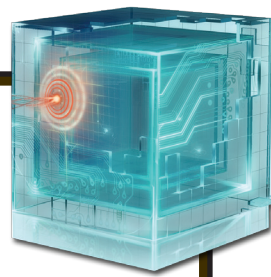
COMPUTER NETWORK DEFENSE (CND)
INFRASTRUCTURE SUPPORT

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

TASK	KSA	
ID	Statement	Competency
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
227	Skill in tuning sensors	Computer Network Defense
229	Skill in using incident handling methodologies	Incident Management
237	Skill in using Virtual Private Network (VPN) devices and encryption	Encryption
893	Skill in securing network communications	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense
900	Knowledge of web filtering technologies	Web Technology
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
989	Knowledge of Voice over Internet Protocol (VoIP)	Telecommunications
1011	Knowledge of processes for reporting network security related incidents	Security
1012	Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels	Internal Controls
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1074	Knowledge of transmission methods (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi], paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

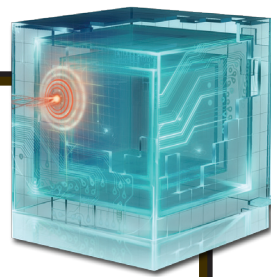
VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

TASK	KSA
ID	Statement
411	Analyze organization's computer network defense (CND) policies and configurations and evaluate compliance with regulations and organizational directives
448	Conduct and/or support authorized penetration testing on enterprise network assets
685	Maintain deployable computer network defense (CND) audit toolkit (e.g., specialized computer network defense [CND] software/hardware) to support computer network defense (CND) audit missions
692	Maintain knowledge of applicable computer network defense (CND) policies, regulations, and compliance documents specifically related to computer network defense (CND) auditing
784	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions
939	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance Countermeasure Reviews [TSCM], TEMPEST ¹ countermeasure reviews)
940	Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure)
941	Assist with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)

¹ TEMPEST is a codename and not an acronym

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

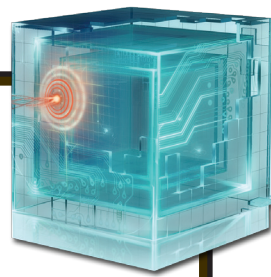
VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

TASK	KSA	
ID	Statement	Competency
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
10	Knowledge of application vulnerabilities	Vulnerabilities Assessment
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
102	Knowledge of programming language structures and logic	Computer Languages
105	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)	Vulnerabilities Assessment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

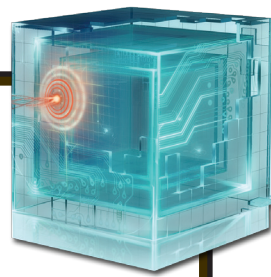
VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

TASK	KSA	
ID	Statement	Competency
115	Knowledge of content development	Computer Network Defense
123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment
181	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
210	Skill in mimicking threat behaviors	Computer Network Defense
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	Vulnerabilities Assessment
225	Skill in the use of penetration testing tools and techniques	Vulnerabilities Assessment
226	Skill in the use of social engineering techniques	Human Factors
897	Skill in performing damage assessments	Information Assurance
904	Knowledge of interpreted and compiled computer languages	Computer Languages
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development



PROTECT AND DEFEND

VULNERABILITY ASSESSMENT AND MANAGEMENT

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

TASK	KSA	
ID	Statement	Competency
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])	Computer Network Defense
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Computer Network Defense (CND) Analysis			Incident Response		Computer Network Defense (CND) Infrastructure Support			Vulnerability Assessment and Management	
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development

INVESTIGATE

Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

Digital Forensics

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Investigation

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

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

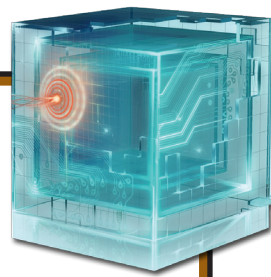
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA
ID	Statement
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise
447	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
463	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis
480	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, compact dis&s (CDs), personal digital assistants (PDAs), mobile phones, global positioning satellite devices (GPSs), and all tape formats
482	Decrypt seized data using technical means
541	Provide technical summary of findings in accordance with established reporting procedures
564	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports)
573	Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence
613	Examine recovered data for information of relevance to the issue at hand
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
743	Perform computer network defense (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation
749	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
752	Perform file signature analysis

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

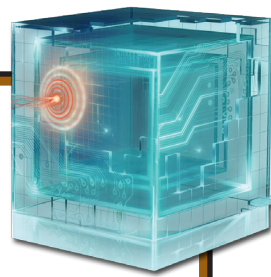
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA
ID	Statement
753	Perform hash comparison against established database
758	Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)
759	Perform timeline analysis
768	Perform static media analysis
771	Perform tier 1, 2, and 3 malware analysis
786	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures)
817	Provide technical assistance on digital evidence matters to appropriate personnel
825	Recognize and accurately report forensic artifacts indicative of a particular operating system
839	Review forensic images and other data sources for recovery of potentially relevant information
868	Use data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost) to extract data for further analysis
870	Use network monitoring tools to capture and analyze network traffic associated with malicious activity
871	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence
882	Write and publish computer network defense (CND) guidance and reports on incident findings to appropriate constituencies
944	Conduct cursory binary analysis
1081	Perform virus scanning on digital media
1082	Perform file system forensic analysis

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

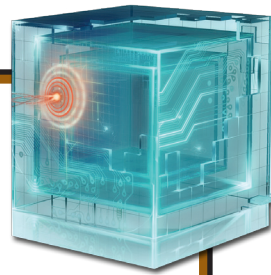
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA
ID	Statement
1083	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive)
1084	Perform static malware analysis
1085	Utilize deployable forensics toolkit to support operations as necessary

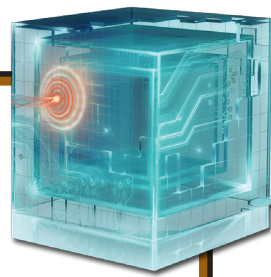
Sub-Specialty Area: Digital Forensics (Law Enforcement/Counterintelligence)

The following tasks, combined with all of the parent tasks/KSAs comprise the entirety of the tasks/KSAs associated with this sub-specialty area.

Digital Forensics (LE/CI) – Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

429	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
620	Employ IT systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
622	Formulate a strategy to ensure chain of custody is maintained in such a way that the evidence is not altered (ex: phones/PDAs need a power source, hard drives need protection from shock and strong magnetic fields)
799	Provide consultation to investigators and prosecuting attorneys regarding the findings of computer examinations
819	Provide testimony related to computer examinations
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
872	Use an array of specialized computer investigative techniques and programs to resolve the investigation

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA	
ID	Statement	Competency
24	Knowledge of basic concepts and practices of processing digital forensic data	Data Management
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
61	Knowledge of incident response and handling methodologies	Incident Management
90	Knowledge of operating systems	Operating Systems
105	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)	Vulnerabilities Assessment
113	Knowledge of server and client operating systems	Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques	Computer Forensics
139	Knowledge of the common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications	Infrastructure Design
193	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans	Information Assurance
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	Vulnerabilities Assessment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

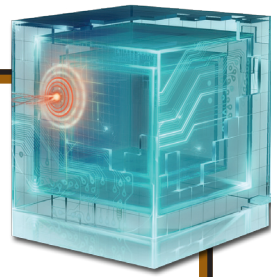
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



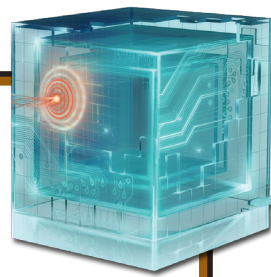
INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA	
ID	Statement	Competency
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics
264	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)	Computers and Electronics
287	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT])	Operating Systems
290	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)	Forensics
294	Knowledge of hacking methodologies in Windows or Unix/Linux environment	Surveillance
302	Knowledge of investigative implications of hardware, operating systems, and network technologies	Computer Forensics
310	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence)	Criminal Law
316	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Criminal Law
340	Knowledge of types and collection of persistent data	Computer Forensics
345	Knowledge of webmail collection, searching/analyzing techniques, tools, and cookies	Web Technology
346	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files	Computer Forensics
350	Skill in analyzing memory dumps to extract information	Reasoning

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA	
ID	Statement	Competency
360	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics)	Computer Forensics
364	Skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files)	Operating Systems
369	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Forensics
374	Skill in setting up a forensic workstation	Forensics
381	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, Forensic Tool Kit [FTK])	Computer Forensics
386	Skill in using virtual machines	Operating Systems
389	Skill in physically disassembling personal computers (PCs)	Computers and Electronics
888	Knowledge of types of digital forensics data and how to recognize them	Computer Forensics
889	Knowledge of deployable forensics	Computer Forensics
890	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems)	Computer Forensics
908	Ability to decrypt digital data collections	Computer Forensics
923	Knowledge of security event correlation tools	Information Systems/Network Security
982	Knowledge of electronic evidence law	Criminal Law
983	Knowledge of legal rules of evidence and court procedure	Criminal Law

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

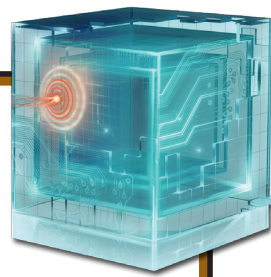
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK	KSA	
ID	Statement	Competency
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1086	Knowledge of data carving tools and techniques (e.g., Foremost)	Computer Forensics
1087	Skill in deep analysis of captured malicious code (e.g., malware forensics)	Computer Network Defense
1088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump)	Computer Languages
1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment
1091	Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5])	Data Management
1092	Knowledge of anti-forensics tactics, techniques, and procedures (TTPS)	Computer Forensics
1093	Knowledge of common forensic tool configuration and support applications (e.g., VMWare, Wireshark)	Computer Forensics
1094	Knowledge of debugging procedures and tools	Software Development
1095	Knowledge of how different file types can be used for anomalous behavior	Vulnerabilities Assessment

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

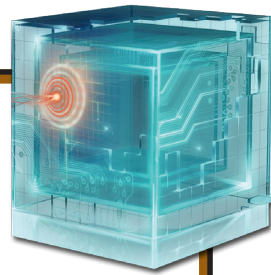
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



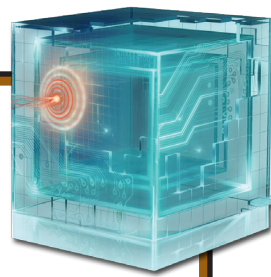
INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK		KSA
ID	Statement	Competency
1096	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro)	Computer Network Defense
1097	Knowledge of virtual machine aware malware, debugger aware malware, and packing	Computer Network Defense
1098	Skill in analyzing anomalous code as malicious or benign	Computer Network Defense
1099	Skill in analyzing volatile data	Computer Forensics
1100	Skill in identifying obfuscation techniques	Computer Network Defense
1101	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures	Computer Network Defense

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



INVESTIGATE

INVESTIGATION

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.

TASK	KSA
ID	Statement
402	Analyze computer-generated threats
429	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
447	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
454	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects
507	Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion
512	Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet
564	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports)
597	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
613	Examine recovered data for information of relevance to the issue at hand
620	Employ information technology (IT) systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
623	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations
633	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action
635	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations
636	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

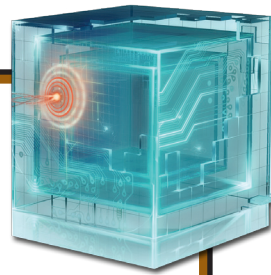
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



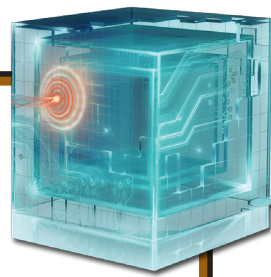
INVESTIGATE

INVESTIGATION

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.

TASK	KSA
ID	Statement
637	Identify elements of proof of the crime
642	Identify outside attackers accessing the system from the Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges
649	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations
663	Conduct large-scale investigations of criminal activities involving complicated computer programs and networks
788	Prepare reports to document analysis
792	Process crime scenes
843	Secure the electronic device or information source
871	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



INVESTIGATE

INVESTIGATION

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.

TASK	KSA	
ID	Statement	Competency
105	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)	Vulnerabilities Assessment
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics
281	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])	Hardware
290	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)	Forensics
310	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence)	Criminal Law
316	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Criminal Law
340	Knowledge of types and collection of persistent data	Computer Forensics
369	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data	Forensics
383	Skill in using scientific rules and methods to solve problems	Reasoning
917	Knowledge of social dynamics of computer attackers in a global context	External Awareness

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

Digital
Forensics

Investigation

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

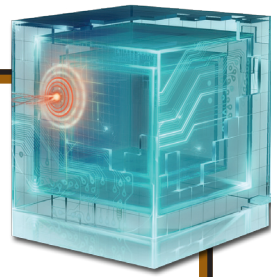
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development



INVESTIGATE

INVESTIGATION

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.

TASK	KSA	
ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

COLLECT AND OPERATE

Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Collection Operations

Executes collection using appropriate strategies and within the priorities established through the collection management process.

Cyber Operations

Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Cyber Operations Planning

Performs in-depth joint targeting and cyber 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.

Due to the unique and highly specialized nature of this work, task and KSA-level content is not provided in this document for the 3 specialty areas in this category.

ANALYZE

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Threat Analysis

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

All Source Intelligence

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.

Exploitation Analysis

Analyzes collected information to identify vulnerabilities and potential for exploitation.

Targets

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Due to the unique and highly specialized nature of this work, task and KSA-level content is not provided in this document for the four specialty areas in this category.

OVERSIGHT AND DEVELOPMENT

Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Legal Advice and Advocacy

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.

Strategic Planning and Policy Development

Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

Education and Training

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

Information Systems Security Operations (Information Systems Security Officer [ISSO])

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

Security Program Management (Chief Information Security Officer [CISO])

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

Legal Advice
and Advocacy

Strategic Planning and
Policy Development

Education
and Training

Information Systems Security Operations
(Information Systems Security Officer [ISSO])

Security Program Management
(Chief Information Security Officer [CISO])

Home

Using This
Document

Sample
Job Titles

Securely
Provision

Operate and
Maintain

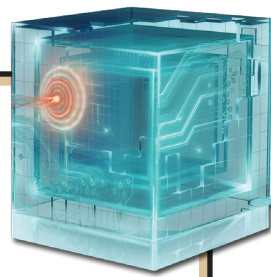
Protect and
Defend

Investigate

Collect and
Operate

Analyze

Oversight and
Development

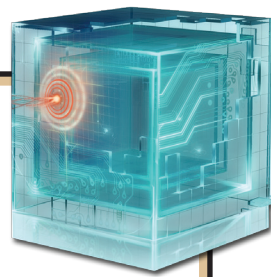


OVERSIGHT AND DEVELOPMENT

LEGAL ADVICE AND ADVOCACY

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.

TASK	KSA
ID	Statement
390	Acquire and maintain a working knowledge of relevant laws, regulations, policies, standards, or procedures
398	Advocate organization's official position in legal and legislative proceedings
451	Conduct framing of allegations to determine proper identification of law, regulatory, or policy/guidance of violation
539	Develop policy, programs, and guidelines for implementation
574	Evaluate, monitor, and ensure compliance with information communication technology (ICT) security policies and relevant legal and regulatory requirements
599	Evaluate contracts to ensure compliance with funding, legal, and program requirements
607	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures
612	Evaluate the impact (e.g., costs or benefits) of changes to laws, regulations, policies, standards, or procedures
618	Explain or provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients
655	Implement new or revised laws, regulations, executive orders, policies, standards, or procedures
675	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues
787	Prepare legal documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery)
834	Resolve conflicts in laws, regulations, policies, standards, or procedures



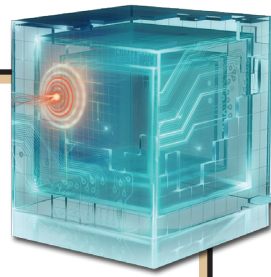
OVERSIGHT AND DEVELOPMENT

LEGAL ADVICE AND ADVOCACY

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.

TASK	KSA	
ID	Statement	Competency
27	Knowledge of cryptology	Cryptography
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
105	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)	Vulnerabilities Assessment
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
300	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (e.g., requirements and priorities), dissemination practices, and legal authorities and restrictions	Organizational Awareness
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
339	Knowledge of the structure and intent of military operation plans, concept operation plans, orders, and standing rules of engagement	Organizational Awareness
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence
954	Knowledge of Export Control regulations and responsible agencies for the purposes of reducing supply chain risk	Contracting/Procurement
981	Knowledge of International Traffic in Arms Regulations (ITARs) and relevance to cybersecurity	Criminal Law

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



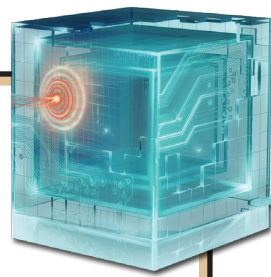
OVERSIGHT AND DEVELOPMENT

LEGAL ADVICE AND ADVOCACY

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.

TASK		KSA
ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1070	Ability to determine impact of technology trend data on laws, regulations, and/or policies	Legal, Government and Jurisprudence

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



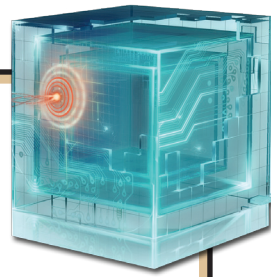
OVERSIGHT AND DEVELOPMENT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

TASK ID	KSA	Statement
410		Analyze organizational information security policy
424		Assess policy needs and collaborate with stakeholders to develop policies to govern information technology (IT) activities
485		Define current and future business environments
492		Design a cybersecurity strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan
524		Develop and maintain strategic plans
539		Develop policy, programs, and guidelines for implementation
565		Draft and publish security policy
594		Establish and maintain communication channels with stakeholders
629		Identify and address information technology (IT) workforce planning and management issues, such as recruitment, retention, and training
641		Identify organizational policy stakeholders
720		Monitor the rigorous application of information security/information assurance (IA) policies, principles, and practices in the delivery of planning and management services
724		Obtain consensus on proposed policy change from stakeholders
812		Provide policy guidance to information technology (IT) management, staff, and users
838		Review existing and proposed policies with stakeholders
840		Review or conduct audits of information technology (IT) programs and projects

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



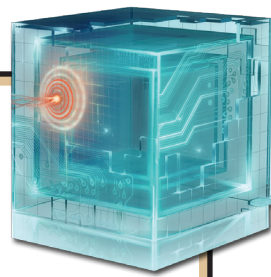
OVERSIGHT AND DEVELOPMENT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

TASK	KSA
ID	Statement
847	Serve on agency and interagency policy boards
854	Support the Chief Information Officer (CIO) in the formulation of information technology (IT)-related policies
884	Write information assurance (IA) policy and instructions
919	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals
946	Ensure established cybersecurity strategy is intrinsically linked to organizational mission objectives
955	Draft and publish a supply chain security/risk management policy
1023	Identify and track the status of protected information assets
1024	Apply assessment data of identified threats in decision-making
1025	Triage protected assets
1026	Oversee development and implementation of high-level control architectures
1027	Translate applicable laws, statutes, and regulatory documents and integrate into policy
1041	Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



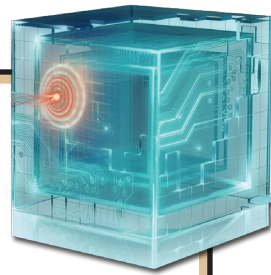
OVERSIGHT AND DEVELOPMENT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

TASK	KSA	
ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
105	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)	Vulnerabilities Assessment
244	Ability to determine the validity of technology trend data	Technology Awareness
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
320	Knowledge of external organizations and academic institutions dealing with cybersecurity issues	External Awareness
336	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII])	Telecommunications
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
954	Knowledge of Export Control regulations and responsible agencies for the purposes of reducing supply chain risk	Contracting/Procurement

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



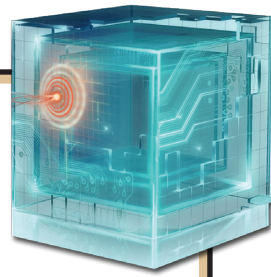
OVERSIGHT AND DEVELOPMENT

STRATEGIC PLANNING AND POLICY DEVELOPMENT

Applies knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

TASK	KSA	
ID	Statement	Competency
1021	Knowledge of risk threat assessment	Risk Management
1022	Knowledge of the nature and function of the relevant information structure	Enterprise Architecture
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



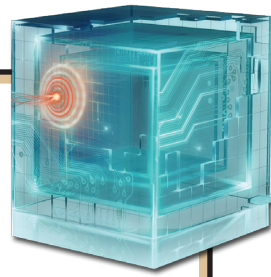
OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

TASK ID	KSA	Statement
453		Conduct interactive training exercises to create an effective learning environment
479		Correlate mission requirements to training
490		Deliver training courses tailored to the audience and physical environment
491		Demonstrate concepts, procedures, software, equipment, and technology applications to coworkers, subordinates, or others
504		Design training curriculum and course content
510		Determine training requirements (e.g., subject matter, format, location)
538		Develop new or identify existing awareness and training materials that are appropriate for intended audiences
551		Develop the goals and objectives for cybersecurity training, education, or awareness
567		Educate customers in established procedures and processes to ensure professional media standards are met
606		Evaluate the effectiveness and comprehensiveness of existing training programs
624		Guide employees through relevant development and training choices
778		Plan classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment
779		Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
841		Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions)
842		Revise curriculum end course content based on feedback from previous training sessions

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



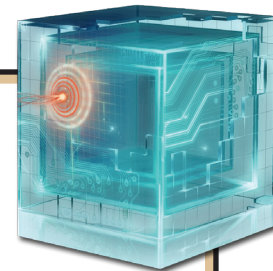
OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

TASK	KSA
ID	Statement
845	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media, cartography)
855	Support the design and execution of exercise scenarios
885	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce
953	Coordinate with human resources to ensure job announcements are written to reflect required training, education, and/or experience

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



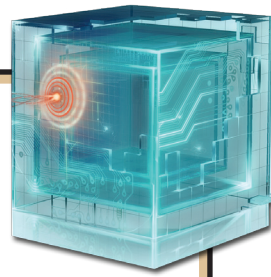
OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

TASK	KSA	
ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
90	Knowledge of operating systems	Operating Systems
246	Knowledge and experience in the Instructional System Design (ISD) methodology	Multimedia Technologies
252	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools, and laws/regulations	Computer Network Defense
264	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)	Computers and Electronics
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
314	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others
332	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience	Teaching Others
344	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



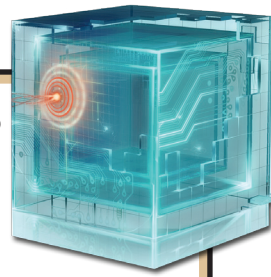
OVERSIGHT AND DEVELOPMENT

EDUCATION AND TRAINING

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

TASK		KSA
ID	Statement	Competency
359	Skill in developing and executing technical training programs and curricula	Computer Forensics
363	Skill in identifying gaps in technical capabilities	Teaching Others
376	Skill in talking to others to convey information effectively	Oral Communication
918	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	Teaching Others
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
952	Knowledge of emerging security issues, risks, and vulnerabilities	Technology Awareness
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



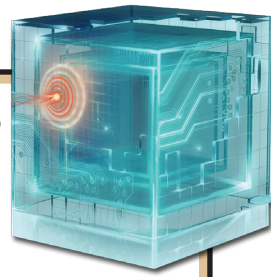
OVERSIGHT AND DEVELOPMENT

**INFORMATION SYSTEMS SECURITY OPERATIONS
(INFORMATION SYSTEMS SECURITY OFFICER [ISSO])**

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

TASK ID	KSA	Statement
397		Advise appropriate senior leadership or authorizing official of changes affecting the organization's information assurance (IA) posture
440		Collect and maintain data needed to meet system information assurance (IA) reporting
584		Ensure that information assurance (IA) inspections, tests, and reviews are coordinated for the network environment
585		Ensure that information assurance (IA) requirements are integrated into the continuity planning for that system and/or organization(s)
590		Ensure that protection and detection capabilities are acquired or developed using the information system security engineering approach and are consistent with organization-level information assurance (IA) architecture
598		Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed
600		Evaluate cost-benefit, economic, and risk analysis in decision-making process
731		Participate in information security risk assessments during the Security Assessment and Authorization (SA&A) process
733		Participate in the development or modification of the computer environment information assurance (IA) security program plans and requirements
790		Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations
816		Provide system related input on information assurance (IA) security requirements to be included in statements of work and other appropriate procurement documents
824		Recognize a possible security violation and take appropriate action to report the incident, as required
828		Recommend resource allocations required to securely operate and maintain an organization's information assurance (IA) requirements
852		Supervise or manage protective or corrective measures when an information assurance (IA) incident or vulnerability is discovered

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



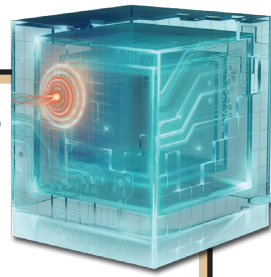
OVERSIGHT AND DEVELOPMENT

**INFORMATION SYSTEMS SECURITY OPERATIONS
(INFORMATION SYSTEMS SECURITY OFFICER [ISSO])**

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

TASK ID	KSA	Statement
869		Use federal and organization-specific published documents to manage operations of their computing environment system(s)
962		Identify security requirements specific to an information technology (IT) system in all phases of the system lifecycle
963		Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
964		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
1016		Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs)
1017		Participate in the acquisition process as necessary, following appropriate supply chain risk management practices
1041		Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



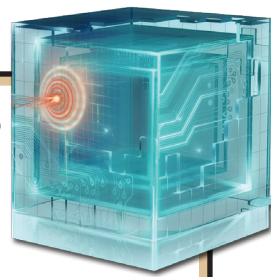
OVERSIGHT AND DEVELOPMENT

**INFORMATION SYSTEMS SECURITY OPERATIONS
(INFORMATION SYSTEMS SECURITY OFFICER [ISSO])**

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

TASK	KSA	
ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
37	Knowledge of disaster recovery and continuity of operations plans	Incident Management
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
77	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	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



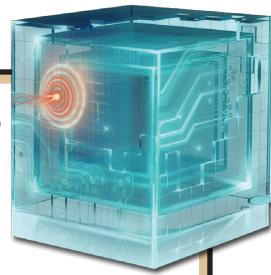
OVERSIGHT AND DEVELOPMENT

**INFORMATION SYSTEMS SECURITY OPERATIONS
(INFORMATION SYSTEMS SECURITY OFFICER [ISSO])**

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

TASK	KSA	
ID	Statement	Competency
121	Knowledge of structured analysis principles and methods	Logical Systems Design
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
143	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
173	Skill in creating policies that reflect system security objectives	Information Systems Security Certification
183	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	Information Assurance
325	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management)	Contracting/Procurement
965	Knowledge of organization's risk tolerance and/or risk management approach	Risk Management
966	Knowledge of enterprise incident response program, roles, and responsibilities	Incident Management
967	Knowledge of current and emerging threats/threat vectors	Information Systems/Network Security
1004	Knowledge of critical information technology (IT) procurement requirements	Contracting/Procurement
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



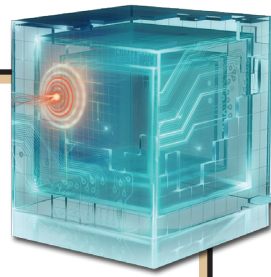
OVERSIGHT AND DEVELOPMENT

**INFORMATION SYSTEMS SECURITY OPERATIONS
(INFORMATION SYSTEMS SECURITY OFFICER [ISSO])**

Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

TASK	KSA	
ID	Statement	Competency
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



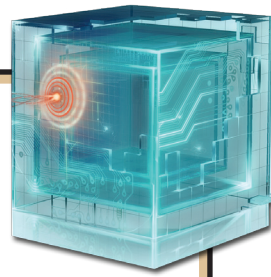
OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK ID	KSA	Statement
391		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
392		Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program
395		Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture
396		Advise senior management (e.g., Chief Information Officer [CIO]) on cost-benefit analysis of information security programs, policies, processes, systems, and elements
445		Communicate the value of information technology (IT) security throughout all levels of the organization's stakeholders
473		Collaborate with organizational managers to support organizational objectives
475		Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance
578		Ensure security improvement actions are evaluated, validated, and implemented as required
596		Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy
600		Evaluate cost-benefit, economic, and risk analysis in decision-making process
628		Identify alternative information security strategies to address organizational security objective
640		Identify information technology (IT) security program implications of new technologies or technology upgrades
674		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 (CND) information
676		Interpret and/or approve security requirements relative to the capabilities of new information technologies

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



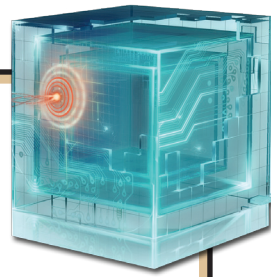
OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK	KSA
ID	Statement
677	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's information assurance (IA) program
679	Lead and align information technology (IT) security priorities with the security strategy
680	Lead and oversee information security budget, staffing, and contracting
705	Manage the monitoring of information security data sources to maintain organizational situational awareness
706	Manage the publishing of computer network defense (CND) guidance (e.g., Time Compliance Network Orders [TCNOs], concept of operations, net analyst reports) for the organization
707	Manage threat or target analysis of computer network defense (CND) information and production of threat information within the enterprise
711	Monitor and evaluate the effectiveness of the enterprise's information assurance (IA) security safeguards to ensure they provide the intended level of protection
730	Oversee the information security training and awareness program
801	Provide enterprise information assurance (IA) and supply chain risk guidance for development of the disaster recovery and continuity of operations plans
810	Provide leadership and direction to information technology (IT) personnel by ensuring that information assurance (IA) security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities
818	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters
848	Recommend policy and coordinate review and approval

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



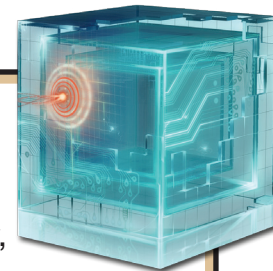
OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK	KSA
ID	Statement
862	Track audit findings and recommendations to ensure appropriate mitigation actions are taken
919	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals
947	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies
948	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk
949	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements
1018	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals
1032	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance
1035	Forecast ongoing service demands and ensure security assumptions are reviewed as necessary
1041	Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



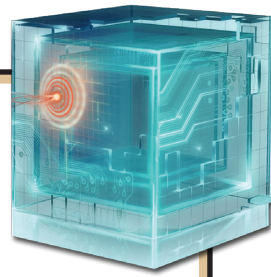
OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK	KSA	
ID	Statement	Competency
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Cryptography
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics
37	Knowledge of disaster recovery and continuity of operations plans	Incident Management
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
61	Knowledge of incident response and handling methodologies	Incident Management
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
66	Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies	Computer Network Defense
81	Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])	Infrastructure Design
87	Knowledge of network traffic analysis methods	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



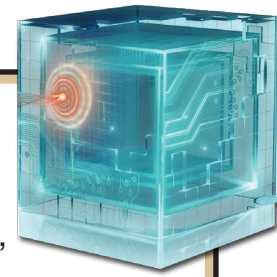
OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK	KSA	
ID	Statement	Competency
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
105	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)	Vulnerabilities Assessment
107	Knowledge of resource management principles and techniques	Project Management
110	Knowledge of security management	Information Assurance
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems
126	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
129	Knowledge of system lifecycle management principles, including software security and usability	Systems Life Cycle
132	Knowledge of technology integration processes	Systems Integration
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security

[NEXT PAGE](#) | [PREVIOUS PAGE](#)



OVERSIGHT AND DEVELOPMENT

**SECURITY PROGRAM MANAGEMENT
(CHIEF INFORMATION SECURITY OFFICER [CISO])**

Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

TASK	KSA	
ID	Statement	Competency
299	Knowledge of information security program management and project management principles and techniques	Project Management
916	Skill in deconflicting cyber operations and activities	Political Savvy
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement
1040	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure	Criminal Law
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management

[NEXT PAGE](#) | [PREVIOUS PAGE](#)

THE NATIONAL CYBERSECURITY
WORKFORCE
FRAMEWORK



NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)
<http://csrc.nist.gov/nice>



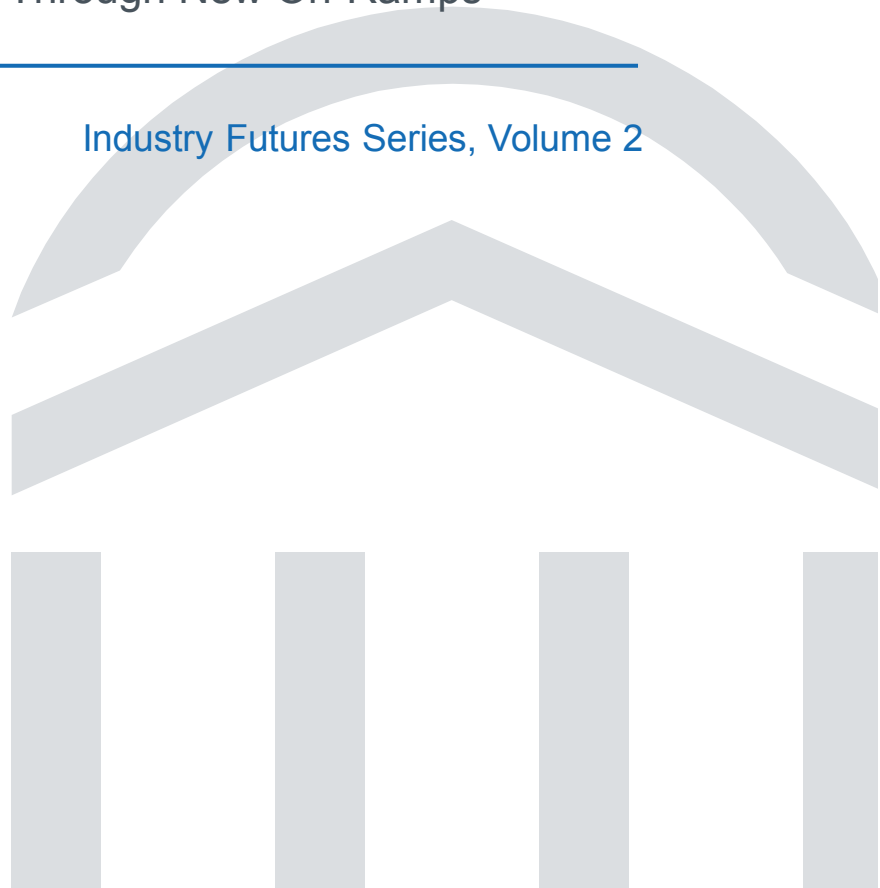
Education
Advisory
Board

Community College Executive Forum

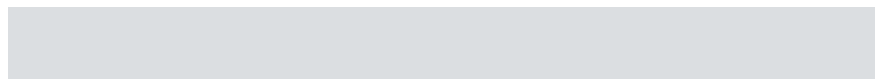
Cybersecurity

Expanding Enrollments Through New On-Ramps

Industry Futures Series, Volume 2



eab.com



Community College Executive Forum

Project Directors

Lisa Geraci

Lisa Qing

Contributing Consultant

Jess Jong

Design Consultant

Nini Jin

Practice Manager

Sarah Zauner

Executive Director

Chris Miller

LEGAL CAVEAT

The Advisory Board Company has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and The Advisory Board Company cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, The Advisory Board Company is not in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. Neither The Advisory Board Company nor its officers, directors, trustees, employees and agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by The Advisory Board Company or any of its employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by The Advisory Board Company, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

The Advisory Board is a registered trademark of The Advisory Board Company in the United States and other countries. Members are not permitted to use this trademark, or any other Advisory Board trademark, product name, service name, trade name, and logo, without the prior written consent of The Advisory Board Company. All other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names and logos or images of the same does not necessarily constitute (a) an endorsement by such company of The Advisory Board Company and its products and services, or (b) an endorsement of the company or its products or services by The Advisory Board Company. The Advisory Board Company is not affiliated with any such company.

IMPORTANT: Please read the following.

The Advisory Board Company has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to The Advisory Board Company. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

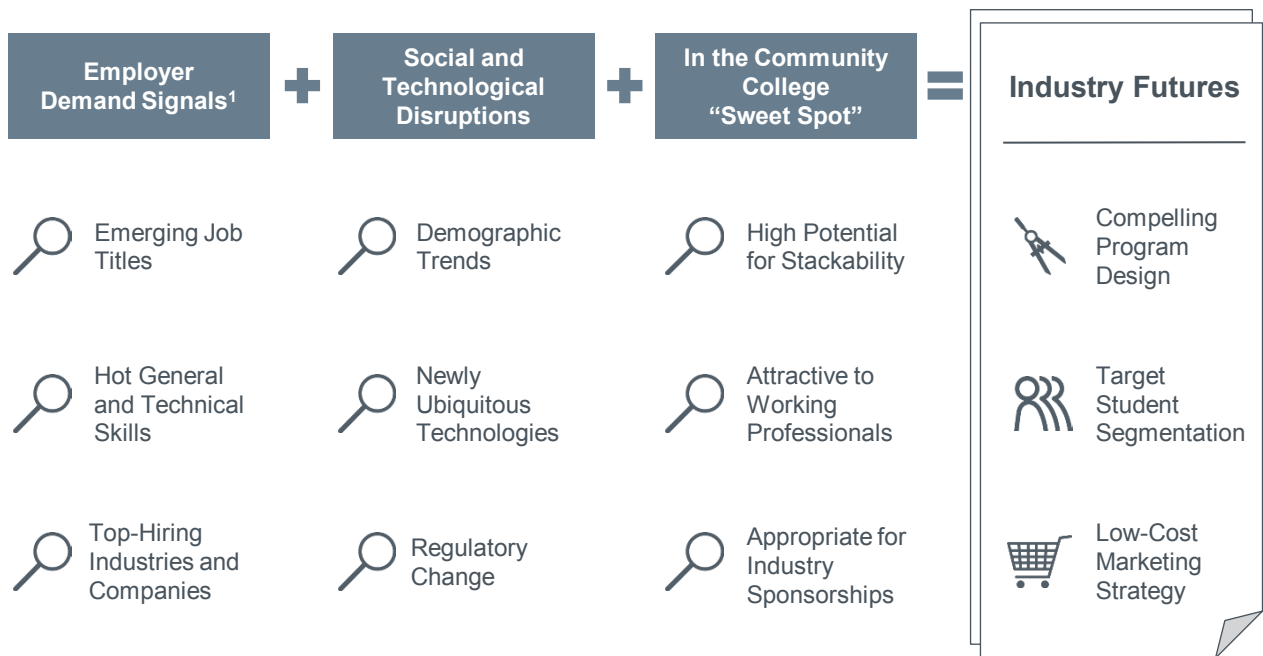
1. The Advisory Board Company owns all right, title and interest in and to this Report. Except as stated herein, no right, license, permission or interest of any kind in this Report is intended to be given, transferred to or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.
2. Each member shall not sell, license, or republish this Report. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.
3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.
4. Each member shall not remove from this Report any confidential markings, copyright notices, and other similar indicia herein.
5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.
6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to The Advisory Board Company.

Anticipating the Workforce Needs of the Next Decade

Volume Two in a Four-Part Series

As technology reshapes industries and the workforce prepares for a mass retirement of Baby Boomers, higher education must anticipate the training deficits of the future while continuing to respond to current employer needs. The Industry Futures Series combines an analysis of employer demand signals (available through a partnership with the labor market analytics firm Burning Glass) with an examination of the social and technological disruptions shaping the next decade's workforce. The methodology outlined below aims to identify opportunities for community colleges to launch or redesign programs that align with emerging student and employer demand.

Our Methodology for Identifying High-Demand Program Opportunities



The Industry Futures Series examines four opportunities for colleges to attract new students while addressing the needs of the local workforce. This second volume explores how to design cybersecurity programs to attract a diverse enrollment pipeline, from K-12 students to career changers from non-technical fields.

Four Opportunities for Community Colleges to Do Well and Good



1) The real-time labor market data in this report comes from the Education Advisory Board's partnership with Burning Glass for use of Burning Glass's proprietary Labor/Insight™ tool.

Study Road Map

1 | Understanding Cybersecurity Demand

2 | New Directions in Cybersecurity Education

3 | Appendix: Assessing the Opportunity

A White Hot Specialty in a Red Hot Field

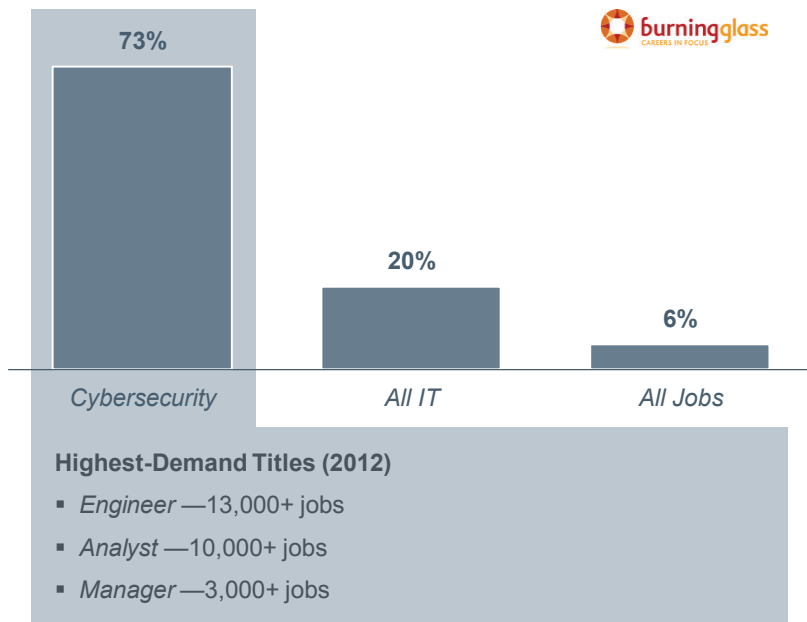
As organizations adopt new technologies, they rapidly develop new security needs. Over the last five years, employer demand for cybersecurity specialists has exploded, outpacing demand for information technology (IT) workers more broadly. According to a study from the labor market analytics firm Burning Glass, the number of cybersecurity job postings grew by 73% from 2007 to 2012, compared to just 20% across all IT roles.

As a reflection of heightened demand, cybersecurity specialists earn more than the average IT worker. In a sample of online job postings from 2012, the average listed salary for cybersecurity positions exceeded that of all IT positions by \$12,000. Despite this salary premium, however, employers still struggle to recruit cybersecurity specialists, and they must frequently repost open cybersecurity positions in search of qualified candidates.

Cybersecurity Growing Faster Than IT Sector Overall

Exploding Employer Demand

Increase in Online Job Postings, 2007-2012



A Growing Wage Premium

\$101K

Average listed salary for cybersecurity professionals

\$89K

Average listed salary across all IT jobs



Hard to Fill Despite High Pay

35%

Rate at which employers are more likely to repost a cybersecurity job, versus another IT job, due to a lack of qualified candidates

Source: "Initial Findings on Cyber Security Jobs," Burning Glass Technologies, February 2013; Burning Glass Labor/Insight; EAB interviews and analysis.

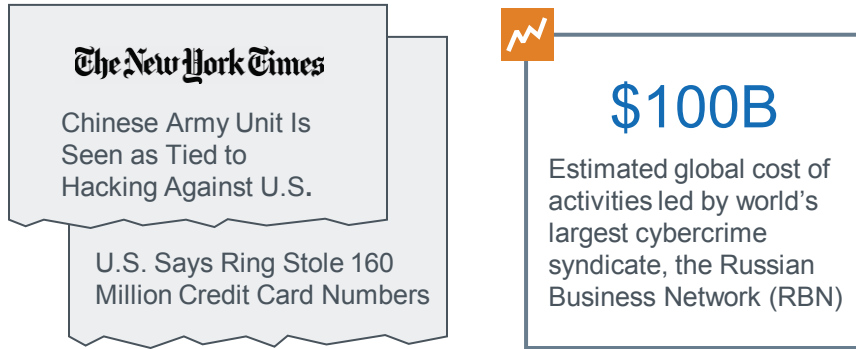
From National Security to Private Sector

The rapid growth in demand for cybersecurity specialists reflects the growing sophistication of cybercrime. Today, the most threatening cyber attacks are rarely the work of individual hackers. Instead, they originate within organized military units and crime syndicates. The largest of these syndicates, the Russian Business Network, causes an estimated \$100 billion in damages each year. Today, analysts estimate that the economic impact of cybercrime exceeds that of the global drug trade.

Although the public sector continues to defend against cybercrime, cybersecurity hiring is shifting toward the private sector. In 2013, the majority of online job postings for cybersecurity roles came from nongovernment employers, who collectively demonstrated 33% more demand for these positions than they had three years earlier.

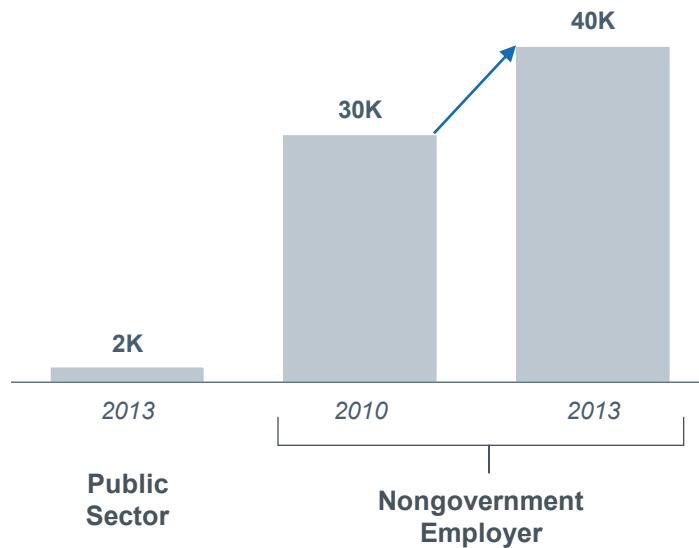
Corporations Hiring to Protect Privacy of Customer Data

From Lone Hackers to Syndicates



Private Sector Staffing Up In Response

U.S. Job Postings in Cybersecurity



Source: Sanger D, et al., "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, Feb. 2013; Popper N and Sengupta S, "U.S. Says Ring Stole 160 Million Credit Card numbers," *New York Times*, July 2013; Umbach F, "Cyber Threats Are Growing in Size, Volume, and Sophistication," *WorldReview*, May 2013; Burning Glass Labor/Insight; EAB interviews and analysis.

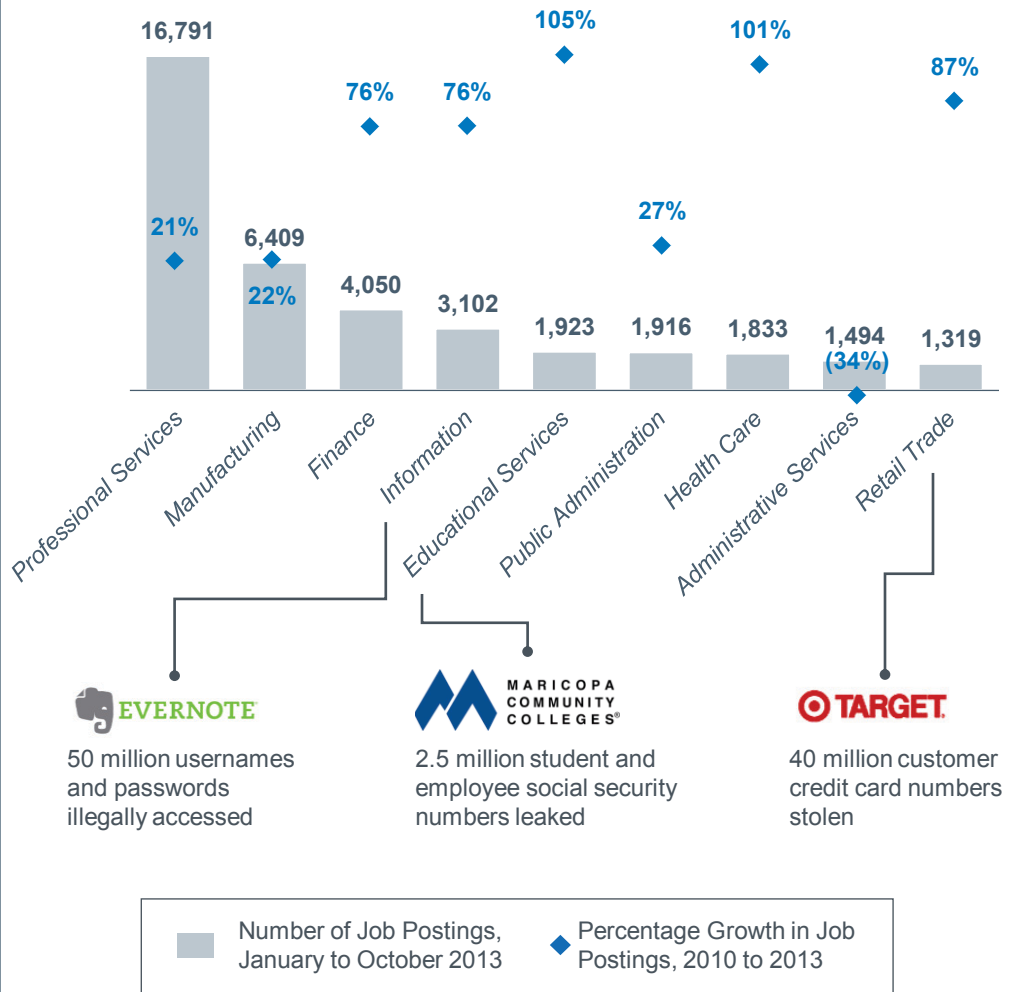
Every Industry Taking Note

Since 2010, demand for cybersecurity professionals has grown across nearly every industry. Manufacturing and finance continue to demonstrate particularly high need, while educational services and health care are experiencing rapid growth in demand as they increasingly rely on technology. In health care, for example, the shift toward electronic medical records has left hospitals much more vulnerable to data breaches.

High-profile incidents have underlined the importance of cybersecurity to business strategy. After hackers captured 40 million credit card numbers from Target shoppers in early December 2013, the company spent \$61 million setting up a customer response operation and faced over 90 lawsuits. The loss of shoppers' trust had an even greater impact, driving the company's holiday season profits down 46% from the year before.

Demand for Cybersecurity Workers Growing Across the Board

Cybersecurity Job Postings by Industry Sector



Source: Burning Glass Labor/Insight; "Evernote Discloses Security Breach" *Wall Street Journal*, Mar. 2013; Dunning M, "Arizona Community College Faces Class Action Suit Over Data Breach," *Business Insurance*, Apr. 2014; Yadron D and Ziobro P, "Target's Cyber Security Staff Raised Concerns in Month Before Breach," *Wall Street Journal Law Blog*, Feb. 2014; EAB interviews and analysis.

But Cybersecurity Supply Still Lags Demand

Despite growing public awareness of the cybersecurity profession and elevated salaries in the field, employers continue to report a pervasive skills gap. Our analysis identified two root causes behind this workforce shortage.

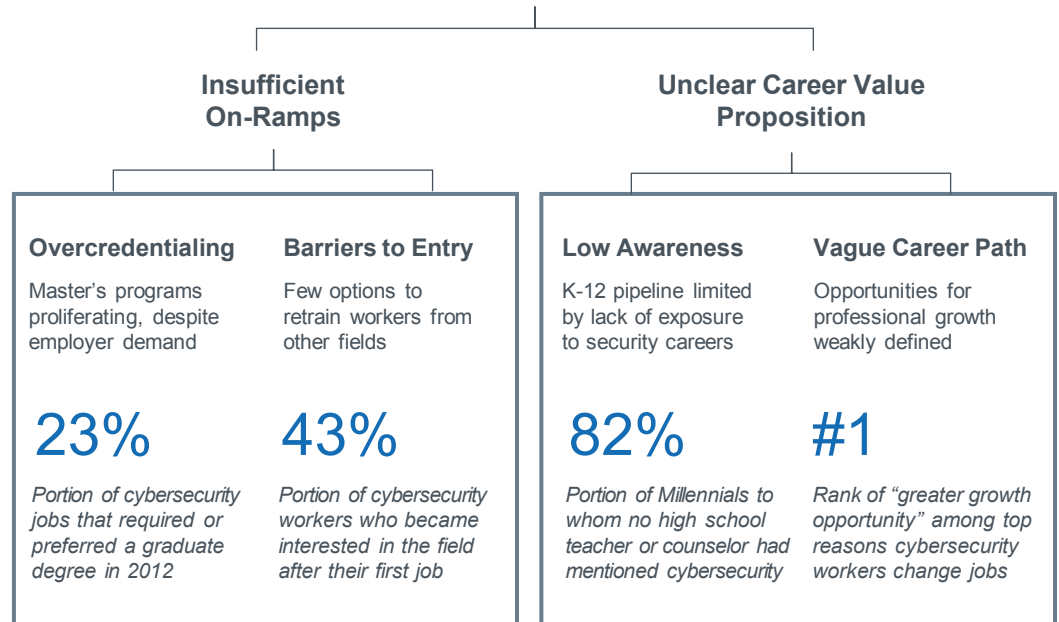
First, existing cybersecurity programs need more on-ramps to accommodate students at various career stages. Though employers typically require undergraduate degrees for cybersecurity roles, many programs prepare students at the graduate level. Because graduate programs often call for prior IT training, they rarely accommodate career changers from non-technical fields.

Second, the robust career value proposition of cybersecurity programs remains unclear to many prospective students. Few middle and high school students learn about the field early enough to select it as a first-choice career. Additionally, because career advancement opportunities remain weakly defined in this emerging field, mid-career professionals may leave it in search of senior positions elsewhere.

Community colleges, with their expertise in designing programs that accommodate students of diverse career stages and academic backgrounds, are especially well positioned to address these challenges facing the cybersecurity workforce.

A Root Cause Analysis of the Workforce Shortage

Why Aren't We Producing Enough Cybersecurity Professionals?



Community Colleges Well Positioned to Address Shortage

Workforce Challenge

- Overcredentialing
- Barriers to Entry
- Low Awareness
- Vague Career Path

Community College Advantage

- Associate degrees and 2+2 programs align with entry-level cybersecurity qualifications
- Open access programs accommodate students without formal technical training
- Extensive high school partnerships provide opportunities for K-12 outreach
- Emphasis on stackability ties additional credentials to career advancement

Source: "Preparing Millennials to Lead in Cyberspace," Raytheon, October 2013; "Cyber Security Census," Semper Secure, August 2013; Burning Glass Labor/Insight; EAB interviews and analysis.

Study Road Map

1 | Understanding Cybersecurity Demand

2 | New Directions in Cybersecurity Education

3 | Appendix: Assessing the Opportunity

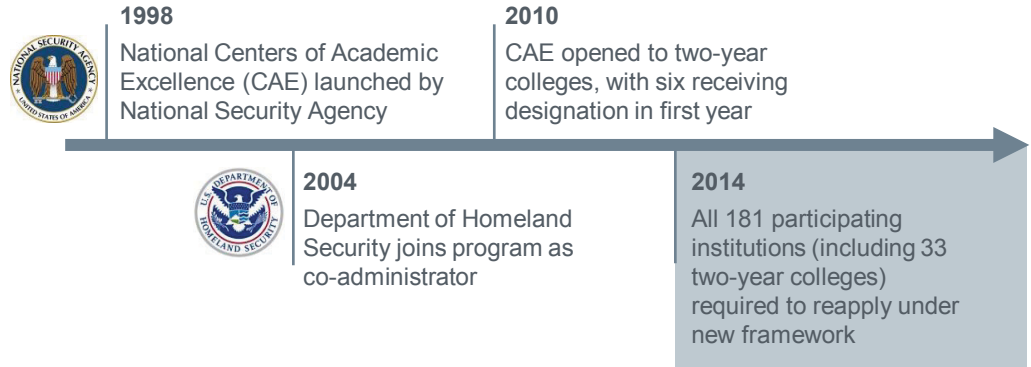
Clarifying Competencies

In response to evolving cybersecurity needs, the National Security Agency (NSA) and the Department of Homeland Security (DHS) recently revised the standards for the National Centers of Academic Excellence (CAE) in Information Assurance program. Currently, 181 colleges and universities have the CAE designation, which recognizes cybersecurity curricula aligned with federal training standards. Among two-year institutions, the designation differentiates 33 leading colleges. However, the designation is so common among four-year institutions that critics have dubbed it the “Centers of Adequacy” program.

To bolster the program’s rigor and realign it with changing employer needs, the NSA and DHS are requiring all 181 participating institutions to reapply for the CAE designation under new standards by December 2014. These standards define 64 “knowledge units” that map to suggested learning outcomes for cybersecurity programs. Because the framework is more flexible than the previous one, colleges may update their programs as the discipline evolves. Moreover, colleges now have more opportunities to develop specializations within their programs.

Bellwether Federal Employers Define Cybersecurity’s Must-Have Skills

Revisiting the National Centers of Academic Excellence



64
Number of discrete knowledge units mandating learning outcomes

“

A More Adaptable Framework

“The framework of Knowledge Units (KUs) was chosen to make the requirements easier to update in the future and to allow differentiation amongst the schools by recognizing the specific areas in which they focus their research and/or educational offerings.”

CAE Team, 2013

Source: “National Centers of Academic Excellence in Information Assurance/Cyber Defense: New Academic Requirements,” National Security Agency and Department of Homeland Security, June 2013; EAB interviews and analysis.

A Stable Core Curriculum with Mix-and-Match Options

The new CAE framework requires all two-year programs to teach 10 core knowledge units, including networking, system administration, and cryptography. Four-year programs must teach these same 10 units, plus an additional five.

The framework also defines 49 optional knowledge units that programs can mix and match. Upon analysis, we identified numerous ways to bundle together these optional units to form certificates and concentrations within degree programs. For example, a college could develop a digital forensics certificate by combining optional units in network forensics, forensic accounting, and advanced cryptography. This specialized expertise in digital forensics could differentiate the program from those of other colleges, even as the CAE designation grows more common at the two-year level.

Room for Specialization in Newly Defined Knowledge Units

10 Two-Year Core Units

Two-Year Programs

- Data Analysis
- Introductory Programming
- Cyber Defense & Cyber Threats
- Fundamental Security Design
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Ethics, and Compliance
- System Administration

+5 Four-Year Core Units

Four-Year Programs

- Databases
- Network Defense, Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

49 Optional Units¹



1) Partial list of optional units. Full list available at <http://www.cisse.info/pdf/2014/2014%20CAE%20Knowledge%20Units.pdf>

Source: "National Centers of Academic Excellence in Information Assurance/Cyber Defense: New Academic Requirements," National Security Agency and Department of Homeland Security, June 2013; EAB interviews and analysis.

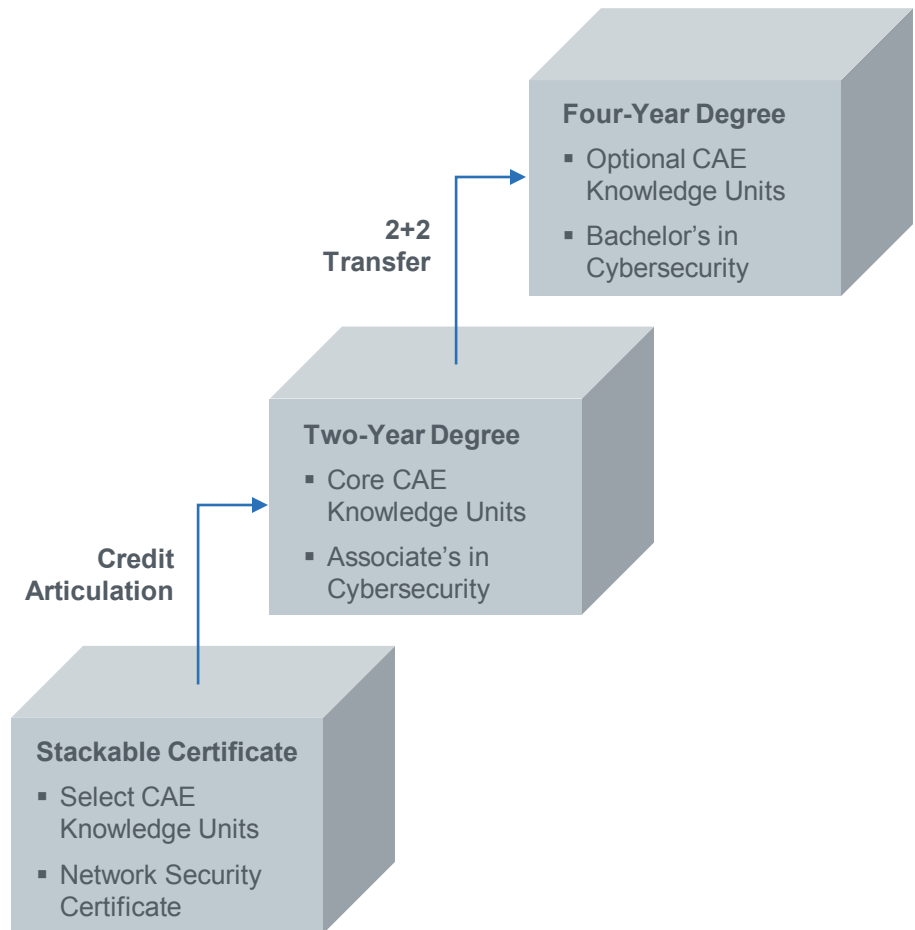
Tremendous Potential for Stackability

By defining learning outcomes at each degree level, the CAE framework facilitates the development of stackable programs built out of a common pool of knowledge units.

Credits from a certificate that teaches a few core knowledge units could articulate into an associate's degree built out of the remaining core units. Through an articulation agreement with a university, that associate's degree could in turn stack into a bachelor's degree containing several optional knowledge units.

In fact, because the CAE framework requires two-year cybersecurity programs to teach two-thirds of the knowledge units required of four-year programs, the curricula of participating community colleges and universities overlap significantly. The 10 shared knowledge units (outlined on page 13) could serve as the basis for future articulation agreements, thus strengthening the value proposition of two-year cybersecurity programs for students who ultimately seek bachelor's degrees.

Shared Knowledge Units Pave Way for Articulation Across Credential Levels



An Option for Every Career Stage

Rose State College's cybersecurity portfolio includes six certificates, an associate's degree, and several four-year articulation agreements. Midcareer cybersecurity professionals may pursue the certificates as stand-alone credentials for advancement, but more often students new to the field complete them on their way to an associate's degree. Over half of associate's degree graduates directly enter bachelor's programs, most commonly at Oklahoma State University Institute of Technology, where all 63 credits from Rose State count toward the Bachelor of Technology degree.

As of 2014, Rose State's cybersecurity program enrolled over 200 declared majors. Although the college is located just one mile from a large air force base, only 20% of its cybersecurity students are military personnel, suggesting the program's appeal to civilians. Many nonmilitary students first learn about the program through K-12 outreach initiatives, which include classroom visits and guidance counselor events at 12 regional high schools.

Diverse Pipeline and Defined Outcomes Sustain Rose State's High Enrollments

A.A.S. in Networking/Cybersecurity

200+ Declared majors in cybersecurity track

Enrollment Pipeline



Building K-12 Awareness

Program director presents during guidance counselor luncheons and STEM classes at 12 regional high schools



Not Only Military

20% of cybersecurity students are employed at air force base near campus, while 80% are civilians



Student Outcomes



Preferred Articulation

Full transfer of A.A.S. credits toward Bachelor of Technology at Oklahoma State University Institute of Technology



Built-in Certificate

Midcareer students may complete advanced courses within degree sequence to earn stand-alone credential

Source: "Networking/Cybersecurity Associate in Applied Science Degree—Cybersecurity Option," Rose State College; "Cyber Security Information Security Certificate Program," Rose State College; EAB interviews and analysis.

Building an Early Enrollment Pipeline

A growing number of colleges are conducting K-12 outreach to address the cybersecurity workforce shortage while expanding their enrollment pipeline. The National CyberWatch Center, an Advanced Technological Education center headquartered at Prince George's Community College, oversees numerous activities that target students and their influencers (parents, teachers, and counselors) from elementary school onward.

As early as fourth grade, students participate in weekly hands-on activity sessions after school. Each session includes materials for students to take home and share with their parents, who may in turn register them for further cybersecurity programs. CyberWatch also hosts career exploration events for high school guidance counselors and STEM coordinators, including an annual workshop that draws up to 100 counselors across Maryland.

Though parent and counselor outreach can influence students to pursue cybersecurity careers, dual credit opportunities provide the most direct pathways into community college programs. CyberWatch, in partnership with the Maryland State Department of Education, has developed coursework that high school students statewide may apply toward associate's degrees in cybersecurity and related fields.

K-12 Outreach Encourages Students to Pursue College Cybersecurity Programs



1



Engaging Youth and Their Parents

After School Programs with Take-Home Activities

- Weekly 90-minute sessions have served over 1,000 elementary and middle school students since 2005
- All sessions include hands-on activities for students and take-home materials to share with parents, ranging from career flyers to small projects (e.g., writing name in binary)
- ✓ Engaged parents encourage students to enroll in further cybersecurity programs and pursue related career paths

2



Educating High School Counselors

Cybersecurity Careers Workshops

- Annual one-day workshop serves up to 100 counselors across Maryland and has been replicated in other states
- Guest speakers discuss cybersecurity roles, career and internship opportunities with local employers, education options, and student experiences
- ✓ Engaged counselors discuss cybersecurity career options with students and parents, and invite college program directors to career fairs

3



Building Accelerated Career Pathways

Dual Credit Cybersecurity Programs

- College-level cybersecurity courses available to high school students throughout Maryland
- Curriculum includes hardware, software, operating systems, networking, and cyber threats
- ✓ Students matriculating to local community college qualify for 6-12 credits toward IT-related associate degree

Source: "Expanding Knowledge in Cyberawareness and Careers in Cybersecurity," National CyberWatch Center; EAB interviews and analysis.

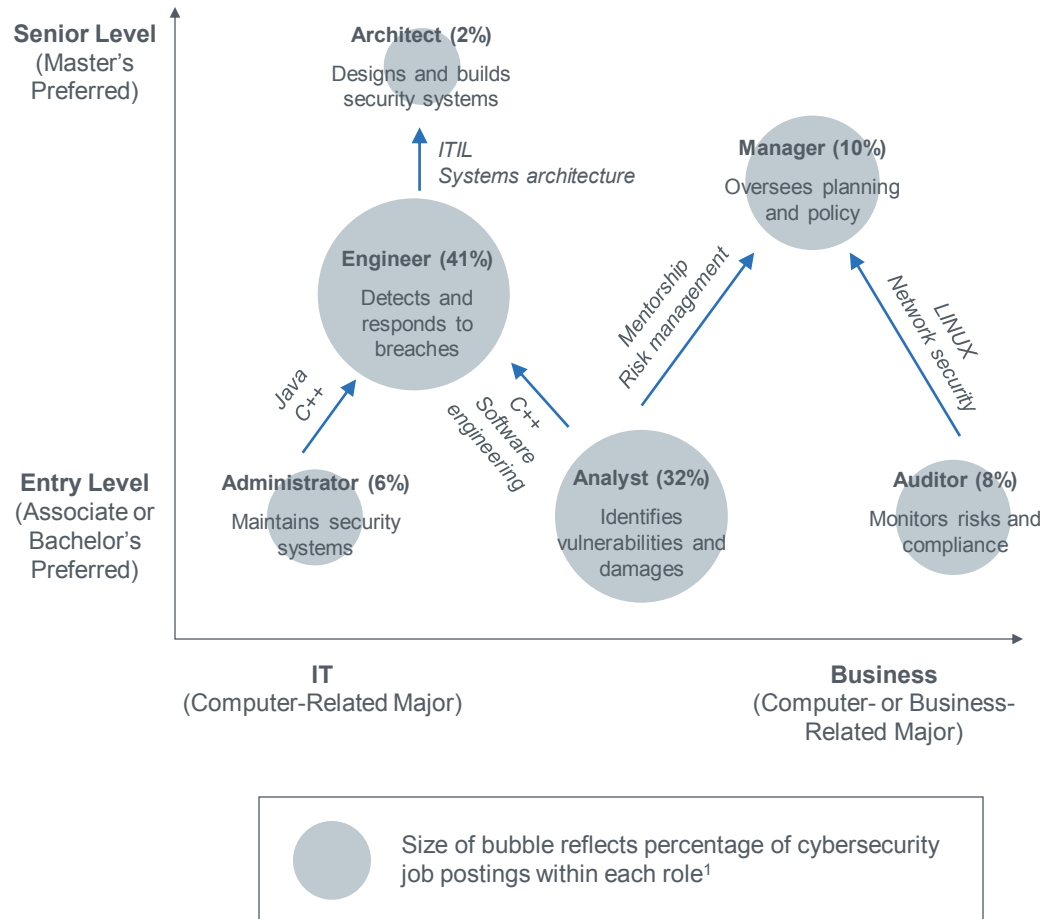
Emerging Career Pathways

Cybersecurity programs must address training needs across diverse career stages to support continued professional growth. To identify the skills most relevant at each stage, we analyzed a sample of 32,000 job postings using the Burning Glass Labor/Insight tool.

This chart presents a simplified taxonomy of cybersecurity roles. The size of each bubble reflects the percentage of cybersecurity job postings within each role. For example, 41% of all identified job postings were for engineers, compared to just 2% for architects. Each bubble's placement on the x-axis reflects the mix of business and technical skills it requires, while its placement on the y-axis reflects the likelihood it requires an advanced degree.

The arrows between bubbles identify select skills that cybersecurity professionals need to move from one role to the next. For example, this chart suggests an opportunity for colleges to train entry-level cybersecurity administrators in programming languages such as Java and C++ to prepare them to advance into cybersecurity engineer roles.

A Map of Cybersecurity Roles by Career Stage and Function



1) Bubble size not to scale.

Source: "Cybersecurity Roles and Job Titles," The George Washington University Department of Computer Science; Burning Glass Labor/Insight; EAB interviews and analysis.

Industry Verticals in Critical Sectors

As cybersecurity demand grows across sectors, forward-thinking colleges are launching programs that address the specialized needs of local industries. These programs also provide on-ramps for workers in other functions in those industries to move into cybersecurity positions.

In fall 2012, River Valley Community College launched a Cybersecurity and Healthcare IT Certificate in response to unmet demand from local hospitals and health systems. This certificate combines existing networking courses with new content specific to health care, including electronic medical records and Health Insurance Portability and Accountability Act (HIPAA) regulations. Though experienced cybersecurity workers may use the certificate for career advancement, those newly entering the field typically count the credits toward an associate's degree.

In fall 2013, in response to the growing complexity of industrial control systems, Cleveland Community College launched a Teleoperation and Cybersecurity Certificate that combines courses from its IT and industrial services programs. As automation displaces workers from traditional manufacturing roles, this certificate often enrolls former machine operators and shift leaders learning how to maintain the same systems that made their previous training obsolete.





New Programs Emphasize Field-Specific Security Skills



Safeguarding Patient Information

Cybersecurity and Healthcare IT Certificate

Seven-course curriculum blends existing IT coursework with new health-specific content:

-  Information Assurance
-  Network Security
-  Enterprise Security Management
-  Healthcare Information Technology

Tuition and fees: \$4,185 in-state
Time to Completion: Three semesters





- | | |
|---|---|
| Job Outcomes | Further Study |
| <ul style="list-style-type: none"> ▪ Information Security Analyst ▪ Health Information Technician | <ul style="list-style-type: none"> ▪ A.S. in Cybersecurity and Healthcare IT ▪ A.S. in Computer Technology-Networking |



Protecting Industrial Infrastructure

Teleoperation and Cybersecurity Certificate

Four-course curriculum blends existing IT and industrial services coursework:

-  Security Concepts
-  Advanced LANs
-  SCADA Systems
-  Automation Troubleshooting

Tuition and fees: \$901 in-state
Time to Completion: Two semesters

- | | |
|--|---|
| Job Outcomes | Further Study |
| <ul style="list-style-type: none"> ▪ Automation Technician ▪ Plant Electrician | <ul style="list-style-type: none"> ▪ A.A.S. in Automation Engineering Technology |

Source: "Cybersecurity & Healthcare IT," River Valley Community College; "Teleoperation and Cybersecurity Certificate," Cleveland Community College; "Tuition," Cleveland Community College; EAB interviews and analysis.

Cybersecurity for the Masses

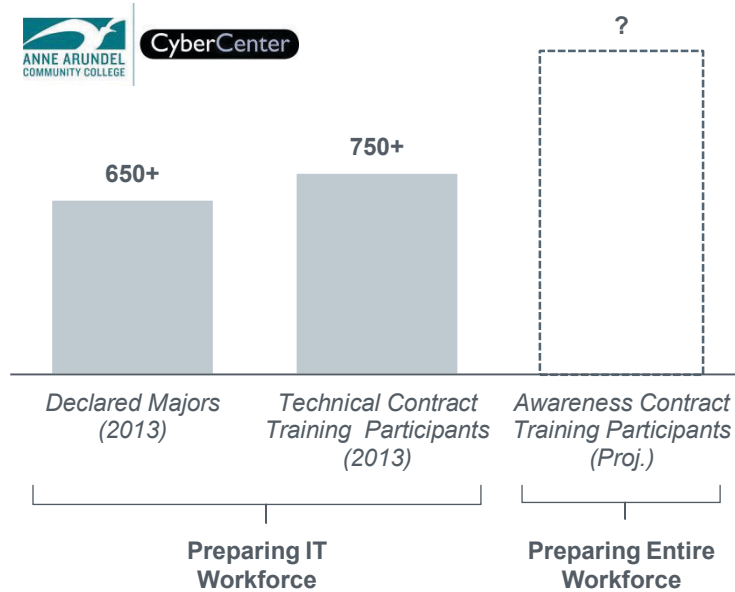
Because of the cost of recruiting cybersecurity professionals, many employers seek to train incumbent workers for cybersecurity positions. The CyberCenter at Anne Arundel Community College offers a range of short-term contract trainings to businesses and government agencies. In 2013, these trainings enrolled over 750 participants from more than 15 employers.

This year, CyberCenter introduced a new set of contract trainings that teach workers outside IT to support enterprise-level security initiatives. These non-IT workers represent a relatively new audience for cybersecurity education, and they reflect the growing need for security awareness across all business functions.

To allow for efficient customization, Anne Arundel's trainings follow a modular structure. Ten core modules are available in broadly applicable topics such as passwords, computer security, and mobile security. Specialized modules that target the needs of particular industries or roles complement the core modules. For example, an accounting firm could require its staff to complete the Cybersecurity for CPAs module or its firm-wide leaders to complete the Cybersecurity for C-Suite Executives module.

Anne Arundel's "Build Your Own" Contract Trainings Target Non-IT Professionals

Expanding Beyond the IT Workforce Cybersecurity Enrollments and Projections



Customized for Industry and Client Available Mix-and-Match Modules

Core		Specialized
Introduction to Security	Workplace Security	Cyber for C-Suite Executives
Passwords	Data Integrity	Cyber for Law Practitioners
Computer Security	WiFi Security	Cyber for CPAs
Online Security	Social Engineering	Cyber for Health Care Professionals
Mobile Security	Network & Cloud Security	

✓ Specialized modules adapt curriculum to needs of diverse industry sectors

✓ Flexible schedules and on-site delivery options provide the convenience of self-paced trainings in a face-to-face group setting

Source: "Cybersecurity Awareness Training," Anne Arundel Community College; EAB interviews and analysis.

Workers Scarce, Teachers Scarcer

As colleges expand existing cybersecurity programs, they almost always face challenges recruiting new faculty. Given the shortage of cybersecurity workers and the high salaries they command, program administrators struggle to identify qualified instructors (i.e., those with both technical and pedagogical skills) and offer them competitive salaries.

Despite the challenge, some colleges have successfully recruited instructors from the professional networks of current faculty. Faculty commonly have contacts within industry who are qualified to teach cybersecurity courses. To identify these contacts, colleges can offer current faculty incentives to bring potential instructors to networking events.

Program administrators may also find potential instructors in professional associations, such as the Information Systems Security Association (ISSA). By attending local chapter meetings, program directors can meet workers committed to career advancement, who may view teaching as a new leadership opportunity.

Recruiting Faculty Through Local Professional Networks



Workforce Shortage Extends to Classrooms

“If there’s a shortage of workers with cybersecurity skills, there’s an even greater shortage of workers with both cybersecurity *and* teaching skills. And given what industry pays cybersecurity professionals, we struggle to offer a competitive faculty salary.”

*Program Director,
Mid-Atlantic Community College*

Locating Qualified and Willing Instructors

Current Faculty Contacts

Professional networks from current or previous roles in industry



“Bring a Friend” Faculty Events

Host a networking reception, offering a small incentive (e.g., gift drawing) to each faculty member who brings a professional contact qualified to teach a course

Professional Associations

Hubs for workers committed to leadership roles within field



Teaching as a “Stretch Role”

Meet with local chapters of IT and cybersecurity associations, presenting part-time instruction as a career advancement opportunity

Professional Benefits of Teaching

- Education:** Tuition waivers on certification and CEU courses
- Influence:** Ability to shape undergraduate curriculum
- Recruitment:** Access to program graduates for hiring

Study Road Map

- 1 | Understanding Cybersecurity Demand
- 2 | New Directions in Cybersecurity Education
- 3 | Appendix: Assessing the Opportunity

Assessing the Opportunity

Where Can Our Institution Launch or Grow Cybersecurity Programs?

Identifying Resources for Program Launch

1. Do we have capacity in (or resources to grow) existing IT and networking courses?
Yes ___ No___
2. Can we leverage the professional networks of current IT faculty to recruit cybersecurity instructors?
Yes ___ No___
3. Do we have the infrastructure to host custom contract trainings in cybersecurity or security awareness?
Yes ___ No___
4. Would existing programs in other fields (e.g., business, policy) benefit from a cybersecurity specialization?
Yes ___ No___

If you answered "yes" to two or more of these questions, please continue to the section below.

Generating Ideas for Program Design and Marketing

1. Could we develop articulation agreements with university partners with bachelor's degrees in IT?
Yes ___ No___ *If "yes," see page 15.*
2. Could we build on existing K-12 partnerships to introduce high school students to cybersecurity careers?
Yes ___ No___ *If "yes," see page 16.*
3. Do any industries with strong local presence (e.g., health care) have specialized cybersecurity needs?
Yes ___ No___ *If "yes," see page 18.*
4. Would local job seekers leaving downsizing industries benefit from on-ramps into the cybersecurity field?
Yes ___ No___ *If "yes," see page 18.*
5. Do employer partners face cybersecurity skill gaps that incumbent workers could be trained to fill?
Yes ___ No___ *If "yes," see page 19.*

Job Market Intelligence: Report on the Growth of Cybersecurity Jobs

Matching People
& Jobs

Resume Parsing &
Management

Reemployment
& Education
Pathways

Real-Time
Labor Market
Intelligence

Market Overview: Cybersecurity Jobs

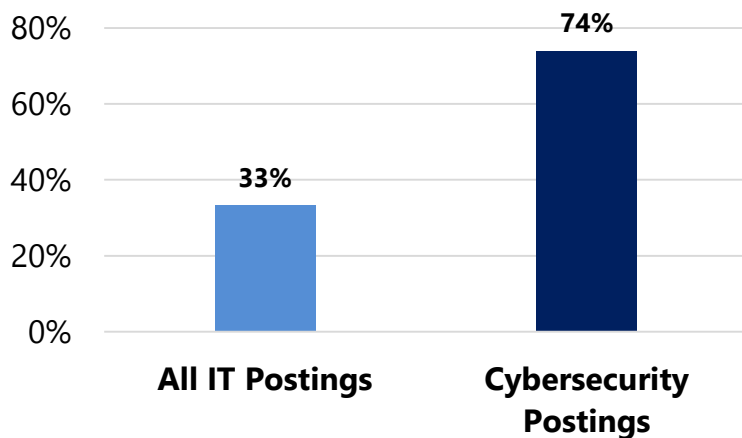
The Market for Cybersecurity Jobs Is Large and Growing

- In 2013, there were 209,749 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for nearly 10% of all IT jobs.**
- Cybersecurity postings have **grown 74%** from 2007-2013. This growth rate is over 2x faster than all IT jobs.

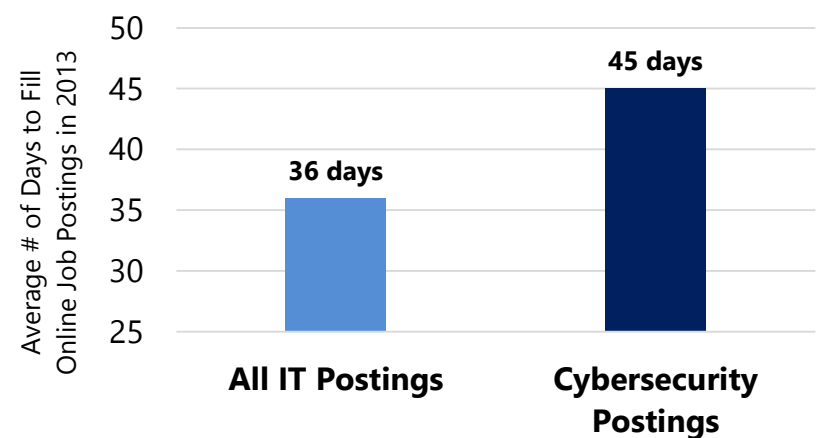
Demand for Cybersecurity Talent Is Outstripping Supply

- Cybersecurity job postings took **24% longer to fill than all IT job postings and 36% longer than all job postings.**
- The demand for cybersecurity talent appears to be outstripping supply. In the US, employers posted 50,000 jobs requesting CISSP, recruiting from a pool of only 60,000 CISSP holders.

Growth in Job Postings (2007-2013)



Posting Duration (2013)

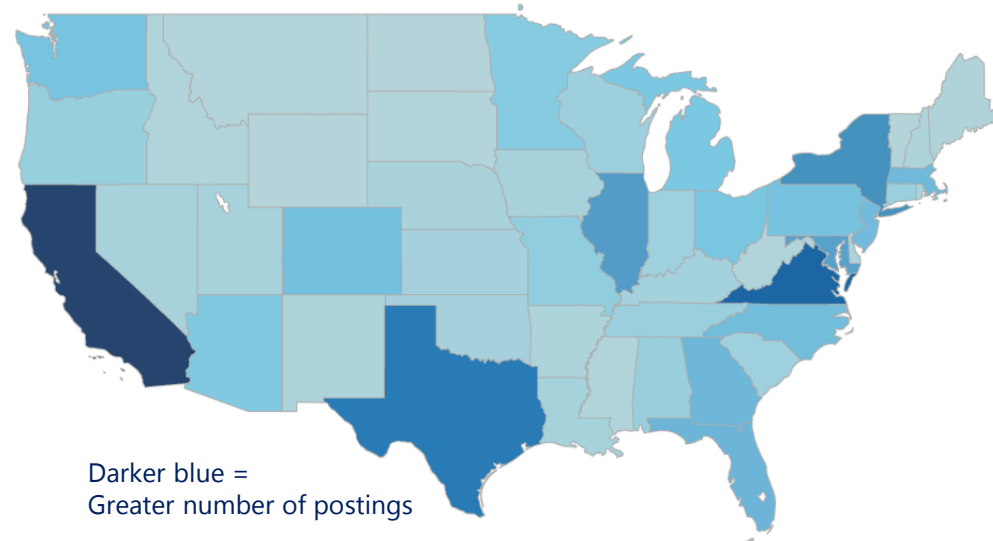


Cybersecurity Job Postings by State

Top States by Total Postings*

	State	Total Postings	Postings/10,000 Residents	% Growth (2007-2013)
1	California	27,084	7.1	64%
2	Virginia	20,507	25.1	53%
3	Texas	16,376	6.3	97%
4	New York	12,405	6.3	59%
5	Illinois	11,136	8.6	116%
6	Maryland	10,627	18.1	94%
7	Florida	7,923	4.1	46%
8	Georgia	7,539	7.6	214%
9	Massachusetts	7,107	10.7	76%
10	New Jersey	6,814	7.7	12%
11	North Carolina	6,676	6.8	129%
12	Colorado	6,039	11.6	158%
13	Pennsylvania	5,630	4.4	22%
14	Washington	5,444	7.9	76%
15	Ohio	5,086	4.4	34%

Cybersecurity Job Postings in 2013 By State



*See Appendix 1 for state-level data tables on total postings and postings growth.

Cybersecurity Job Postings by City

Top Cities by Total Postings

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Washington D.C.	23,457	35%
2	New York	15,632	38%
3	San Francisco/ San Jose	12,697	67%
4	Chicago	9,723	115%
5	Dallas	7,669	110%
6	Los Angeles	7,123	38%
7	Boston	6,336	87%
8	Atlanta	5,883	204%
9	Baltimore	4,514	116%
10	Seattle	4,470	63%









Top Cities by Growth

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Atlanta	5,883	204%
2	Denver	3,482	200%
3	Austin	1,979	172%
4	Charlotte	2,410	127%
5	Portland (OR)	1,981	119%
6	Baltimore	4,514	116%
7	Chicago	9,723	115%
8	Phoenix	2,885	114%
9	San Diego	3,665	112%
10	Dallas	7,669	110%

*Top cities by growth were calculated by taking the top 25 cities by total postings, and ranking them by growth in job postigs

Cybersecurity: Demand by Industry Sector

- Professional Services, Manufacturing, and Finance are the leading industries for cybersecurity professionals.
- The share of cybersecurity jobs coming from the Manufacturing & Defense, Public Administration, and Retail Trade industries is increasing over time compared to other industries.

Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)	2010-2013 Postings Growth
Professional Services	38%	80,446 	29%
Manufacturing & Defense*	14%	28,331 	16%
Finance and Insurance	12%	24,145 	89%
Information	8%	15,820 	36%
Health Care	6%	12,257 	73%
Public Administration	5%	11,204 	N/A**
Retail Trade	5%	10,203 	94%
Other	13%	27,384 	N/A**

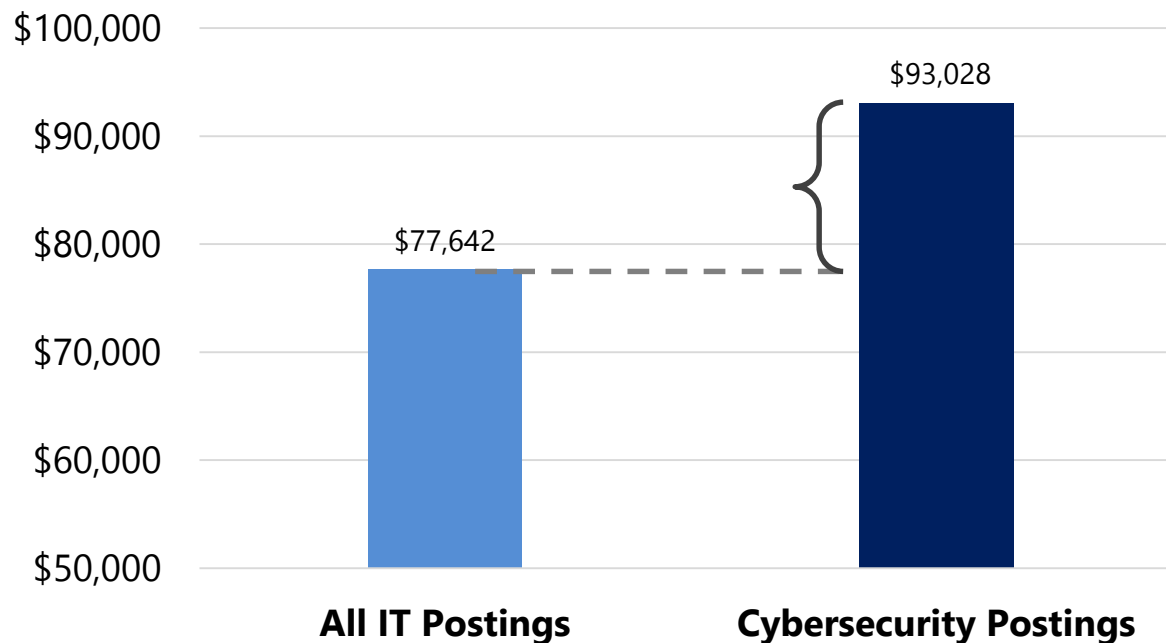
*Manufacturing Sector includes services divisions of a number of defense contractors (e.g. Raytheon) and computer manufacturers (e.g. Hewlett Packard).

** Industry growth rates are suppressed for the Public Administration and Other industry sectors because a significant portion of labor market demand in these industries exists offline.








Cybersecurity Jobs Offer Increased Salaries

Cybersecurity Jobs Pay a Premium

On average, cybersecurity salaries offer a premium of over \$15,000 over the salaries for IT jobs overall.











Cybersecurity: Demand by Role

Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	28%	40,898 
Manager/Administrator (e.g. Data Security Administrator, Information Security Manager)	19%	28,310 
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	26,219 
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	9%	13,154 
Auditor (e.g. IT Auditor, IT Sarbanes-Oxley Auditor)	5%	7,307 
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	6,670 
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,121 

Demand for Certifications

Certification requirements are more common in cybersecurity roles than in IT generally.

- 51% of all cybersecurity positions request at least one of the certifications listed below.
- 14% of all IT positions request a certification of any kind.

Certification*	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)
CISSP Certified Information System Security Professional	24%	49,522 
CISA Certified Information Systems Auditor	16%	33,290 
Security+ Certified Information Security Manager	8%	17,019 
CISM Certified Information Security Manager	7%	15,083 
GIAC Security Essentials	3%	5,639 
CIPP Certified Information Privacy Professional	2%	4,168 
SSCP Systems Security Certified Practitioner	2%	4,039 
GIAC GCIH GIAC Certified Incident Handler	2%	3,163 

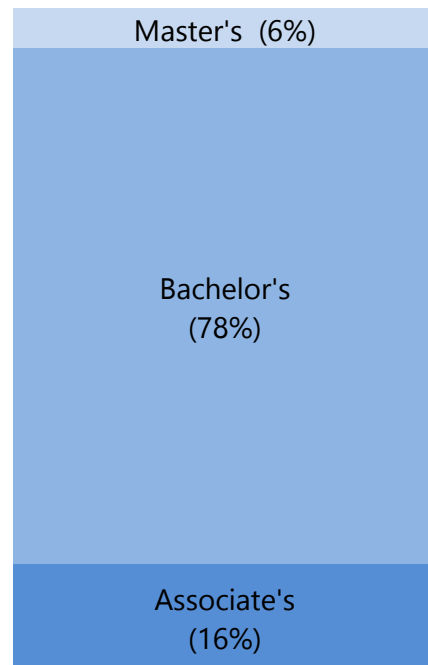
*Certification requirements are not mutually exclusive

Education and Experience Requirements

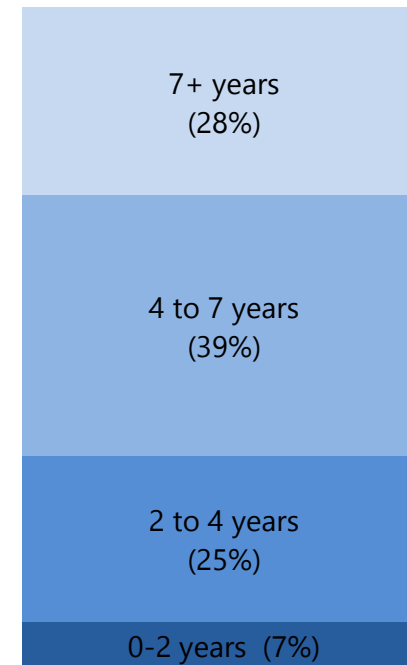
Cybersecurity Jobs Require Significant Education and Experience

- 84% of cybersecurity postings specify at least a Bachelor's.
- 2/3 of cybersecurity postings require at least 4 years of experience.

Minimum Education Level



Minimum Experience



Methodology

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100M worldwide postings collected since 2007. Each day, Burning Glass visits over 32,000 online jobs sites to collect postings. Using advanced text analytics, over 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials and salary. Postings are then deduplicated and placed in a database for further analysis.

This report classifies cybersecurity jobs as those which have a cybersecurity-related title, require a cybersecurity certification or request cybersecurity specific skills. Cybersecurity related titles used to define the roles analyzed in this report include "network security", "information security", "information assurance", and "penetration tester". Cybersecurity skills include information assurance, cryptography, computer forensics, malware analysis, 800-53, and ArcSight. The cybersecurity related certifications are listed on Slide 7.

The data in this report use a broader definition of cybersecurity roles than Burning Glass's 2012 report examining the same topic. That report looked only at those roles with cybersecurity specific titles, whereas, this update includes jobs with cybersecurity titles, certifications or skills.

About Burning Glass

Burning Glass's tools and data are playing a growing role in informing the global conversation on education and the workforce by providing researchers, policy makers, educators, and employers with detailed real-time awareness into skill gaps and labor market demand. Burning Glass's job seeker applications power several government workforce systems and have been shown to have substantive impact on reemployment outcomes and on labor market literacy.

With headquarters in Boston's historic Faneuil Hall, Burning Glass is proud to serve a client base that spans six continents, including education institutions, government workforce agencies, academic research centers, global recruitment and staffing agencies, major employers, and leading job boards.

For More Information

Dan Restuccia

Director of Applied Research

t +1 (617) 227-4800

drestuccia@burning-glass.com

www.burning-glass.com

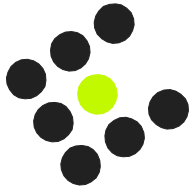
Appendix 1: Top Cities Ranked By Total Postings

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Washington, D.C.	23,457	35%
2	New York	15,632	38%
3	San Francisco/San Jose	12,697	67%
4	Chicago	9,723	115%
5	Dallas	7,669	110%
6	Los Angeles	7,123	38%
7	Boston	6,336	87%
8	Atlanta	5,883	204%
9	Baltimore	4,514	116%
10	Seattle	4,470	63%
11	Philadelphia	4,032	-4%
12	San Diego	3,665	112%
13	Houston	3,648	67%

	City (MSA)	Total Postings	% Growth (2007-2013)
14	Denver	3,482	200%
15	Detroit	3,093	84%
16	Minneapolis	2,929	42%
17	Phoenix	2,885	114%
18	St. Louis	2,506	82%
19	Miami	2,496	29%
20	Charlotte	2,410	127%
21	Virginia Beach	2,335	74%
22	Portland (OR)	1,981	119%
23	Austin	1,979	172%
24	Tampa	1,932	58%
25	San Antonio	1,841	68%

Appendix 2: State-Level Data

	State	Total Postings	Postings/ 10,000 Residents		State	Total Postings	Postings/ 10,000 Residents		State	Total Postings	Postings/ 10,000 Residents
1	California	27,084	7.1	21	Alabama	2,266	4.7	41	Maine	489	3.7
2	Virginia	20,507	25.1	22	Connecticut	2,234	6.2	42	West Virginia	475	2.6
3	Texas	16,376	6.3	23	Tennessee	2,134	3.3	43	Idaho	434	2.7
4	New York	12,405	6.3	24	Wisconsin	1,991	3.5	44	Alaska	402	5.5
5	Illinois	11,136	8.6	25	Indiana	1,916	2.9	45	Mississippi	399	1.3
6	Maryland	10,627	18.1	26	South Carolina	1,846	3.9	46	South Dakota	234	2.8
7	Florida	7,923	4.1	27	Kentucky	1,451	3.3	47	Montana	199	2.0
8	Georgia	7,539	7.6	28	Kansas	1,261	4.4	48	North Dakota	186	2.7
9	Massachusetts	7,107	10.7	29	Oklahoma	1,253	3.3	49	Vermont	141	2.3
10	New Jersey	6,814	7.7	30	Louisiana	1,229	2.7	50	Wyoming	109	1.9
11	North Carolina	6,676	6.8	31	Utah	1,202	4.2				
12	Colorado	6,039	11.6	32	Iowa	1,182	3.8				
13	Pennsylvania	5,630	4.4	33	Hawaii	1,177	8.5				
14	Washington	5,444	7.9	34	Nevada	1,103	4.0				
15	Ohio	5,086	4.4	35	Rhode Island	1,053	10.0				
16	Michigan	4,691	4.7	36	Nebraska	1,008	5.4				
17	Arizona	4,252	6.5	37	Delaware	836	9.1				
18	Minnesota	3,718	6.9	38	New Mexico	703	3.4				
19	Missouri	3,079	5.1	39	Arkansas	679	2.3				
20	Oregon	2,349	6.0	40	New Hampshire	532	4.0				



C·O·E

CENTERS OF EXCELLENCE
Inform Connect Advance

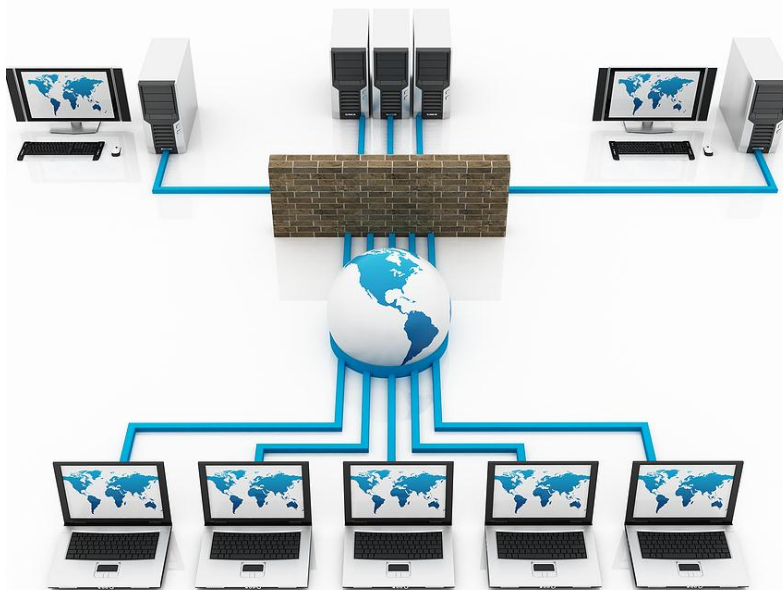
ENVIRONMENTAL SCAN

CYBERSECURITY

Los Angeles and Orange Counties

JUNE 2012

ENVIRONMENTAL SCAN



CENTER OF EXCELLENCE
Los Angeles and
Orange Counties

Audrey Reille, Director
Mt. San Antonio College
1100 N. Grand Avenue,
Walnut, CA 91789
909-274-6106
areille@mtsac.edu

www.coecc.net

An Initiative of



**ECONOMIC &
WORKFORCE
DEVELOPMENT**
through the
**CALIFORNIA
COMMUNITY
COLLEGES**



Mission: The Centers of Excellence, in partnership with business and industry, deliver regional workforce research customized for community college decision making and resource development.

Vision: We aspire to be the premier source of regional economic and workforce information and insight for community colleges.

Please consider the environment before printing. This document is designed for double-sided printing.

© California Community Colleges' Centers of Excellence, 2012.

Contents

Executive Summary 4

Introduction..... 5

Industry Overview 5

Occupational Overview 10

Employer Needs and Challenges 13

Educational Requirements 18

Community Support and Resources 20

College Response 21

Implications and Recommendations for Community Colleges..... 23

Conclusion 23

Recommendations 24

References and Resources..... 25

Appendix A: How to Utilize this Report..... 27

Appendix B: Complete List of Most Common Security Threats 28

Appendix C: Complete List of Occupational Skills 29

Appendix D: Complete List of Regional Programs and Courses 38

“There are only about 1,000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace; however, the United States needs about 10,000 to 30,000 such individuals.”

— Center for Strategic and International Studies, 2011¹

Executive Summary

Cybersecurity is crucial not only to the economy but also to homeland security; therefore, training a qualified workforce to enter this field is a top priority for the United States. According to the Center for Strategic and International Studies, “There are only about 1,000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace; however, the United States needs about 10,000 to 30,000 such individuals.”²

To understand the regional workforce development needs for cybersecurity, the COE conducted secondary research, analyzed skill requirements from dozens of online job postings, and conducted a survey of 100 companies employing cybersecurity professionals. Respondents to the survey reported difficulty hiring Systems Analysts (87%), Security Support Specialists (86%), Programmers (86%), Computer Specialists (84%), Software Engineers (82%), Computer and Information Systems Managers (79%), Database Administrators (77%), Network and Computer Systems Administrators (76%) and Network Systems and Data Communications Analysts (72%).

In 2011, there were 163,607 jobs in Los Angeles and Orange Counties in the computer and information technology sector. Employment forecasts predict a 7% growth, adding 12,241 new jobs by 2016. Considering turnover rates and projected retirements, the number of job openings could be as high as 26,495 in the five-year period. Individuals working in computer and information technology jobs need to be knowledgeable about cybersecurity to perform their jobs, and thousands should become cybersecurity experts to meet the demand from employers.

This report presents data on the labor market (i.e., employment, job growth, wages), industry trends, employment requirements (skills, experience and education), existing community college programs, and recommendations to meet employers’ needs. Colleges are encouraged to:

1. Consider adding courses in cybersecurity to their computer science programs.
2. Create new Certificates or Degrees in Cybersecurity.
3. Make sure that their programs and curriculum include the skills listed for cybersecurity occupations in this report (see appendix C for details).
4. Include representation from cybersecurity employers on advisory committees to be aware of new trends keep programs up to date.
5. Contact CyberWatch West³, a valuable resource for curriculum development, partnership with businesses and services to students.
6. Coordinate with other colleges in the region to avoid duplication of efforts and possible competition.
7. Organize internships and opportunities for their students to gain hands-on experience.

¹Center for a New American Security. “America’s Cyber Future: Security and Prosperity in the Information Age, Volume I.” June, 2011.

²Ibid.

³CyberWatch West: <http://cyberwatchwest.org/>

Introduction

The California Community Colleges System has charged the Centers of Excellence (COE), part of the Economic & Workforce Development (EWD) Network, to identify industries and occupations with unmet employee development needs and introduce partnering potential for colleges. The focus of this report is to examine the workforce development needs of cybersecurity occupations.

Accompanying the advances in modern computer technology there is a need for information, program, and network protection. It is the responsibility of cybersecurity professionals to protect such networks and electronic information systems from unauthorized access to sensitive information. Employee responsibilities are vast and may include functions such as: protecting computer and online-based systems as well as designing new systems, software, and processes that will be impervious, or at least resistant, to cyber attacks. Given this broad skill-set, the workforce expands well beyond the firms providing security-related goods and services (e.g. McAfee or Norton). In fact, every business storing and managing data via computer technology has a need for network and data security.

While computer technology offers many modern conveniences – such as mass data storage, online banking and bill paying, and digital collaboration, to name a few – it simultaneously creates a new world of virtual threats. Such threats range from viruses and worms, which can cause damage to personal computers, to identity and credit theft. In 2010 IBM found 8,000 new web vulnerabilities and attacks to online information, representing a 27% increase from the previous year.⁴ It is the responsibility of cybersecurity professionals to protect the end user from such threats and to ensure that sensitive information remains private.

However, as illustrated in the leading quote of this report, there is a shortage of qualified cybersecurity professionals in the United States. In May 2011 Dice, North America's leading career website for technology and engineering professionals, reported that California has the largest shortage of qualified technology related talent, including cybersecurity, as there are nearly three jobs open to every computer science graduate. Further, Dice named Los Angeles as one of the most impacted areas.⁵

The purpose of this report is to determine the workforce development needs related to cybersecurity in Los Angeles and Orange Counties. Specifically, the Center of Excellence studied these occupations to determine: (a) job growth; (b) the most important skills, and educational and experience requirements to gain employment in the field; and (c) recommendations for the community colleges to strengthen cybersecurity curriculum.

To determine skill sets needed to work in cybersecurity, the COE conducted an in depth analysis of 44 job postings, consequentially compiling a list of 15 critical skills. In addition, 100 employers participated in an industry survey to determine the importance of each of the 15 skills for prospective job candidates, firm-level job growth, educational and experience requirements for new hires, and recommendations for the community colleges.

Industry Overview

Cybersecurity extends far beyond its roots in information technology. In fact, it can be found in nearly every industry that utilizes computer technology to store and manage information. The workforce is composed of various occupations that protect networks and electronic information systems from unauthorized access to sensitive information. As such cybersecurity spans both the private and public sectors.

⁴ Takanashi, Dean. "IBM Says it Sees 13 Billion Cybersecurity Alerts Every Day." March 31, 2011.

⁵ Dice. "America's Tech Talent Crunch." May 1, 2011.

Cybersecurity in the Private Sector

In the private sector, cybersecurity is necessary in both business and our personal lives. In addition to being a key element of computing companies such as Intel and Google it is essential to most large industries such as health care, banking, and credit. The health care industry, for example, needs data security to protect patients' medical records. Banking requires rigorous online security to protect customer funds. And the credit industry requires elaborate security networks to ensure individuals' personal identity and information, amongst other things. In addition, any business storing company information via cyberspace requires intense security to ensure that valuable information is kept confidential.

The number of cyber attacks in the U.S. has grown tremendously over the past few years and can absorb an extensive amount of organizational resources. A study of 45 U.S. businesses, by the Ponemon Institute, discovered an alarming 50 successful cyber attacks per week. This averages out to one successful attack to each business every week. Further it was concluded that these attacks — ranging from theft of employee, credit, customer, and competitive business information — were estimated to cost a median-based average of \$3.8 million yearly.⁶ A recent press release from the U.S. Office of Homeland Security made claim that over \$1 trillion of intellectual property has been stolen from U.S. businesses.⁷



Since information is the keystone of many modern organizations, it can be very costly if lost, leaked out, or stolen — even if by a single employee. A report by Google estimated that the average employee laptop contains \$525,000 worth of sensitive information.⁸ Therefore, to ensure the highest quality of information security, cybersecurity professionals are not only required to focus on the business at large, but also on determining the information access needs to each individual employee.

Further, cybersecurity is equally important at the personal level as it is to business. As individuals have the modern conveniences of online banking, bill paying, and social networking (to name a few), these capabilities create vulnerabilities to personal information. In 2010, the U.S. Department of Justice published a report claiming that 11.7 million persons, representing 5% of all North Americans above the age of 16, had experienced some form of identity theft within a two-year period.

These breaches of personal identity varied from breaking into personal credit cards and existing bank accounts to the theft of personal information (e.g. social security numbers).

Most common amongst the listed crimes was the unauthorized usages of personal credit cards, which impacted 6.2 million people over the same two-year period.⁹ Given these outrageous statistics, it is critical that cybersecurity professionals are trained to develop networks, systems, and software that are impenetrable to such attacks.



Cybersecurity in the Public Sector

The full spectrum of cyber threats, however, runs all the way to the highest level of national security. According to President Barack Obama, in the 21st century, not only is North America's economic prosperity dependent on cybersecurity but it "is also a matter of public safety and national security."¹⁰

⁶ Ponemon Institute. "First Annual Cost of Cyber Crime: Bench Mark Study of U.S. Companies." July 2010.

⁷ Phillips, Leslie. "Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack." January 26, 2011.

⁸ Google. "Off-Network Workers – the Weakest Link to Corporate Web Security," 2008.

⁹ Langton, Lynn & Planty, Michael. "Victim of Identity Theft, 2008." U.S. Dept. of Justice, Bureau of Justice Statistics, December 2010

¹⁰Obama, President Barack. "Remarks By The President On Securing Our Nation's Cyber Infrastructure." May 29, 2009.

President Obama continued his remarks by asserting that we are dependent on computer networks to deliver our oil, gas, power and water – all of public interest.¹¹ Since these plants are controlled by online systems they are vulnerable to cyber threats and must be protected.¹²

On the other hand, cyber threats at the National level may take the shape of breaches to government systems, interferences with communications, and loss of classified military information, to name a few. According to a recent study published by the Center of New American Security, government networks experience 1.8 million cyber attacks each month. These attacks, varying in sophistication, target Congress and other federal agencies.¹³ Further, U.S. intelligence officials predict that the next significant terrorist attack against the country will be a cyber attack aimed at damaging financial and government systems.¹⁴

Given the high level of concern with cybersecurity at the National level, multiple initiatives and bills have been passed to increase the security of North America’s digital infrastructure. For example, on January 26, 2011 the Senate Committee on Homeland Security and Governmental Affairs introduced a bipartisan bill to put a stop to cyber crime aimed at harming our technology infrastructures.

“The legislation calls for urgent action to safeguard critical infrastructure, including the electric grid, military assets, the financial sector, and telecommunications networks. It urges incentive for the private sector to assess the risk of cyber terrorism and take action to prevent it and promote investments in the American IT sector, which will create high-paying jobs. The bill also seeks to improve the capability of the U.S. government to assess cyber risks, and to prevent, detect and respond to attacks. It calls for safeguards to protect consumers by preventing identity theft and guarding against abuses of personal information, and seeks to promote cooperation between nations in responding to cyber threats.¹⁵

Employer Survey

Cybersecurity professionals work across all industries. The Center of Excellence conducted an online employer survey to collect more information on businesses that employ cybersecurity professionals, industries, firm size, occupations, skills, job requirements and trends. One hundred businesses in Los Angeles and Orange counties responded to the survey. They indicated the industries to which they belong. Eleven percent (11%) of the firms surveyed was in the field of education. Another 11% were in health care and social services. Following these industries, 9% of the firms were in professional and technical services, 8% were in computer hardware or software, and 7% were in financial services.

Exhibit 1: Percentage of cybersecurity firms connected to specific industries

Industries represented in the Employer Survey			
Education	11%	Engineering	6%
Health care/Social services	11%	Entertainment	6%
Professional and technical services	9%	Wholesale distribution and services	6%
Computer hardware or software	8%	Government	4%
Financial services	7%	Telecommunications	3%
Manufacturing	7%	Other ¹⁶	22%

¹¹Obama, President Barack. “Remarks By The President On Securing Our Nation’s Cyber Infrastructure.” May 29, 2009.

¹²Bliss, Jeff. “U.S. Nuclear Plants Vulnerable to Cyber Attacks, Analysts Say,” November 17, 2010.

¹³Center for a New American Security. “America’s Cyber Future: Security and Prosperity in the Information Age, Volume I.” June, 2011.

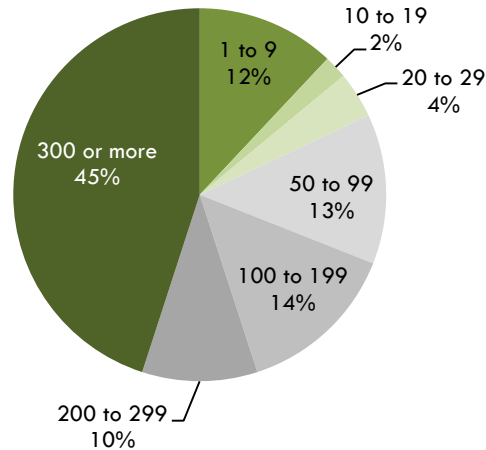
¹⁴Serrano, Richard A. “U.S. Intelligence Officials Concerned About Cyber Attacks,” February 11, 2011.

¹⁵Senate Committee on Homeland Security and Governmental Affairs. “Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack.” January, 26, 2011.

¹⁶Industries reported as other: retail, insurance, professional services (business), real estate, travel and transportation, utilities, advertising, broadcast cable/television/radio/media, construction, legal, and non-profit.

The majority of firms (69%) that participated in this survey are large firms employing over 100 individuals; 13% are medium sized firms employing between 50 and 99 individuals; and 18% are small firms employing 49 individuals or fewer. Exhibit 2 illustrates firm size of our sample.

Exhibit 2: Sample Firm Size



Cybersecurity Trends

As computer technology becomes increasingly complex, so do its vulnerabilities. Due to their rapid emergence and adoption, mobile devices and mobility, social media, and cloud computing,¹⁷ present some of the greatest challenges to the current cybersecurity workforce.

Mobile Devices and Mobility

Mobile devices have revolutionized personal communication and business alike. From a handheld device, individuals can access sensitive personal information including financial information and health records. Likewise, employees no longer need to be in their place of work to access sensitive company data. This vast access to private information creates several security concerns including the use of unsecured networks, personal negligence, and data leaks due to lost or stolen devices. Because of these threats a recent survey of 10,431 industry professionals commissioned by the (ISC)² – a global leader in educating and certifying information security professionals – has concluded that mobile devices could be the single most dangerous threat to organizations in the proximal future.¹⁸

Social Media

The overwhelming popularity of social networking sites makes them and their users a prime target for cyber crime. The vulnerabilities of these sites are based in part on the large amounts of personal information posted on them by their users. As the sites' owners encourage development of third party applications to monetize their infrastructure, the vulnerabilities grow.¹⁹ However, the largest threat produced by these sites emerges as businesses link up to them for various networking activities. For example, Salesforce, a company that aids customers to effectively use cloud computing, is linked to Facebook and Google. Further, IBM has partnered with LinkedIn, a professional social networking site, and Salesforce. This linking creates a shared vulnerability for each of these enterprises as the breaching of one system could potentially give grant access to them all.²⁰

¹⁷ Frost & Sullivan. "The 2011 (ISC)² Global Information Security Workforce Study." March 31, 2011.

¹⁸ Frost & Sullivan. "The 2011 (ISC)² Global Information Security Workforce Study." March 31, 2011.

¹⁹ Barrett, Larry. "Systantec's 'Unlucky 13' Security Trends for 2010." November 20, 2009.

²⁰ Adhikari, Richard. "Online Trust: A Thing of the Past?" January 28, 2009.

Cloud Computing

Cloud computing is the practice of housing information, applications, and systems on a distant server rather than on an organization's server or individual's computer. It offers one of the most secure and cost effective ways of storing data and providing access to shared organizational resources and information.²¹ However, this mode of computing also produces numerous security concerns that the current workforce is not adequately prepared to meet. In a survey conducted on behalf of the (ISC)², 74% of industry professionals reported the need for further training and skill development to be able to address the security challenges of cloud computing.²²

Most Common Security Threats

Though current trends in technology – such as mobile devices and mobility, social media, and cloud computing – greatly impact the nature of cybersecurity, the workforce must also be equipped to handle the most common forms of cyber threats. Recently Norton has listed the top 11 most commonly occurring security threats. Below is a list of the top three. For a complete listing, see appendix B.²³

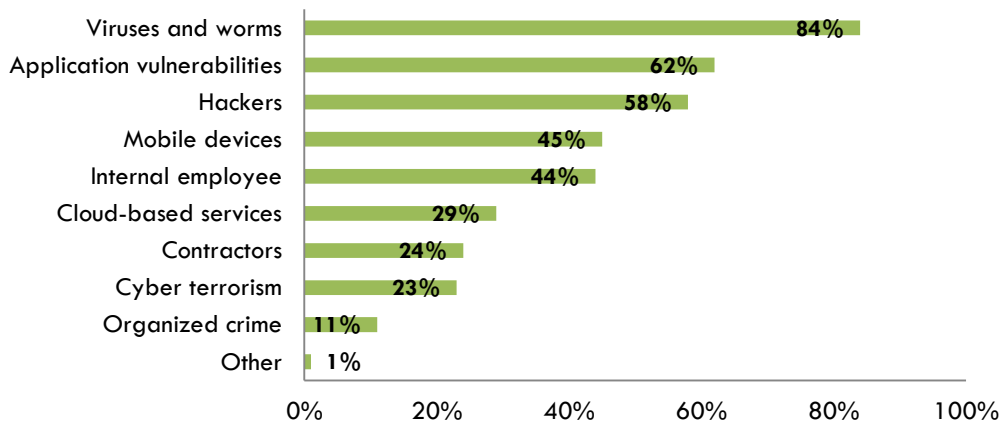
Viruses. A virus is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. The danger level and prevalence of viruses are extremely high, and can cause an entire network to crash, resulting in a massive loss of valuable information.

SPAM, SPIM, and SPIT are all forms of junk mail: SPAM via email, SPIM via instant messenger, and SPIT via internet technology. Though their danger level is generally low, they are extremely prevalent and can grant access to sensitive information if opened by the receiver.

Spoofing, phishing, and pharming are all forms of a program, web page, or individual falsification. Spoofing occurs when a person or program is being impersonated; phishing is the replication of a legitimate webpage; and pharming redirects online traffic to a counterfeit website. The danger level of these forms of falsification is high with an extremely high prevalence, and they can grant access to sensitive information if the user is not careful.

The COE survey also asked 100 employers to identify the most prevalent cybersecurity threats to their organizations.²⁴ The top threats include: viruses and worms (84%); application vulnerabilities (62%); hackers (58%); mobile devices (45%); and internal employees (44%).

Exhibit 3: Most Prevalent Cyber Threats to Employers



²¹ Google. "Off-Network Workers – the Weakest Link to Corporate Web Security." 2008.

²² Frost & Sullivan. "The 2011 (ISC)² Global Information Security Workforce Study." March 31, 2011.

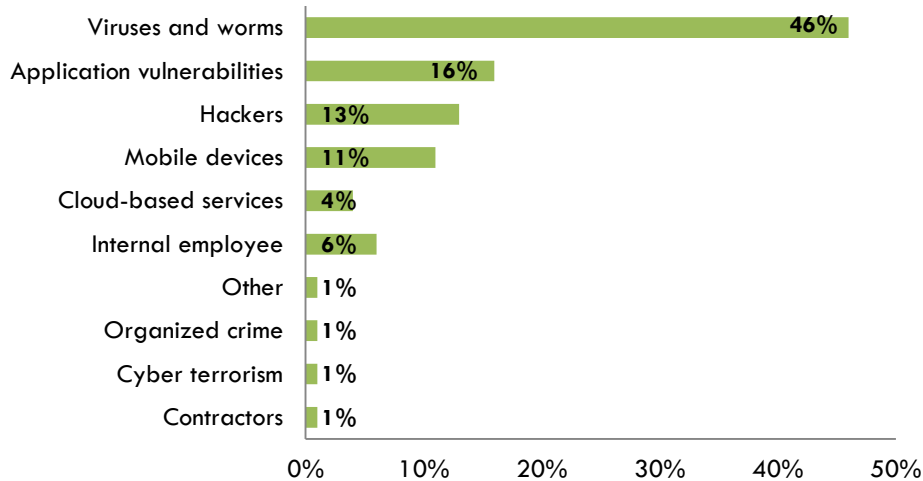
²³ Norton. Available at: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

²⁴ Note: Employers were allowed to give multiple responses regarding the most prevalent cyber threats to their organization.

Employers were also asked which threats posed the single greatest risk to their firm's security.

- Nearly half (46%) of employers claimed viruses and worms pose the greatest threat to their firm.
- 16% claimed that application vulnerabilities pose the greatest threat to their firm.
- 13% claimed that hacker pose the greatest threat to their firm.
- 11% claimed that mobile devices pose the greatest threat to their firm.

Exhibit 4: Greatest Cyber Threat to Employers



Occupational Overview

Cybersecurity professionals do not have specific occupational titles but are included in the broader Information Technology (IT) occupational titles listed below:

- Computer and information systems managers
- Computer programmer
- Computer software engineers, applications
- Computer software engineers, systems software
- Computer support specialists
- Computer system analysts
- Database administrators
- Network and computer systems administrators
- Network systems and data communications analysts
- Computer specialists, all other



Occupational Growth and Wages

Job forecasts predict a 7% growth rate in the next five years for IT professions in Los Angeles and Orange Counties — translating to 12,241 new jobs. Adding turnover and retirements to job growth, the number of job openings is expected to reach 26,495 between 2011 and 2016. The data suggests the strongest growth, in number of new jobs, for computer software engineers and network system and data communication analysts. The occupation of computer programmer is the only one expected to decline slightly, by 1%. Exhibit 5 details the regional growth rate of each of the selected 10 occupations and their respective average hourly wages.

Exhibit 5: Projected Growth, Job Openings and Wages

Occupation	2011 Jobs	2016 Jobs	% Growth	New Jobs	Job Openings*	2011 Median Hourly Wage
Computer And Information Systems Managers	15,247	16,063	5%	816	2,054	\$55.50
Computer Programmers	14,049	13,927	(1%)	(122)	1,340	\$33.14
Computer Software Engineers, Applications	21,461	24,057	12%	2,596	3,498	\$41.10
Computer Software Engineers, Systems Software	21,880	24,217	11%	2,337	3,256	\$44.77
Computer Support Specialists	22,796	23,762	4%	966	4,122	\$22.50
Computer Systems Analysts	21,145	22,517	6%	1,372	3,651	\$33.90
Database Administrators	5,221	5,598	7%	377	812	\$38.18
Network And Computer Systems Administrators	12,912	13,983	8%	1,071	2,148	\$33.27
Network Systems And Data Communications Analysts	18,361	20,615	12%	2,254	3,904	\$28.04
Computer Specialists, All Other	10,535	11,109	5%	574	1,709	\$34.09
Total	163,607	175,848	7%	12,241	26,495	\$36.10

Source: Economic Modeling Specialists, Inc. (EMSI); *Job Openings refers to new jobs (growth) plus replacements.

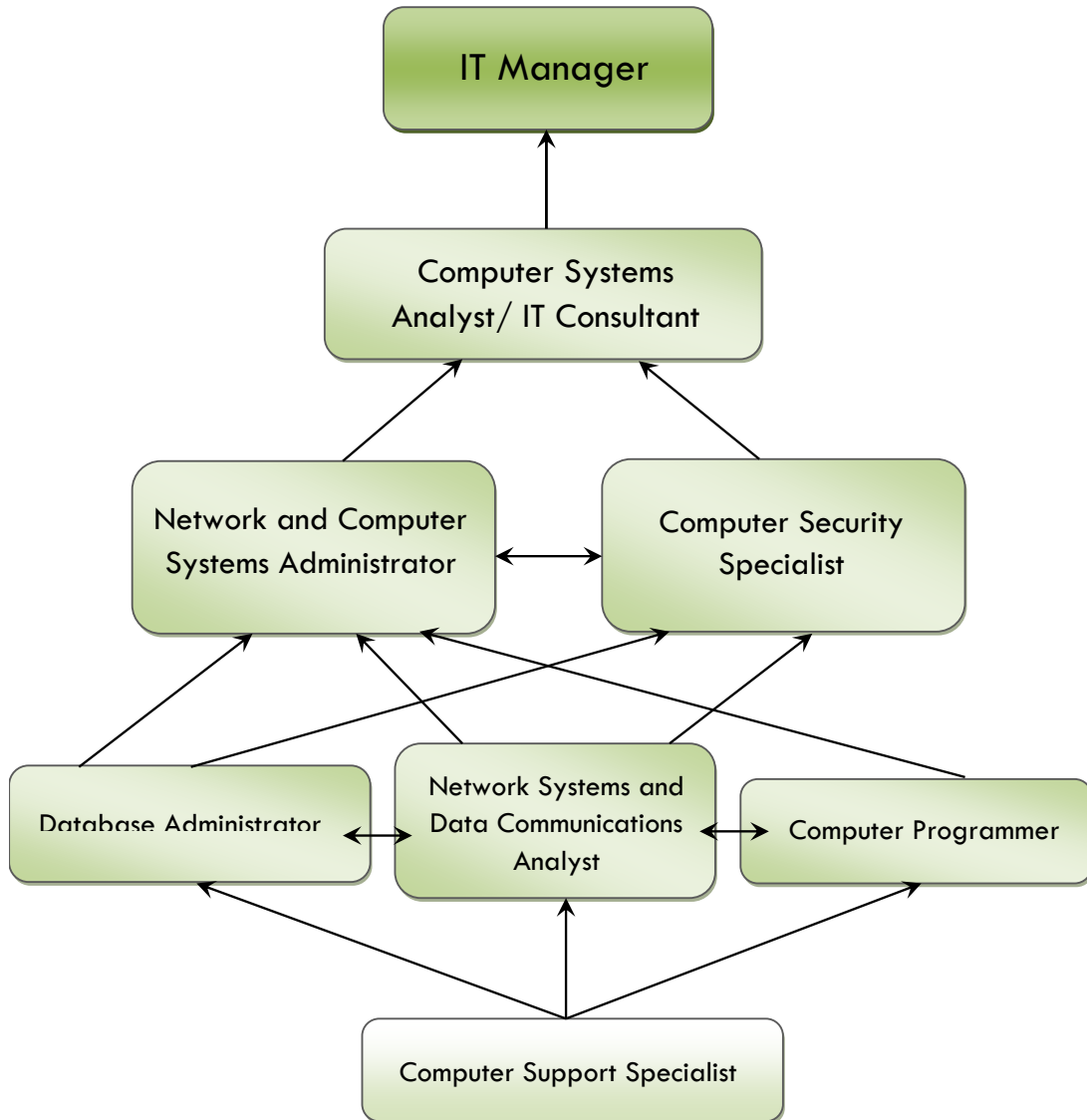
Job growth for these occupations is being driven by three important factors:²⁵

- The complexity of devices, systems, networks, applications, and users drives security concerns and the need to protect information and data. This is highlighted above in discussing a few modern trends that impact security needs.
- Security is becoming operationalized. As a part of this movement, both government and business are moving towards proactive, as opposed to reactive security.
- Government compliance requires due diligence and a longer-term strategy: Government regulations are forcing organizations to evaluate and modify their business processes and operations with security in mind.

These trends and challenges present an excellent opportunity for training at the Community Colleges as individuals seek to complete their first post-secondary degree or certificate, upgrade skills, seek professional development, or simply continue in lifelong learning. Median hourly wages for these professionals range from \$22.50 for entry level jobs such as Computer Support Specialists, to \$55.50 for Computer and Information Systems Managers. Cybersecurity jobs offer high wages and an appealing career ladder.

²⁵Godbe Research. Computer and Information Security Labor Market Study, June 2006.

Cybersecurity Career Ladder

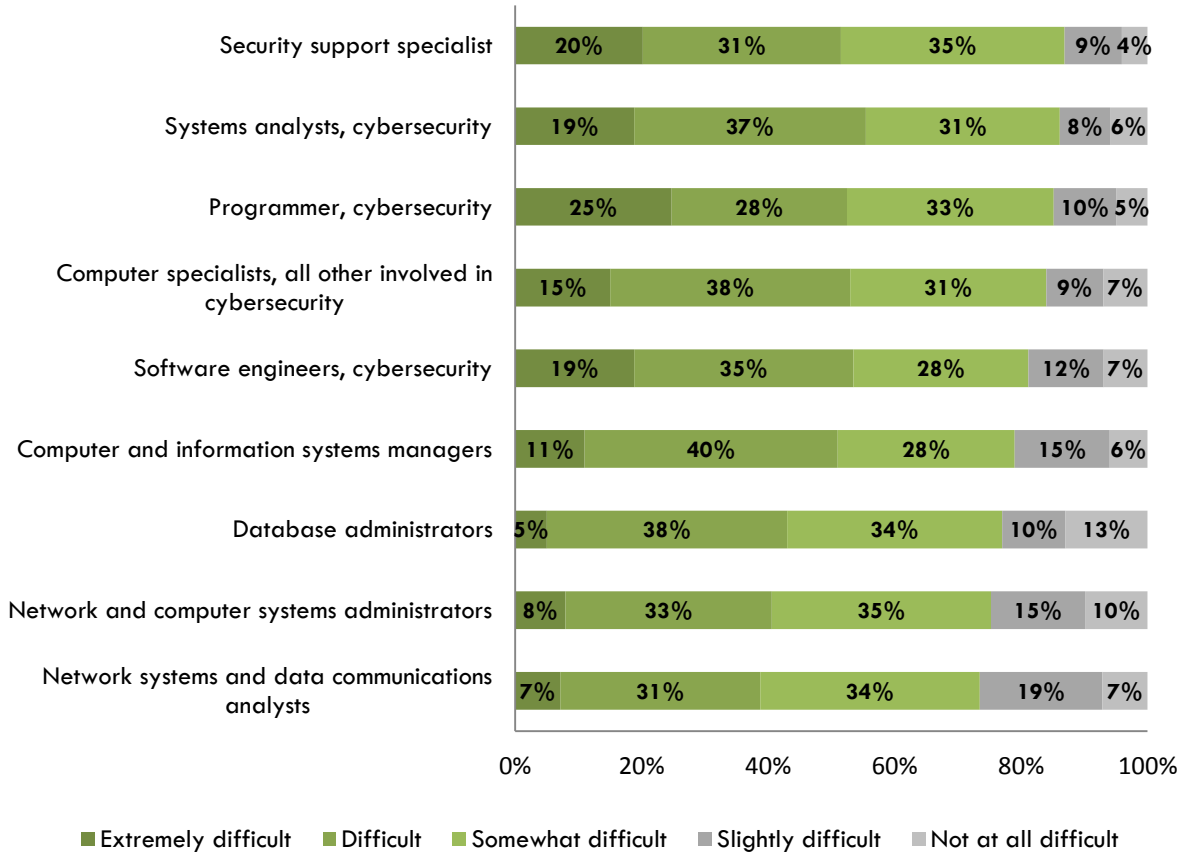


Source: careeronestop.org,
www.careeronestop.org/competencymodel/careerpathway/ReviewCareerPathways/IT_CPW.pdf

Employer Needs and Challenges

The majority of employers surveyed in Los Angeles and Orange Counties indicated that they experience at least some degree of difficulty hiring qualified applicants in all of the cybersecurity occupations. Exhibit 6 illustrates these hiring challenges.

Exhibit 6: Difficulty in Hiring for Cybersecurity Occupations



Note that the previous section on labor market information had 10 occupations. For the purpose of the survey, we grouped two similar occupations together (Computer Software Engineers, Applications, and Computer Software Engineers, Software) to make it easier for employers to respond.

Skill Requirements

To understand the primary skill sets needed to perform each of the selected jobs, the COE conducted an in depth analysis of 44 job postings throughout Los Angeles and Orange Counties. A list of the top 15 skills needed to work each occupation was created.

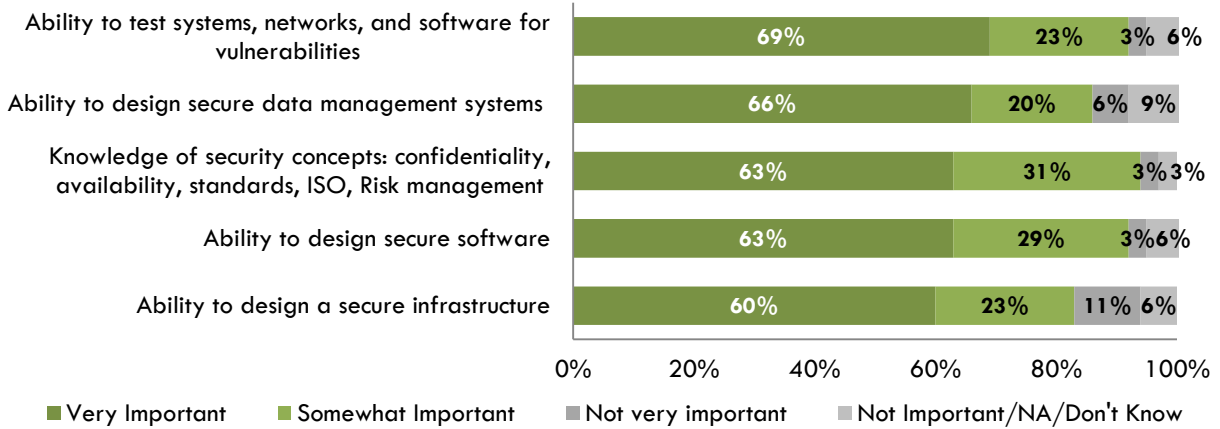
Following the compilation of the skills list, 100 regional employers were asked to validate the importance of each skill needed for a potential job candidate. Following are the top five skills for each occupation and their respective importance for prospective job candidates. For a complete list of the 15 skills identified and their importance see Appendix C.

Cybersecurity programmers

Cybersecurity programmers write programs, work to update, repair, and modify existing programs. Employers reported that:

- The most valued skill for cybersecurity programmer is the ability to test systems, network, and software for vulnerabilities (69% very important).
- Additional very important skills are the ability to: design secure data management systems (66%); design secure software (63%) and infrastructure (63%); and knowledge of security concepts (63%).

Exhibit 7: Cybersecurity Programmers (N=35)

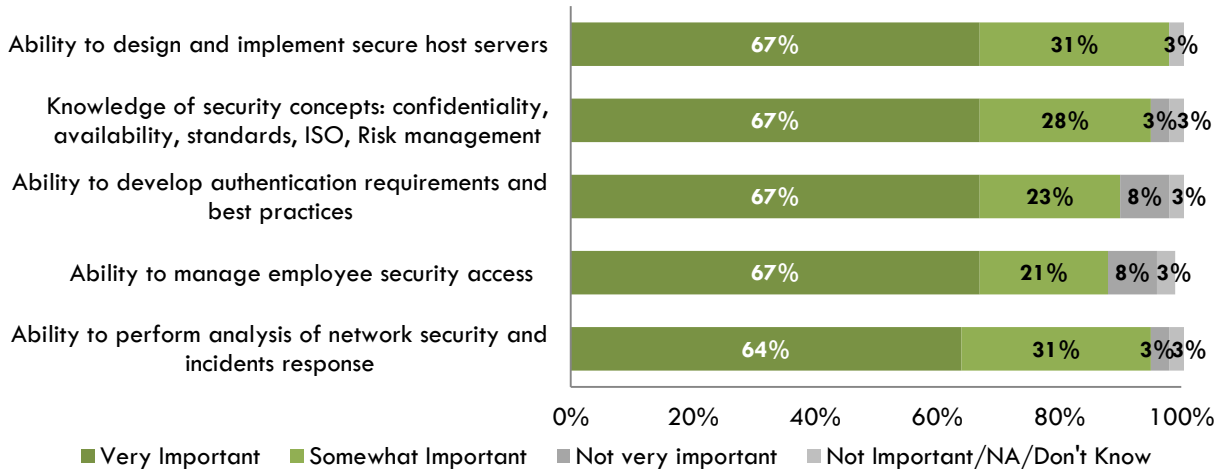


Cybersecurity software engineers

Cybersecurity software engineers develop, enhance, and maintain security software sold to customers and business partners.

- Employers reported that the most valued skills for cybersecurity software engineers is the ability to: design and implement secure host servers; develop authentication requirements and best practices; manage employee security access; and knowledge of security concepts (all 67% very important).
- Employers indicated that an additional very important skill is the ability to perform analysis of network security and incidents response (64%).

Exhibit 8: Cybersecurity Software Engineers (N=39)

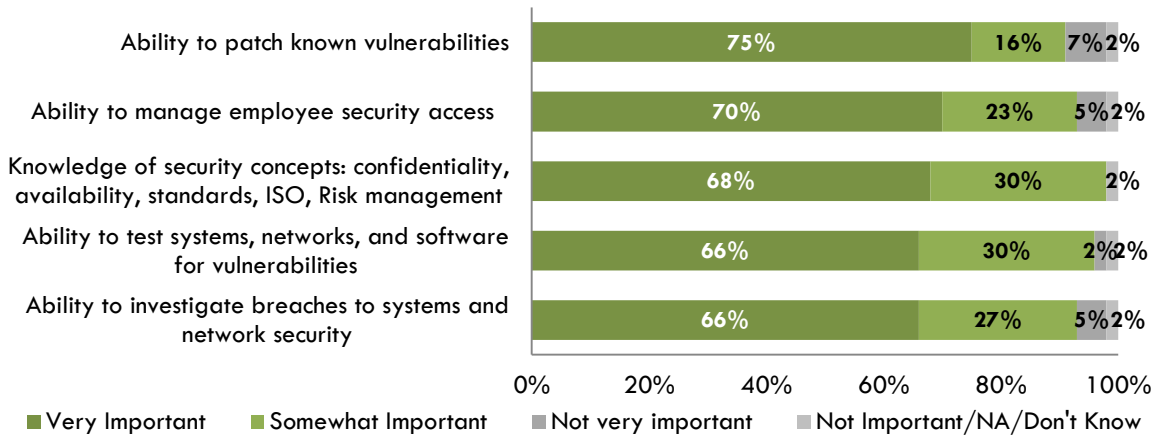


Security support specialists

Security support specialists help customers, business partners, and those within their organizations to safely utilize their computer equipment.

- Employers reported that the most valued skill for security support specialists is the ability to patch known vulnerabilities (75% very important)
- Employers indicated that additional very important skills are: the ability to manage employee security access (70%); knowledge of security concepts (68%); the ability to test systems, network, and software for vulnerabilities (66%); and the ability to investigate breaches to system and network security.

Exhibit 9: Security Support Specialist (N=44)

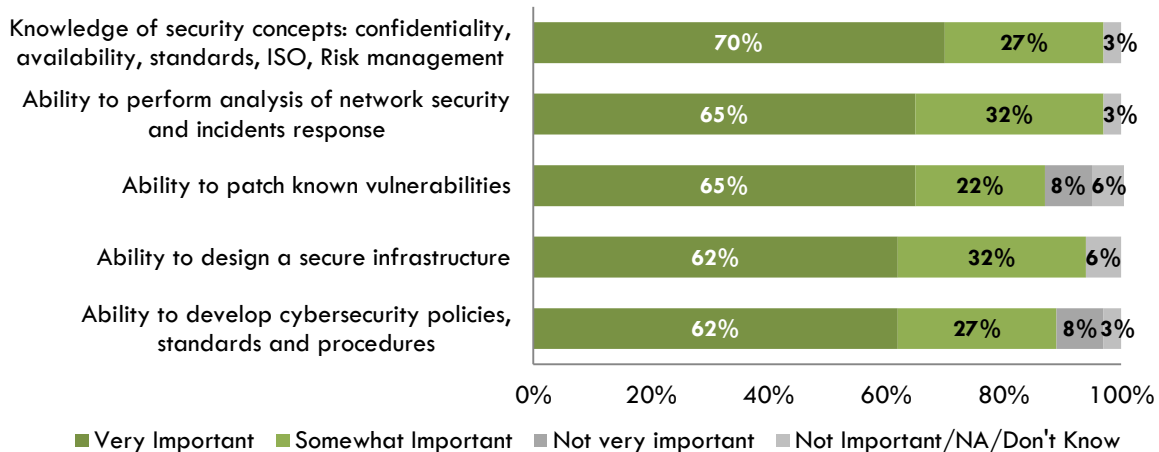


Systems Analysts, Cybersecurity

Security systems analysts investigate security problems and help the user to find solutions. Analysts may perform these tasks for individuals or for the business a whole.

- Employers reported that the most valued skill for cybersecurity systems analysts is knowledge of security concepts (70% very important).
- Employers indicated that additional very important skills are the ability to: perform analysis of network security and incidents response (65%); patch known vulnerabilities (65%); design a secure infrastructure (62%); and develop cybersecurity policies, standards, and procedures (62%).

Exhibit 10: Systems Analysts, Cybersecurity (N=37)

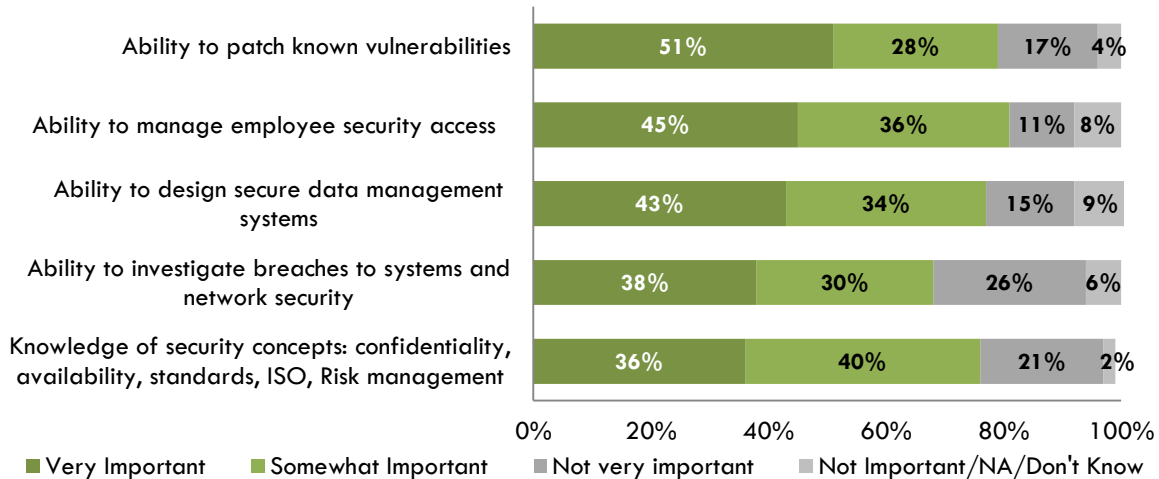


Cybersecurity database administrators

Database administrators of cybersecurity develop ways to store data both safely and effectively. They identify user needs, develop databases, and perform system tests.

- Employers reported that the most valued skill for cybersecurity database administrators is the ability to patch known vulnerabilities (51% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (45%); design secure data management systems (43%); investigate breaches to systems and network security (38%); and knowledge of security concepts (36%).

Exhibit 11: Cybersecurity Database Administrators (N=47)

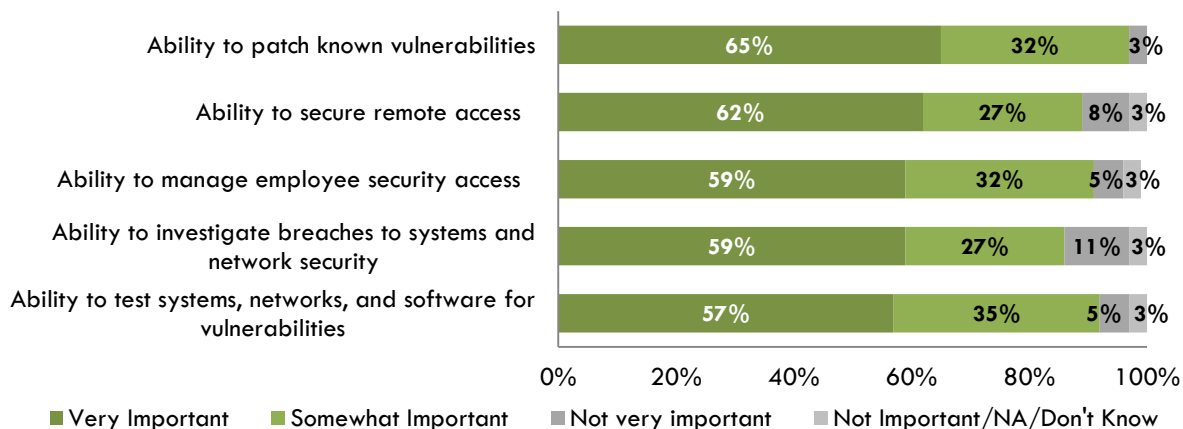


Network and computer systems administrators

Network and computer systems administrators work with businesses to design, install, and support the computer system for the organization.

- Employers reported that the most valued skill for network and computer systems administrators is the ability to patch known vulnerabilities (65%).
- Employers indicated that additional very important skills is the ability to: secure remote access (62%); manage employee security access (59%); investigate breaches to systems and network security (59%); and test systems, network, and software for vulnerabilities (57%).

Exhibit 12: Network and Computer Systems Administrators (N=37)

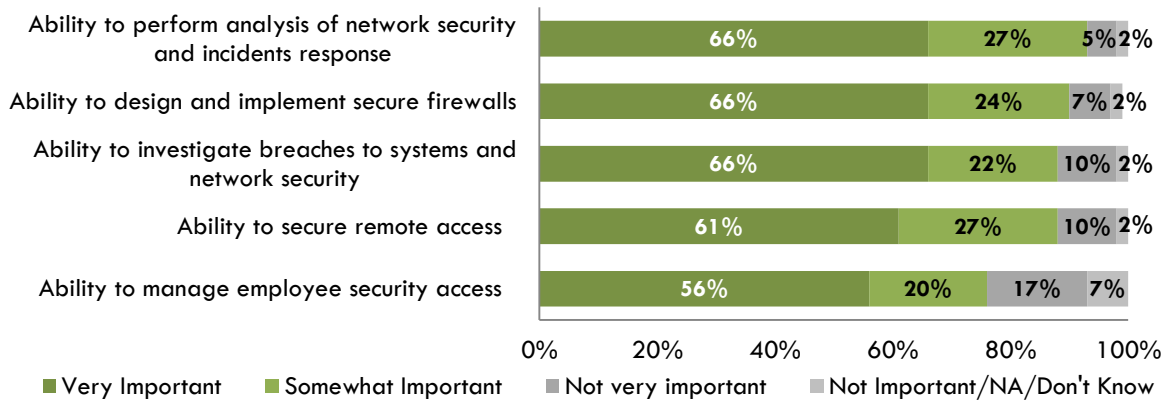


Network systems and data communications analysts

Network systems and data communications analysts work with data communications systems such as local area networks (LAN), wide area networks (WAN), company intranets, internet, etc. They perform tests and recommend improvement to these communications systems.

- Employers reported that the most valued skill for network systems and data communications analysts is the ability to perform analysis of network security and incidents response (66% very important).
- Employers indicated that additional very important skills are the ability to: design and implement secure firewall (66%); investigate breaches in systems and network security (66%); secure remote access (61%); and manage employee security access (56%).

Exhibit 13: Network Systems and Data Communications Analysts (N=41)

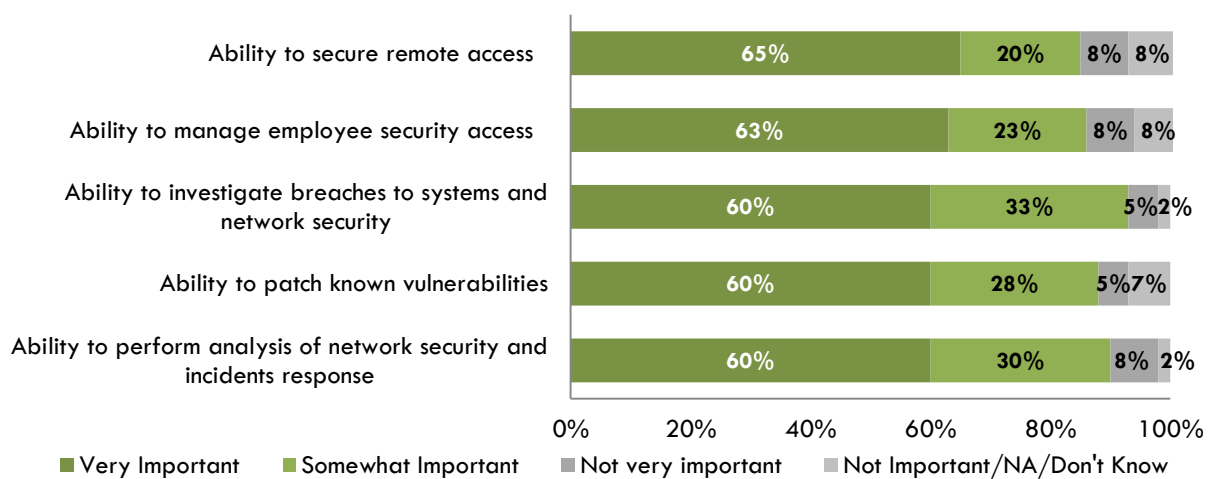


Computer specialists involved in cybersecurity, all other

This term includes all cybersecurity workers not already included in the previous categories.

- Employers reported that the most valued skill for these professional is the ability to secure remote access (65% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (63%); investigate breaches to systems and network security (60%); patch known vulnerabilities (60%); and perform analysis of network security and incidents response (60%).

Exhibit 14: Computer Specialists involved in Cybersecurity, All Other (N=40)

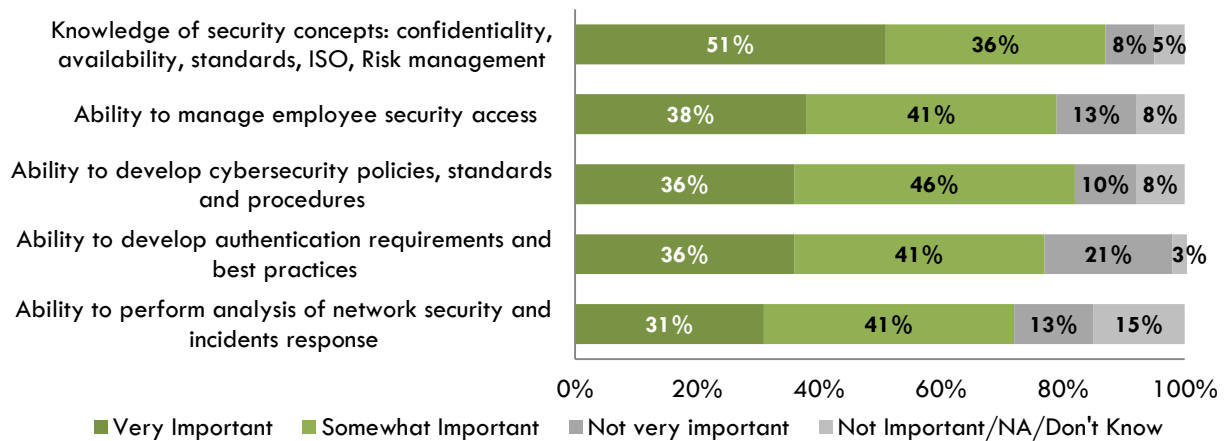


Computer and Information Systems Managers

Computer information systems managers are responsible for researching computer-related use in their organizations. They also oversee use the use and implementation of technology and technical solutions in their organizations.

- Employers reported that the most valued skill for computer information systems managers is the knowledge of security concepts: confidentiality, availability, standards, ISO, risk management (51% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (38%); develop cybersecurity policies, standard, and procedures (36%); develop authentication requirement and best practices (36%); and perform analysis of network security and incidents response (31%).

Exhibit 15: Computer and Information Systems Managers (N=39)

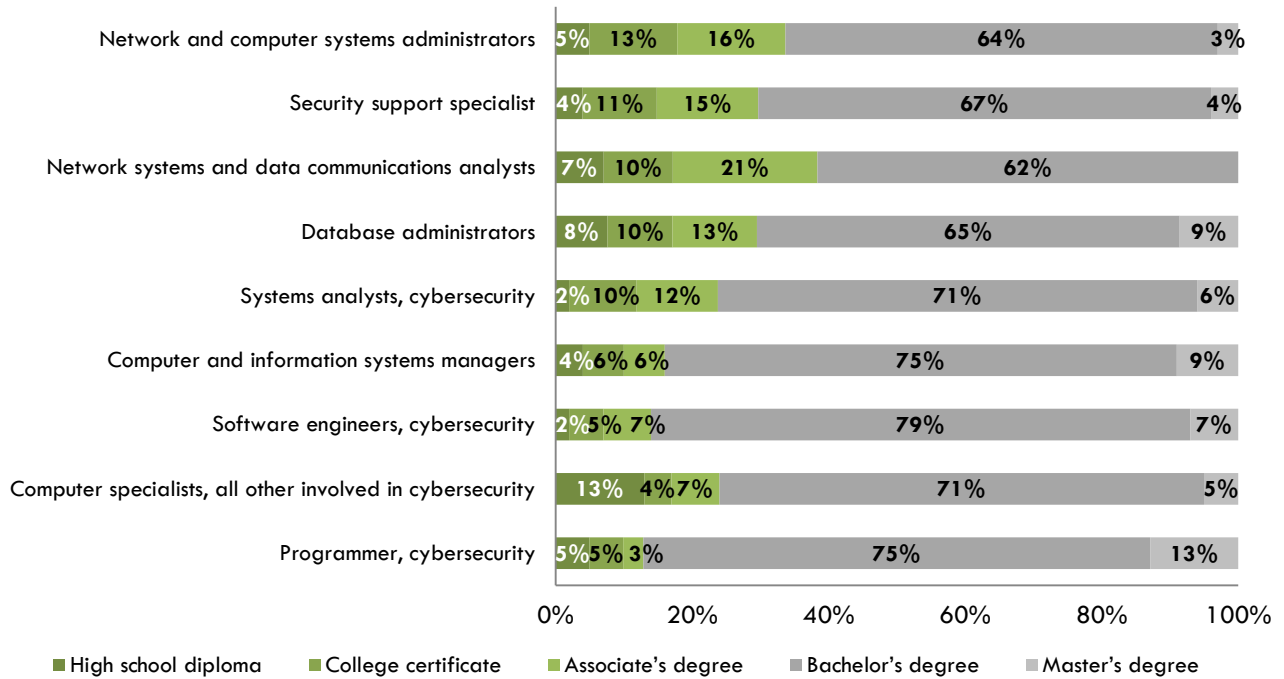


Educational Requirements

Employers surveyed were asked what their educational requirements for cybersecurity job candidates were. Exhibit 16 illustrates the preferred level of education for each occupation.

- For most occupations, employers prefer a Bachelor’s degree.
- However, employers do indicate that there are entry level positions available for individuals with a Certificate or Associate degree:
 - 31% of employers claim to prefer hiring network systems and data communications analysts with an Associate’s degree or Certificate.
 - 29% of employers claim to prefer hiring network systems and computer systems administrators with an Associate’s degree or Certificate.
 - 26% of employers claim to prefer hiring security support specialists with an Associate’s degree or Certificate.
- These results suggest that the Community College can play a critical role in preparing students to:
 - Begin a career in cybersecurity, and/or
 - Transfer into a Bachelor’s degree program.

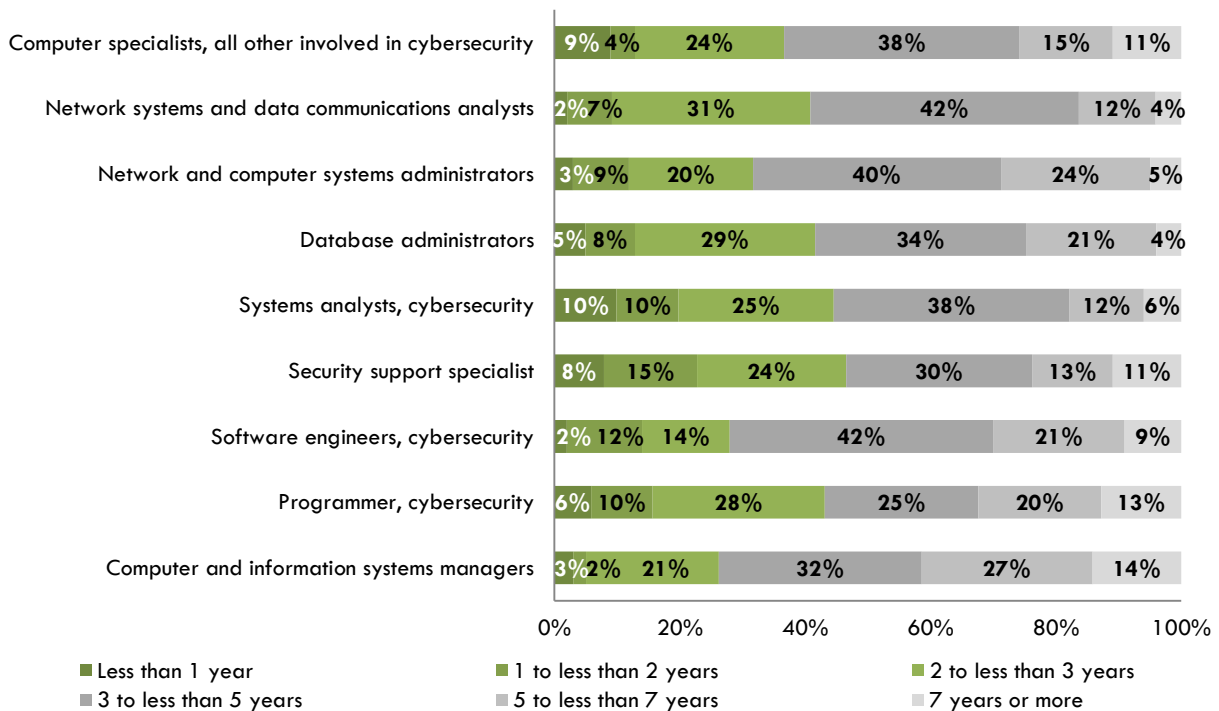
Exhibit 16: Preferred Level of Education for Cybersecurity New Hires



Work Experience Requirement

Employers were also asked their requirements for work experience when hiring for cybersecurity jobs. The majority of employers require at least two years of experience to gain employment. Thus community colleges should strive to build internships opportunities into cybersecurity programs to give students an opportunity to prove themselves and perhaps get hired in an entry-level position, to obtain practical skills and build experience.

Exhibit 17: Preferred Level of Experience When Hiring



Community Support and Resources

Regional colleges that want to address the training needs of cybersecurity professionals have access to the following resources:

Exhibit 18: Cybersecurity Resources

Organization	Services Provided
Center for Security Systems and Information Assurance www.cssia.org	“Advances Cyber Security education programs at the secondary and post-secondary levels by providing innovative teaching and learning opportunities through skills based student competitions and faculty professional development.”
CyberWest Watch cyberwatchwest.org	“Cyberwatch West offers the most current information in Cybersecurity in the form of educational partnerships, business industry partnerships, professional, and student development programs and events.”
DHS Cyber Security R&D Center www.cyber.st.dhs.gov	Partners with public and private sectors to increase valid cybersecurity research.
National Security Agency, Information Assurance www.nsa.gov/ia/ia_at_nsa	Offers training and security awareness support, as well as assessment and solutions for information security.
The Center for a New American Security www.cnas.org	“Develops strong, pragmatic and principled national security and defense policies.”
Cyber Security Forum Initiative www.csfi.us	“Provides Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners.”
International Information Systems Security Certification Consortium, (ISC²) www.isc2.org	A world leader for certifying cybersecurity professionals.
Building a Cybersecurity Pipeline: Call to Serve www.ourpublicservice.org/OPS/programs/calltoserve/schools	A joint effort of the Partnership for Public Service and the Office of Personnel Management dedicated to partnering with college campuses to educate students about careers in the federal government. ²⁶

²⁶ Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica. “Improving our Nation’s Cybersecurity through the Public-Private Partnership: A White Paper.” March, 8, 2011.

College Response

Community Colleges in Los Angeles and Orange Counties

Training and education from the community colleges in Los Angeles and Orange Counties range from individual courses to certificate and Associate degree programs. Exhibit 19 presents a summary of community college offerings. For a detailed list of programs and courses see Appendix D.

Exhibit 19: Regional Security Programs, Certificates, and Courses

College	Degree Program	Certificate or Award	Number of Cybersecurity Courses
Cerritos College		Cyber Security Certification	5 Courses
Citrus College			1 Course
Coastline Community College		Computer Networking Certificate: Concentration in Security	11 Courses
		Network Security Specialist Certificate	17 Courses
Cypress College		Computer Forensics Certificate	6 Courses
El Camino College			1 Course
Fullerton College			2 Courses
Glendale Community College			1 Course
Irvine Valley College			2 Courses
Long Beach Community College		Information Security Certificate	5 Courses
LA City College			1 Course
LA Southwest College			1 Course
LA Trade Tech College			2 Courses
Mt. San Antonio College	A.S. in Computer and Network Security	CIS Professional Certificate in Network Security	7 Courses
		Information and Operating Systems Security Certificate	3 Courses
			3 Courses
Orange Coast College			2 Courses
Pasadena City College			4 Courses
Rio Hondo College			3 Courses
Saddleback College		Information Security: Security Occupational Skills Award	8 Courses
Santa Ana College			1 Course
Santa Monica College			4 Courses
West Los Angeles College	A.S. or A.A. - Computer Network and Security Management	Certificate of Achievement- Computer Network & Security Management	15 Courses
			14 Courses
		Low-Unit Certificate of Achievement in Computer Network & Information System Security	11 Courses

Other Training Providers

Many private training and education providers such as DeVry University, ITT Technical Institute, Westwood College, the United Education Institute, Versitas, or Hands On Technology Transfer, Inc., offer courses in computer technology. However, the cost of attending any of these providers' courses is much higher than community colleges' cost. In addition, it is preferable for students to take courses which can be transferred to four-year universities. Obtaining a more advanced degree will expand students' career opportunities in cybersecurity.

Gap Analysis

In spite of the high number of educational institutions that prepare students for information technology careers, the number of completions remains lower than the number of job openings for every program in the region. Exhibit 20 presents the number of job openings (new jobs and replacement jobs), the number of completion the same year (2010) and the gap, meaning the difference between open positions and students completing corresponding programs. These figures were provided by EMSI, based on completion data reported by educational institutions to IPEDS. Data includes all education institutions (i.e., community colleges, universities, proprietary schools etc.).

Exhibit 20: Gap Analysis per Program in LA/OC

CIP Code	Program Name	Number of Job Openings	Number of Completions	Gap
11.0103	Information Technology	2,155	543	1,612
11.0201	Computer Programming/Programmer, General	260	93	167
11.0501	Computer Systems Analysis/Analyst	1,689	59	1,630
11.0701	Computer Science	1,386	1,159	227
11.0802	Data Modeling/Warehousing and Database Administration	105	10	95
11.0901	Computer Systems Networking and Telecommunications	1,039	503	536
11.1001	System Administration/Administrator	479	32	447
10.1006	Computer Support Specialist	643	9	634
11.9999	Computer and Information Sciences and Support Services, Other	542	47	495

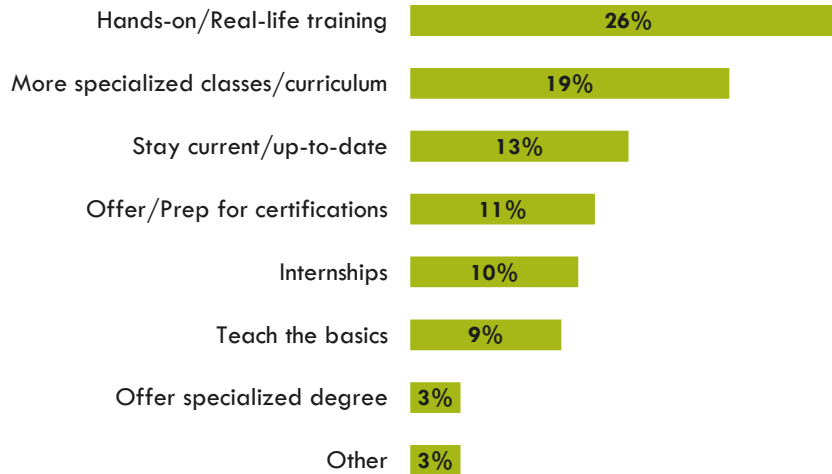
Source: EMSI

Implications and Recommendations for Community Colleges

Employer Suggestions

Respondents to the COE survey were asked to offer recommendations for Community Colleges regarding training the future cybersecurity workforce. Their responses were as follows:

Exhibit 21: Employer Recommendations



Employers emphasized the importance of applying skills directly in the classroom, working on real-life cybersecurity cases, and organizing internships for the students to gain experience. They also recommended adding more classes specific to cybersecurity to information technology programs. They highlighted the importance of staying current in a field that changes extremely rapidly.

Conclusion

Cybersecurity is important not only for business' success, but also for homeland security, and to protect individuals' privacy rights and safety. Firms must be prepared to face new threats that can arise each day, and need the expertise of cybersecurity professionals. There is a shortage of qualified cybersecurity experts in the country, and colleges have to play a key role in preparing a pipeline. Employment projections predict the creation of 12,241 new jobs between 2011 and 2016 (a 7% growth in 5 years). Adding replacement jobs (due to retirement and turnover), the number of job openings may be as high as 26,495 in Los Angeles and Orange Counties.

Cybersecurity jobs are in high demand, continue to grow, and offer high wages as well as career ladders. The number of students completing programs in computer and information science continues to be lower than the number of job openings. The gap is even more problematic for cybersecurity jobs. Employers who responded to our survey reported difficulty for all of the occupations studied. The highest level of difficulty (extreme difficulty) was reported for hiring Programmers, Security Support Specialists and Systems Analysts. Although not the majority, some employers require less than two years of work experience and an Associate degree or certificate, making community college students good candidates for these job opportunities.

Recommendations

Only two community colleges in the Los Angeles-Orange region offer an Associate Degree in Cybersecurity (Mt. San Antonio College and West Los Angeles College). Seven colleges offer Certificates in cybersecurity (see appendix D for details), and twenty have related courses. Given the high demand for cybersecurity professionals, there is an opportunity for more colleges to develop Certificates and Degree Programs in cybersecurity. It is recommended that colleges:

1. Consider adding courses in cybersecurity to their computer and information technology programs.
2. Create new Certificates or Degrees in Cybersecurity.
3. Make sure that their programs and curriculum include the skills listed for cybersecurity occupations in this report (see appendix C for details).
4. Include representation from cybersecurity employers on advisory committees to be aware of new trends keep programs up to date.
5. Contact CyberWatch West,²⁷ a valuable resource for curriculum development, partnership with businesses and services to students.
6. Coordinate with other colleges in the region to avoid duplication of efforts and possible competition.
7. Organize internships and opportunities for their students to gain hands-on experience.

²⁷ CyberWatch West: <http://cyberwatchwest.org/>

References and Resources

- Adhikari, Richard. "Online Trust: A Thing of the Past?" January 28, 2009.
(<http://www.internetnews.com/security/article.php/3799141/Online+Trust+A+Thing+of+the+ast.htm>)
- Barrett, Larry. "Systantec's 'Unlucky 13' Security Trends for 2010." November 20, 2009.
(<http://www.internetnews.com/security/print.php/3849371>)
- Bliss, Jeff. "U.S. Nuclear Plants Vulnerable to Cyber Attacks, Analysts Say," November 17, 2010.
(<http://www.businessweek.com/news/2010-11-17/u-s-nuclear-plants-vulnerable-to-cyber-attacks-analysts-say.html>)
- Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica. "Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper." March, 8, 2011.
(http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf)
- Center for a New American Security. "America's Cyber Future: Security and Prosperity in the Information Age, Volume I." June, 2011.
(http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf)
- Dice. "America's Tech Talent Crunch." May 1, 2011.
(http://marketing.dice.com/pdf/Dice_TechTalentCrunch.pdf)
- Edmunds Community College Digital Forensics and Information Security. (<http://infosec.edcc.edu/>)
- Evans, Karen and Reeder, Franklin. "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters," Center for Strategic and International Studies, November, 2010. (http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf)
- Frost & Sullivan. "The 2011 (ISC)² Global Information Security Workforce Study." March 31, 2011. (https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf)
- Google. "Off-Network Workers – the Weakest Link to Corporate Web Security," 2008 (http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en/security/pdf/off_network_workers.pdf)
- Godbe Research. Computer and Information Security Labor Market Study, June 2006.
- Langton, Lynn & Planty, Michael. "Victim of Identity Theft, 2008." U.S. Department of Justice: *Bureau of Justice Statistics*, December, 2010 (<http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf>).
- Mt. San Antonio Community College Regional Information Systems Security Center.
(http://rissc.mtsac.edu/RISSC_NEW/default.asp)
- Norton. (http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx).
- Obama, President Barack. "Remarks by the President on securing our Nation's cyber infrastructure." May 29, 2009. (<http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>).

- Phillips, Leslie. "Senate Democrats Introduce Bipartisan Legislation Calling For New Safeguards For National Security, American Economy Against Cyber Attack." January 26, 2011. (http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_i=e7362a98-5056-8059-7668-42e3de5aa933) (\$1 trillion in intellectual property stolen)
- Ponemon Institute. "First Annual Cost of Cyber Crime: Bench Mark Study of U.S. Companies." July 2010. (<http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study%281%29.pdf>).
- Senate Committee on Homeland Security and Governmental Affairs. "Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack." January, 26, 2011. (http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf).
- Serrano, Richard A. "U.S. Intelligence Officials Concerned About Cyber Attacks," February 11, 2011. (<http://www.latimes.com/news/nationworld/nation/la-na-intel-hearing-20110211,0,2209934.story>)
- Takanhashi, Dean. "IBM Says it Sees 13 Billion Cybersecurity Alerts Every Day." March 31, 2011. (<http://venturebeat.com/2011/03/31/ibm-says-it-sees-13-billion-cybersecurity-alerts-every-day/>)

Appendix A: How to Utilize this Report

This report is designed to provide current industry data to:

- Define potential strategic opportunities relative to an industry's emerging trends and workforce needs;
- Influence and inform local college program planning and resource development;
- Promote a future-oriented and market responsive way of thinking among stakeholders; and,
- Assist faculty, Economic Development and CTE administrators, and Community and Contract Education programs in connecting with industry partners.

The information in this report has been validated by employers and also includes a listing of what programs are already being offered by colleges to address those workforce needs. In some instances, the labor market information and industry validation will suggest that colleges might not want to begin or add programs, thereby avoiding needless replication and low enrollments.

About the Centers of Excellence

The Centers of Excellence (COE), in partnership with business and industry, deliver regional workforce research customized for community college decision making and resource development. This information has proven valuable to colleges in beginning, revising, or updating economic development and Career Technical Education (CTE) programs, strengthening grant applications, assisting in the accreditation process, and in supporting strategic planning efforts.

The Centers of Excellence Initiative is funded in part by the Chancellor's Office, California Community Colleges, Economic and Workforce Development Program. The total grant amount (grant number 10-305-024 for \$205,000) represents funding for multiple projects and written reports through the Center of Excellence. The Centers aspire to be the premier source of regional economic and workforce information and insight for California's community colleges.

More information about the Centers of Excellence is available at www.coeccc.net.

Important Disclaimer

All representations included in this report have been produced from primary research and/or secondary review of publicly and/or privately available data and/or research reports. Efforts have been made to qualify and validate the accuracy of the data and the reported findings; however, neither the Centers of Excellence, COE host District, nor California Community Colleges Chancellor's Office are responsible for applications or decisions made by recipient community colleges or their representatives based upon components or recommendations contained in this study.

Appendix B: Complete List of Most Common Security Threats

Below is a complete list of Norton's top 11 most commonly occurring security threats:²⁸

Viruses. A virus is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. The danger level and prevalence of viruses are extremely high, and can cause an entire network to crash, resulting in a massive loss of valuable information.

SPAM, SPIM, and SPIT are all forms of junk mail: SPAM via email, SPIM via instant messenger, and SPIT via internet technology. Though their danger level is generally low, they are extremely prevalent and can grant access to sensitive information if opened by the receiver.

Spoofing, phishing, and pharming are all forms of a program, web page, or individual falsification. Spoofing occurs when a person or program is being impersonated; phishing is the replication of a legitimate webpage; and pharming redirects online traffic to a counterfeit website. The danger level of these forms of falsification is high with an extremely high prevalence and they can grant access to sensitive information if the user is not careful.

Spyware refers to software that is installed on a computer without user consent. The danger level and prevalence of spyware is high and can result in the loss of sensitive information, even the changing of computer setting which can lead to system slowing.

Keystroke logging (keylogging) is a software program designed to capture keystrokes (e.g. user input, such as passwords and credit card account information). They are often installed by a Trojan horse or virus. Because they capture sensitive user information their danger level and prevalence are high.

Adware is a form of software that is used to automatically direct a user to an advertisement. Though highly prevalent, it is relatively harmless unless being used as spyware.

Botnets are automated software agents that can create interaction with communities of users in a manner that is personalized to each individual. Because botnets typically run programs such as worms, Trojan horses, and backdoors they are considered to be highly dangerous. They are also highly prevalent.

Worm. Like a virus, a worm is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. Unlike a virus, a worm does not need to attach itself to a program, thus it is extremely dangerous. Worms are highly prevalent.

Trojan horse. A Trojan horse is a piece of software that poses as another piece of software or an application. At first it may function properly, but quickly begins to steal sensitive information and cause system malfunction. Trojans are extremely dangerous, but only moderately prevalent.

Blended threats employ a combination of attacks (e.g. worms, Trojan horses, and viruses sent together) to breach the security of a computer system. They are extremely dangerous, but only moderately prevalent.

Denial-of-service attack (DoS attack). A DoS is an attempt to make resources unavailable to its end user. Because these attacks are often launched through a network of systems they are especially dangerous to large businesses and government, and can be highly dangerous. However, they are not very prevalent.

²⁸ Norton. Found at: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

Appendix C: Complete List of Occupational Skills

Exhibit 21: Computer and Information Systems Managers (N=39)

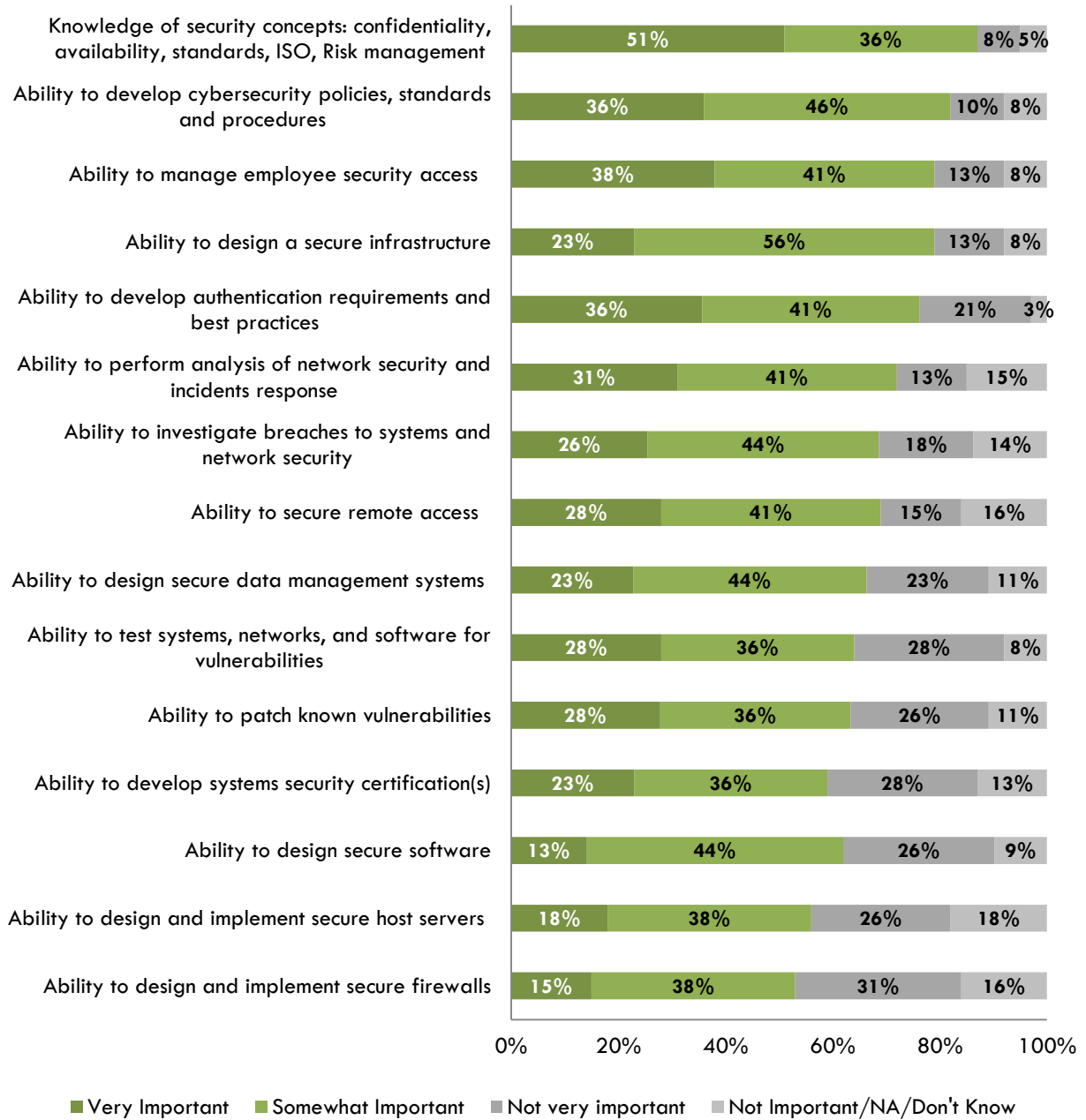


Exhibit 22: Programmer, Cybersecurity (N=35)

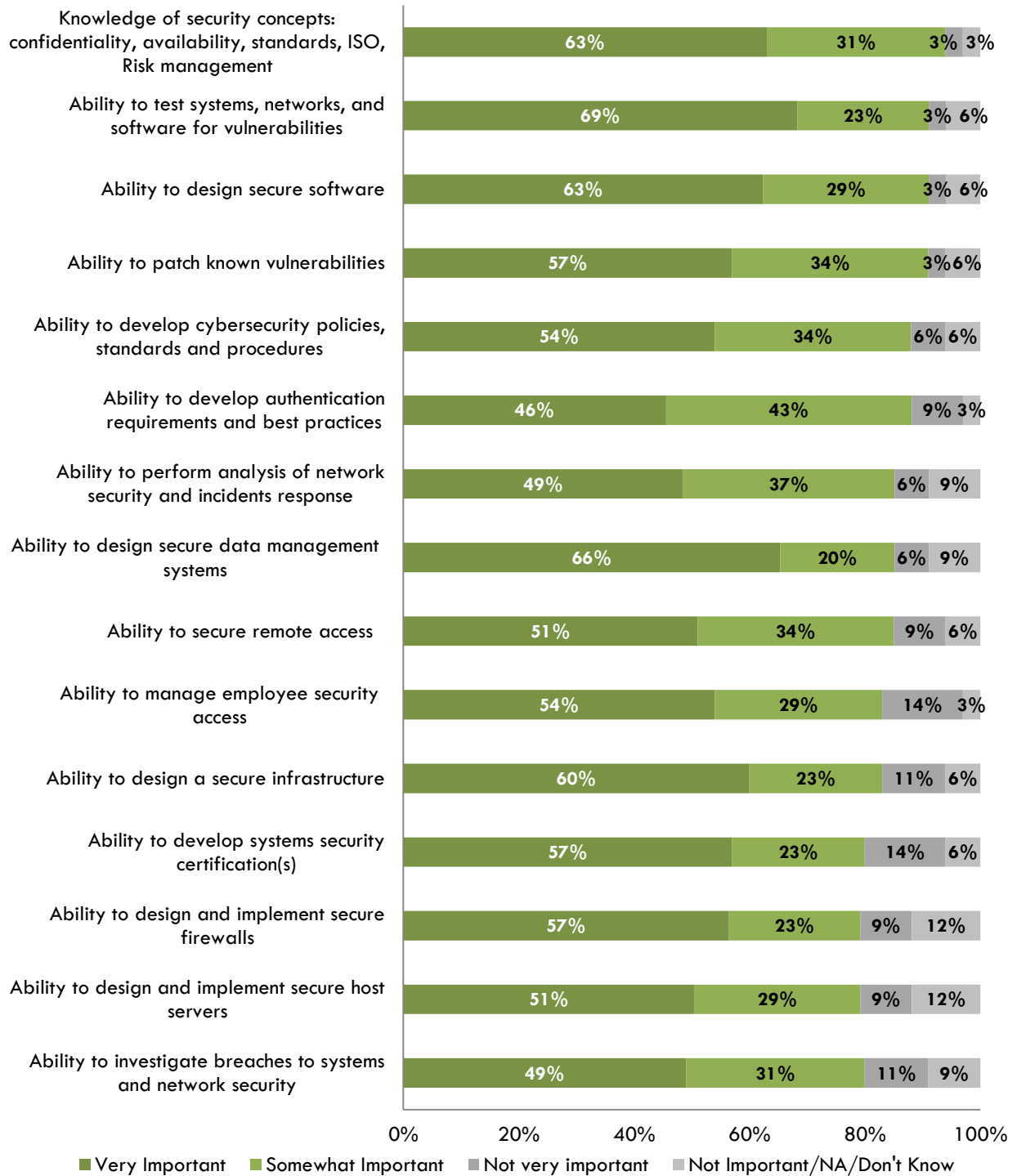


Exhibit 23: Software Engineers, Cybersecurity (N=39)

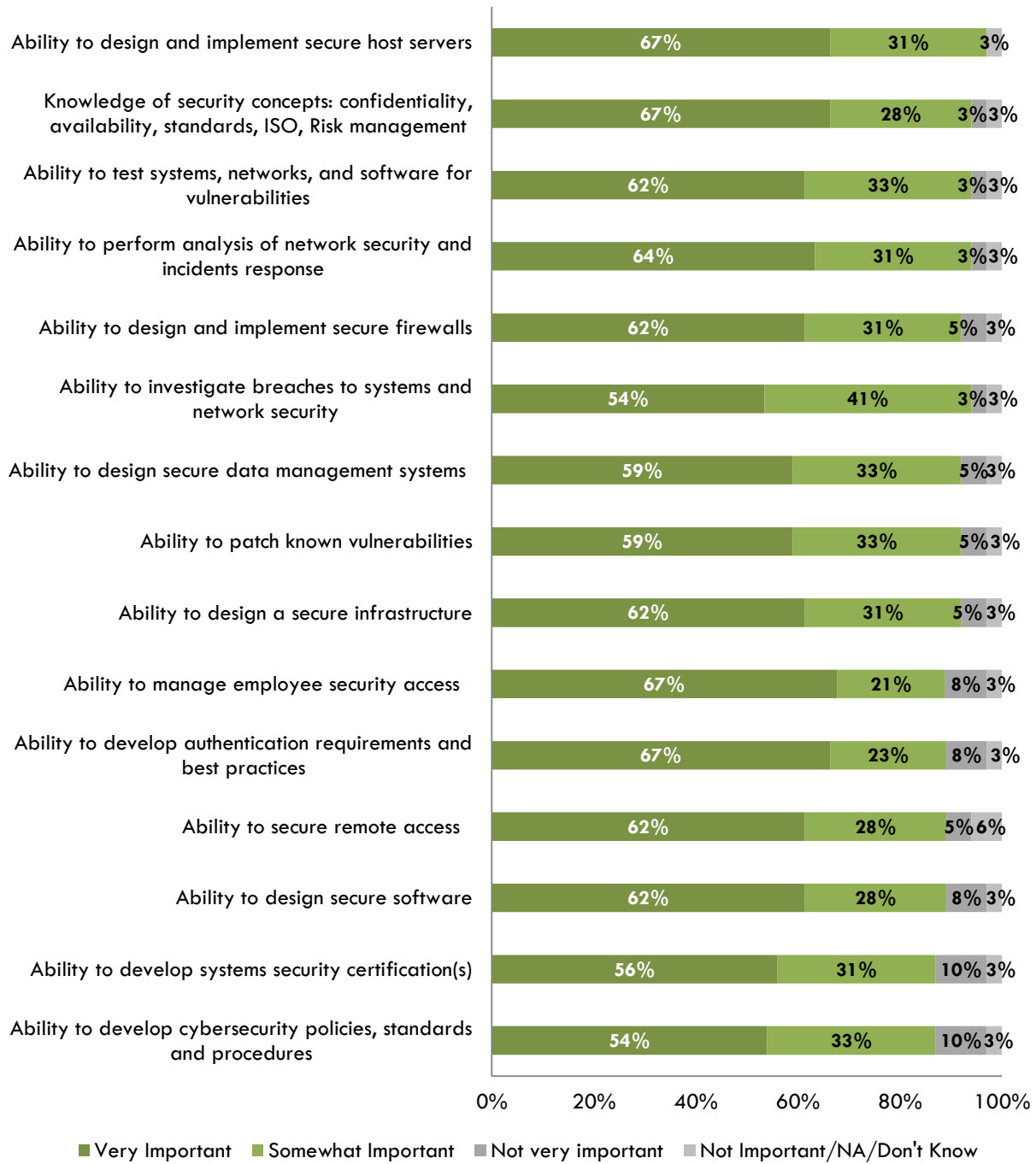


Exhibit 24: Security Support Specialist (N=44)

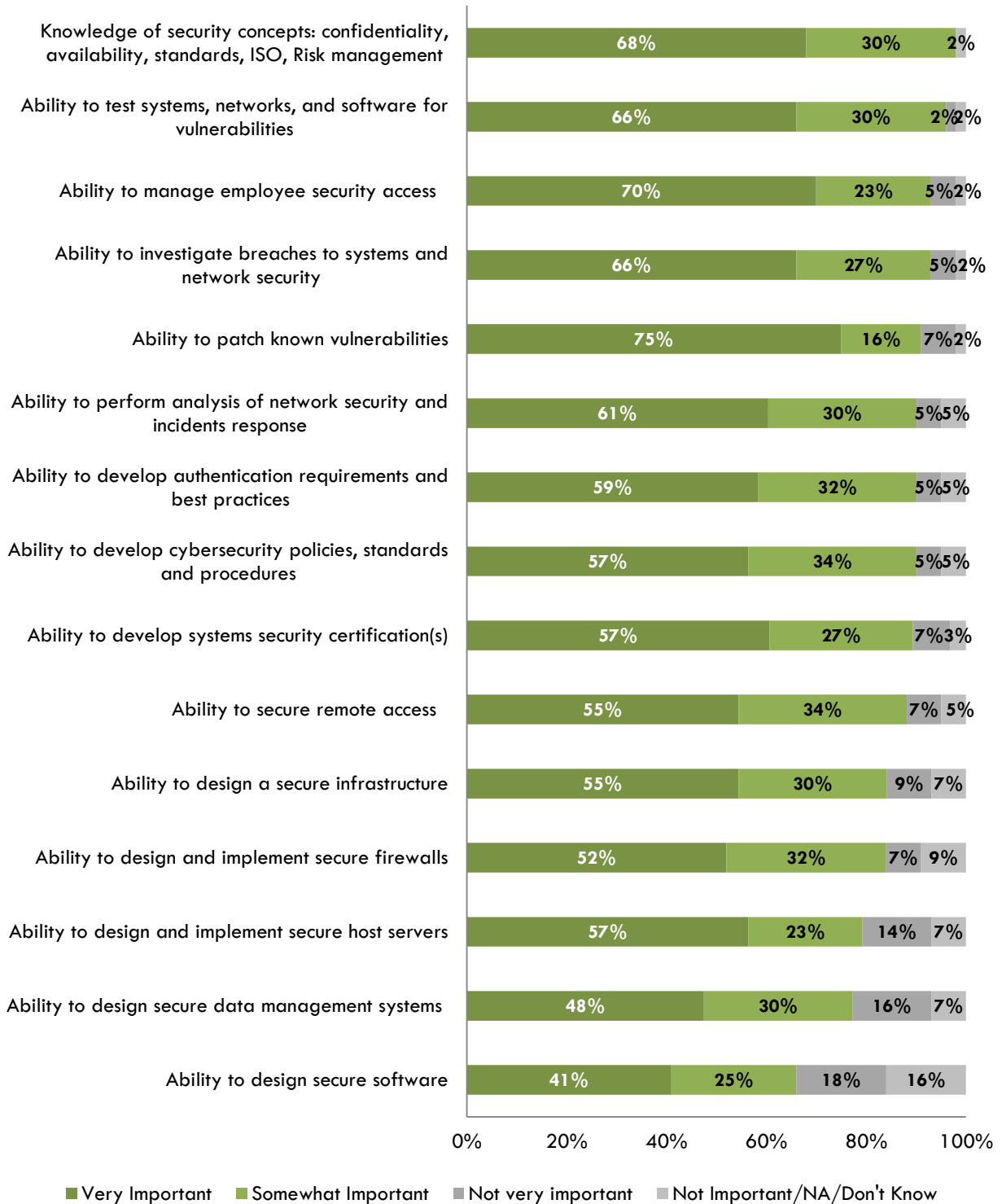


Exhibit 25: Systems Analysts, Cybersecurity (N=37)

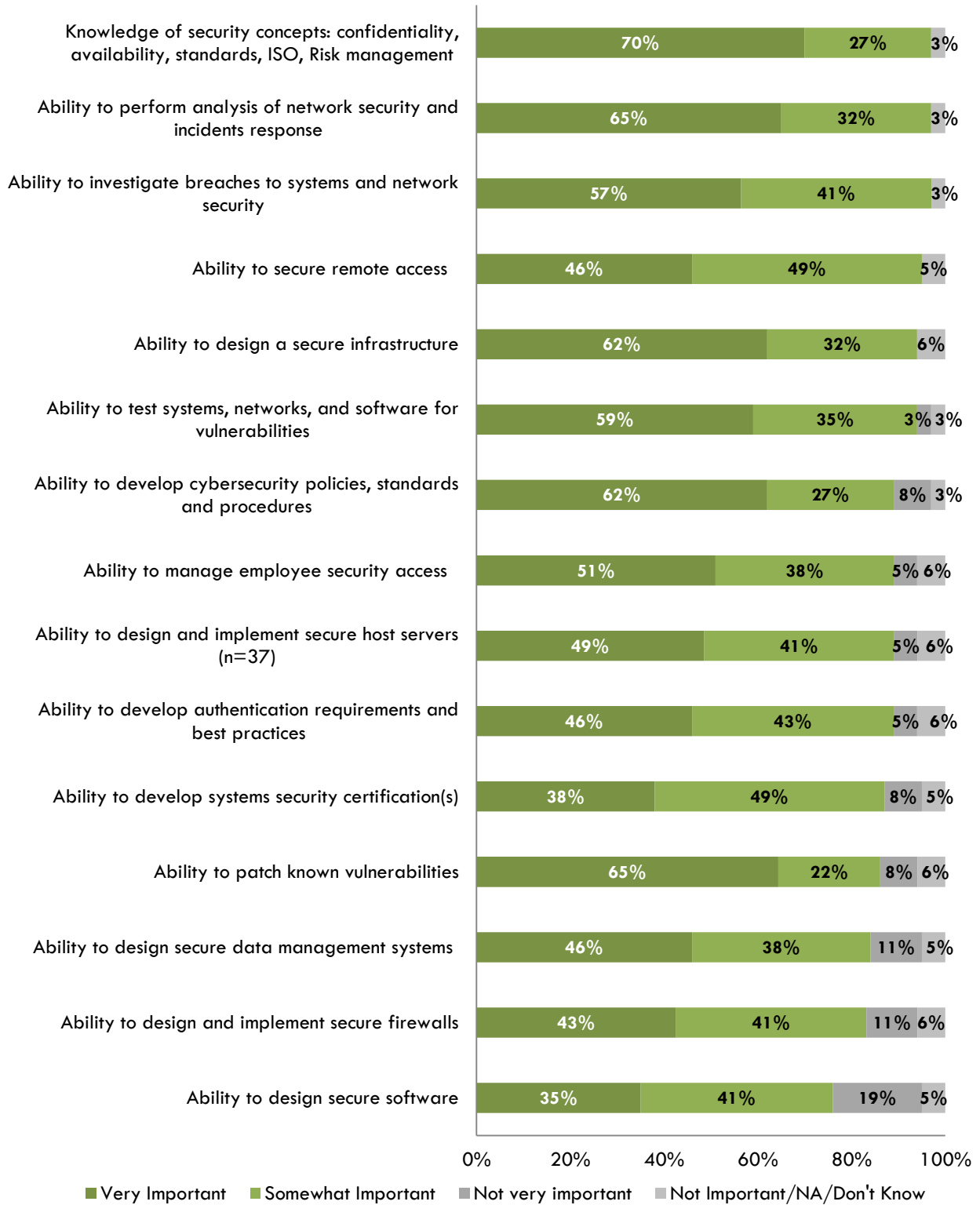


Exhibit 26: Database Administrators (N=47)

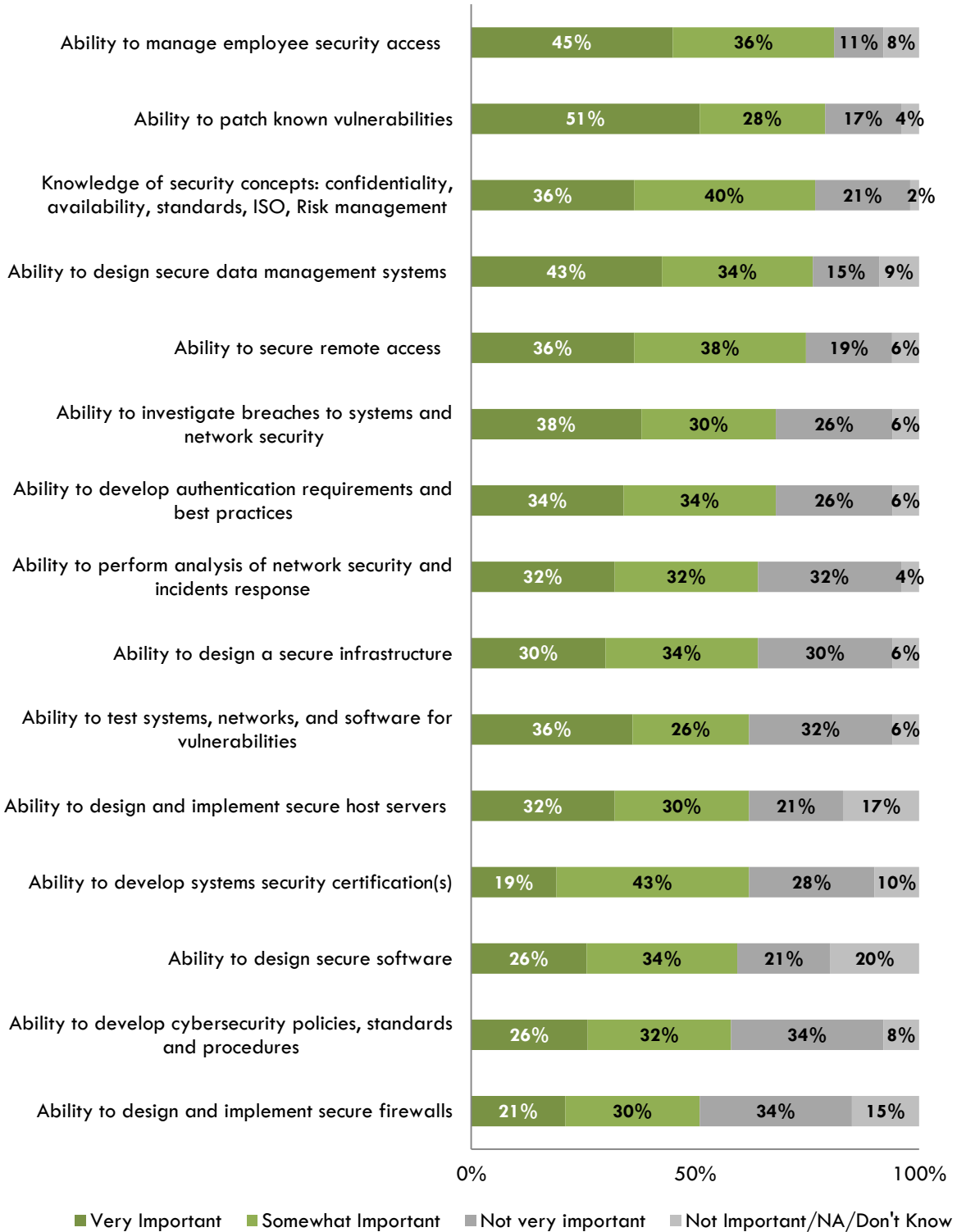


Exhibit 27: Network and Computer Systems Administrators (N=37)

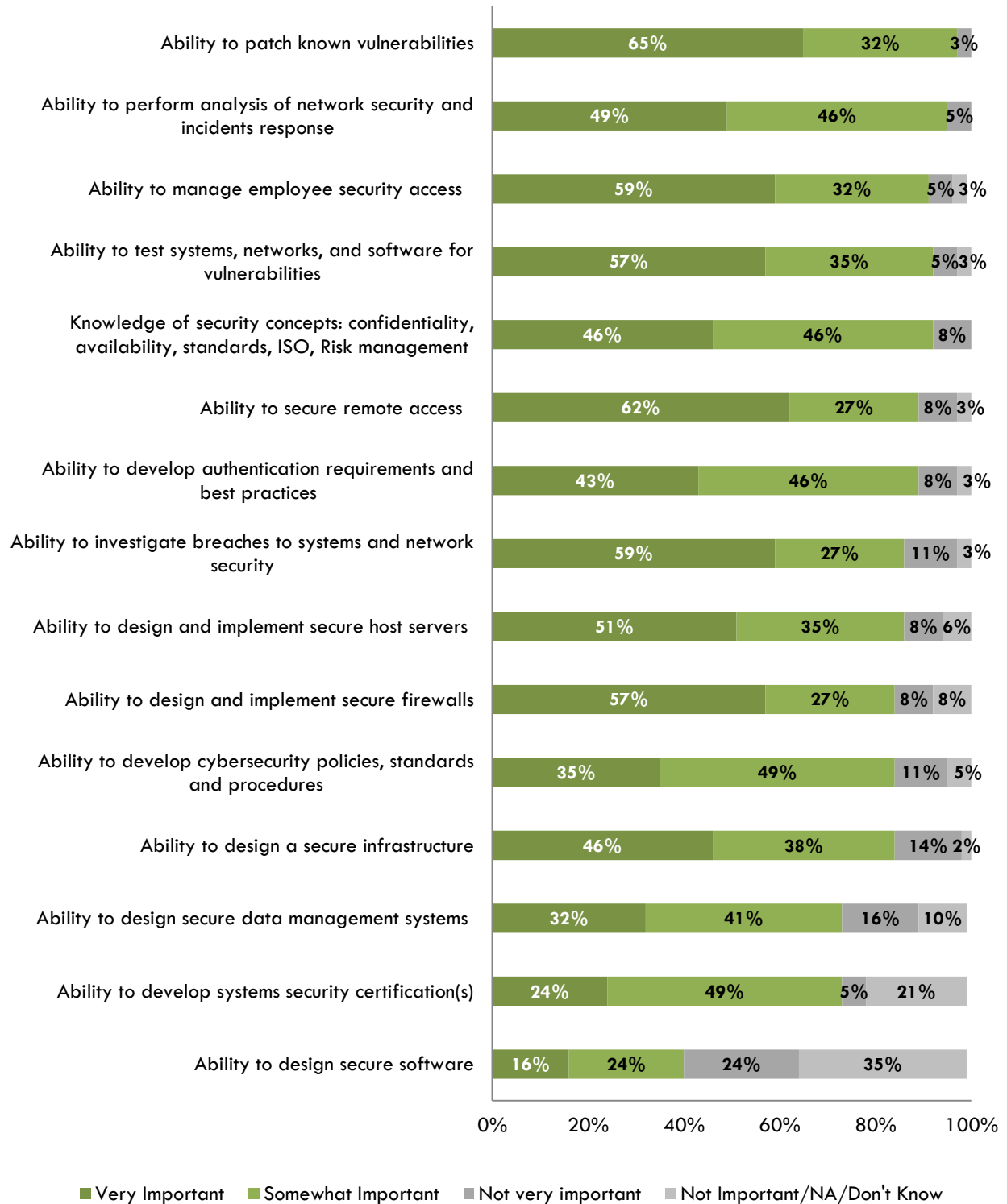


Exhibit 28: Network Systems and Data Communications Analysts (N=41)

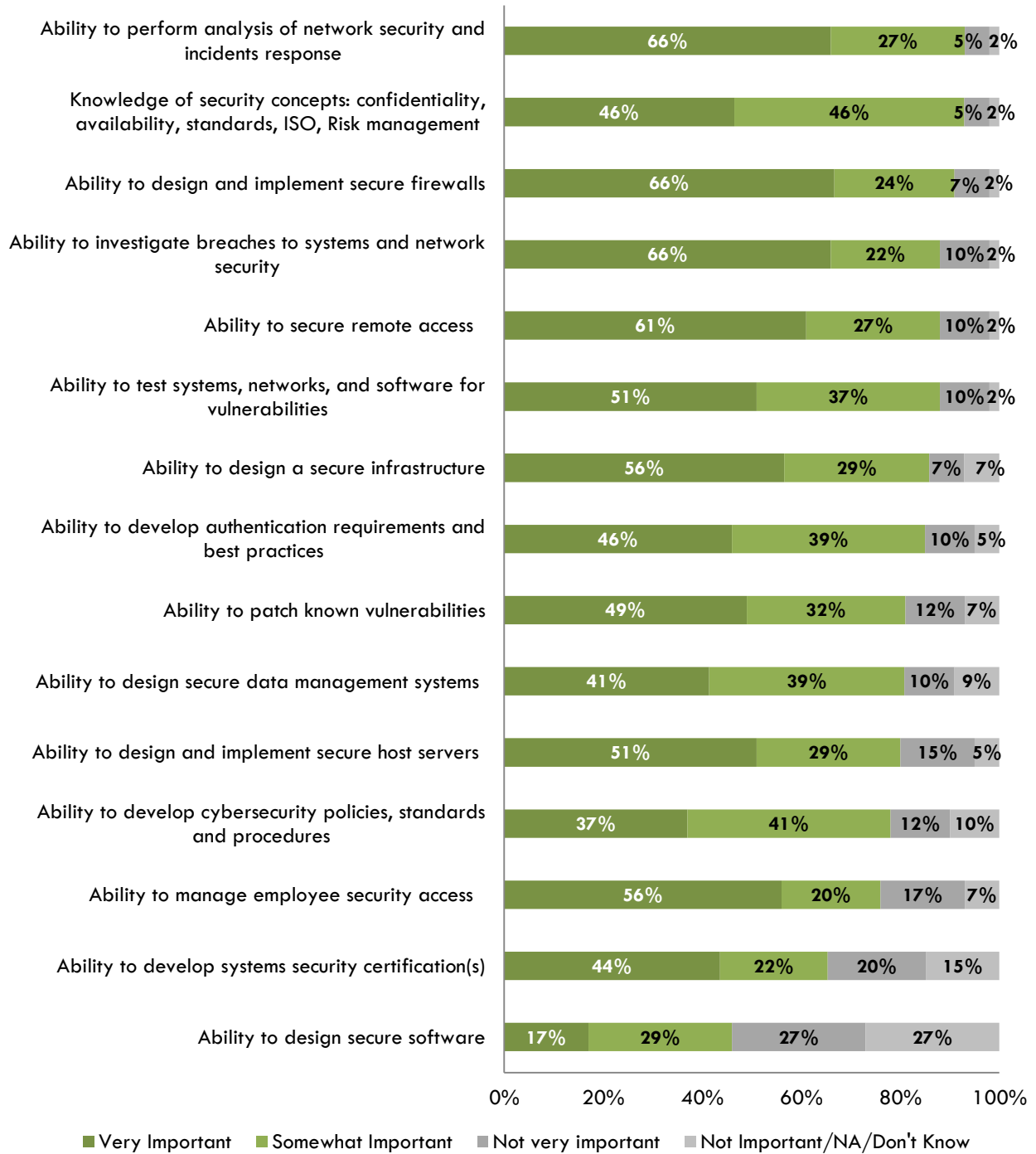
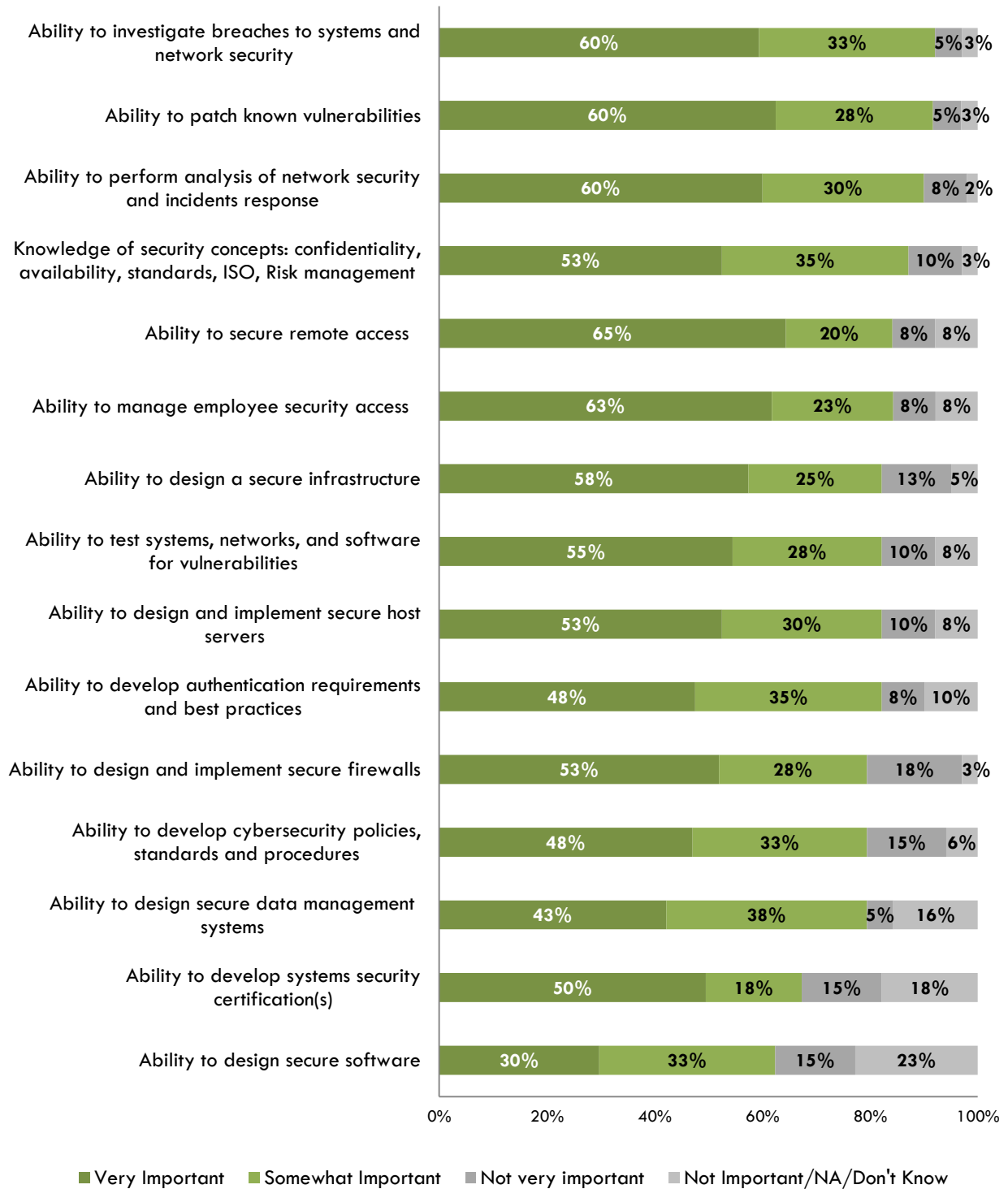


Exhibit 29: Computer Specialists, All Others, involved in Cybersecurity (N=40)



Appendix D: Complete List of Regional Programs and Courses

Cerritos College

Cyber Security Certification, 17 units, 5 classes:

- Network Fundamentals (required)
- Introduction to Wireless Networking (required)
- Network Security Fundamentals (required)
- Special Topics in Security (required)
- Microsoft Windows Security (required)

Citrus College

4 units, 1 class:

- Network and Computer Security

Coastline Community College

Computer Networking Certificate: Concentration in Security, 27 units, 11 classes:

- Security Essentials (required)
- Ethical Hacking (required)
- A + Essentials Hardware (required)
- Network +/Introduction to Networking (required)
- Configuring MS Windows 7 (required)
- CompTIA Linux (required)
- Cisco Fundamentals/CCNA 1 (required)
- Introduction to Geographic Information Systems (elective)
- Certified Wireless Network Administrator (elective)
- Cisco ASA, PIX, and Network Security (elective)
- Linux Networking and Security (elective)

Network Security Certificate, 39 units, 17 classes:

- Security Essentials (required)
- Ethical Hacking (required)
- MS Server 2008: Network Infrastructure (elective)
- Cisco ASA and Network Security (elective)
- Intrusion Detection Systems (elective)
- Firewall and Access Control Lists (elective)
- Computer Forensics (elective)
- Exploring Computer Forensics (elective)
- Certified Wireless Network Administrator (elective)
- Cisco Security Virtual Private Networks (VPNs) (elective)
- Cisco ASA, PIX, and Network Security (elective)
- Cisco IPS/CCSP (elective)
- Linux Networking and Security (elective)
- Advanced Linux Security (elective)
- Certified Information Systems (elective)
- Security Professional (CISSP) (elective)
- Become a Security Consultant (elective)

Cypress College

Computer Forensics Certificate, 18 units, 6 classes:

- Computer Forensics I (required)
- Computer Forensics II (required)
- Cyber Crime (required)
- Comp Forensics Legal Aspects (required)
- Analysis of Digital Media (required)
- Computer Forensics Capstone (required)

15 units, 5 classes:

- Internet Security (ISA) Server
- Network Security
- Anti-Hacking Network Security
- CCNA Security

El Camino College

4 units, 1 class:

- CompTIA Security+ Certification Preparation for Computer Hardware Systems

Fullerton College

5 units, 2 classes:

- Personal Computer Security
- Network Security Fundamentals

Glendale Community College

3 units, 1 class:

- Advanced Networking: Security

Irvine Valley College

5.5 units, 2 classes:

- Fundamentals of Computer Security for Home Users
- Fundamentals of Network Security

Long Beach Community College

Information Security Certificate, 13.5 units, 5 classes:

- Networking Fundamentals (required)
- i-Net+Internet Technologies (required)
- Introduction to Information Security (required)
- Network Security Fundamentals (required)
- LINUX Networking and Security (recommended)

Los Angeles City College

3 units, 1 class:

- UNIX System Security

Los Angeles Southwest College

3 units, 1 class:

- Computer Forensics I

Los Angeles Trade Tech College

6 units, 2 classes:

- Network Security Fundamentals
- Web Security

Mt. San Antonio College

A.S. Degree in Computer and Network Security, 28 units, 7 classes:

- Telecommunication Networking (required)
- Windows Server Network & Security Administration (required)
- Cisco CCNA Networking Fundamentals and Routing (required)
- Network Vulnerabilities and Countermeasures (required)
- Network Analysis and Intrusion Detection Systems (required)
- Network Security and Firewalls (required)
- Linux Networking and Security (required)

CIS Professional Certificate in Network Security, 12 units, 3 courses:

- Network Vulnerabilities and Countermeasures (required)
- Network Analysis and Intrusion Detection Systems (required)
- Network Security and Firewalls (required)

Information and Operating Systems Security Certificate, 10 units, 3 courses

- Practical Computer Security (required)
- Principles of Information Systems Security (required)
- Operating Systems Security (required)

Orange Coast College

7 units, 2 classes:

- Network Security Design
- Ethical Hacking and Network Defense

Pasadena City College

12 units, 4 classes:

- Fundamentals of Network Security
- CCNA Security
- Network Security 1
- Network Security 2

Rio Hondo College

9 units, 3 classes:

- Introduction to Information Security
- Network Security I
- Network Security II

Saddleback College

Information Security: Security Occupational Skills Award, 24 units, 8 classes:

- Information Security Fundamentals (required)
- Network Defense and Countermeasures (required)
- Information Security Management (required)
- Security + (required)

- Cyberlaw (required)
- Network and Security Administration Using UNIX/LINUX
- Advanced Network and Security Administration Using UNIX/LINUX
- Introductory Computer Forensics

Santa Ana College

3 units, 1 class:

- Internet Security

Santa Monica College

12 units, 4 classes:

- Computer Security Concepts
- Secure Server Installation and Administration
- Security in VB.NET Applications
- Security in J2EE Applications

West Los Angeles College

Associate of Arts or Science Degree- Computer Network and Security Management Option,
45 units, 15 classes:

- Operating Systems (required)
- Introduction to Linux+ (required)
- Introduction to Computer Networks (required)
- Introduction to Cisco Network Fundamentals (required)
- Introduction to Cisco Routers (required)
- Introduction to Computer and Information Security I (required)
- Introduction to Microsoft Server Operating System (required)
- Network and Information System Security (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Administering Computer Networks and Security (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)
- Microsoft SQL Server (elective)
- Microsoft Exchange Server (elective)

Certificate Of Achievement - Computer Network & Security Management, 30 units, 14 classes:

- Operating Systems (required)
- Introduction to Linux+ (required)
- Introduction to Computer Networks (required)
- Introduction to Cisco Network Fundamentals (required)
- Introduction to Cisco Routers (required)
- Introduction to Computer and Information Security I (required)
- Introduction to Microsoft Server Operating System (required)
- Network and Information System Security II (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)

- Microsoft Exchange Server (elective)
- Microsoft Exchange Server (elective)

Low-Unit Certificate of Achievement in Computer Network & Information System Security, 16 units, 11 classes:

- Introduction to Computer Networks (required)
- Introduction to Computer and Information Security I (required)
- Network and Information System Security II (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Administering Computer Networks and Security (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)
- Microsoft Exchange Server (elective)
- Installing, Configuring, Administering Microsoft SQL (elective)
- A+ & Network+ Hardware Lab (elective)

Job Market Intelligence: Cybersecurity Jobs, 2015



Introduction: Cybersecurity and the Job Market

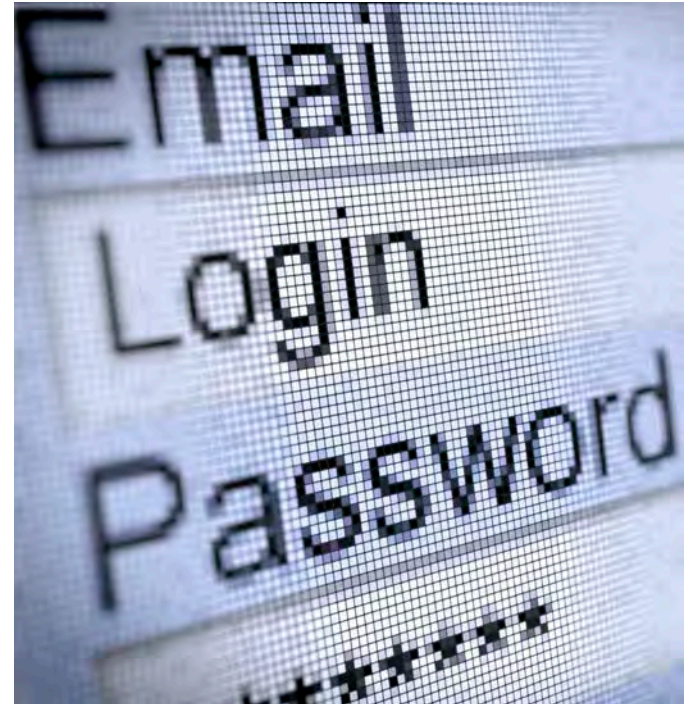
American employers have realized the vital importance of cybersecurity—but that realization has created a near-term shortage of workers that may require long-term solutions.

Cybersecurity was once the province of defense contractors and government agencies, but in this, the third edition of our annual analysis, we find **hiring has boomed in industries like Finance, Health Care, and Retail**. A glance at the headlines is enough to explain why. In addition to the federal Office of Personnel Management, recent cyber breaches have hit major consumer companies like Chase and Target. According to [PwC's 2015 State of US Cybercrime Survey](#), a record 79% of survey respondents said they detected a security incident in the past 12 months. Many incidents go undetected, however, so the real tally is probably much higher.

Yet we are also seeing multiple signs that demand for these workers is outstripping supply. **Job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall** and it takes companies longer to fill cybersecurity positions than other IT jobs. That's bad for employers but good news for **cybersecurity workers, who can command an average salary premium of nearly \$6,500 per year**, or 9% more than other IT workers.

Or put another way, there were nearly 50,000 postings for workers with a CISSP certification in 2014, the primary credential in cybersecurity work. That amounts to three-quarters of all the people who hold that certification in the United States—and presumably most of them already have jobs.

This is a gap that will take time to fill. The skills for some IT positions can be acquired with relatively little training, but cybersecurity isn't one of them. For example, five years of experience are required to even apply for a CISSP certification. That doesn't even consider the rising demand for experience in a specific industry, like finance or health care. This suggests that the shortage of cybersecurity workers is likely to persist, at least until the education and training system catches up.



Key Trends in Cybersecurity Demand

Cybersecurity jobs are in demand and growing across the economy

- The Professional Services, Finance, and Manufacturing/Defense sectors have the highest demand for cybersecurity jobs.
- The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%).

Positions calling for financial skills or a security clearance are even harder to fill than other cybersecurity jobs

- The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of these “hybrid jobs.”
- More than 10% of cybersecurity job postings advertise a security clearance requirement. These jobs, on average, take 10% longer to fill than cybersecurity jobs without a security clearance.

Cybersecurity positions are more likely to require certifications than other IT jobs

- One third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall.

Cybersecurity employers demand a highly educated, highly experienced workforce

- Some 84% of cybersecurity postings specify at least a bachelor’s degree, and 83% require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved through short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

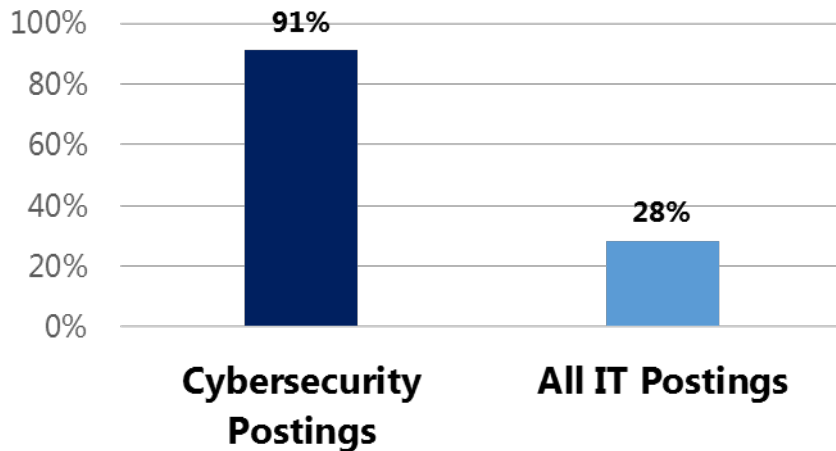
Geographically, cybersecurity jobs are concentrated in government and defense hubs, but are growing most quickly in secondary markets

- On a per capita basis, the leading states are Washington D.C., Virginia, Maryland, and Colorado; all have high concentrations of jobs in the federal government and related contractors.

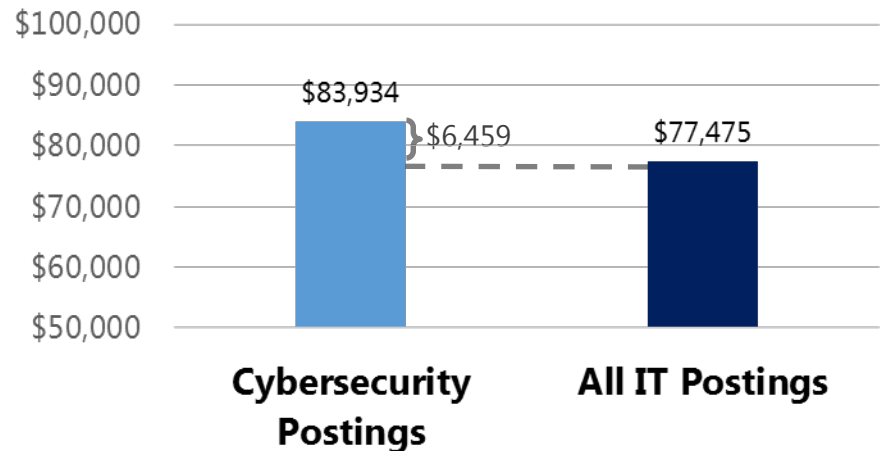
By the Numbers: The Cybersecurity Job Market

- In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for 11% of all IT jobs.**
- Cybersecurity postings have **grown 91%** from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took **8% longer to fill than IT job postings overall.**
- The demand for certificated cybersecurity talent is outstripping supply. In the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.*

Growth in Job Postings (2010-2014)











Cybersecurity Salary Premium



*According to the International Information System Security Certification Consortium, Inc., (ISC)²® membership counts as of July 14, 2015

Cybersecurity Demand Grows in Finance, Professional Services








- **Professional Services, Finance, and Manufacturing & Defense are the leading sectors** for cybersecurity professionals.
- Sectors managing increasing volumes of consumer data such as **Finance, Health Care, and Retail Trade have the fastest increases in demand** for cybersecurity workers.
- Within these sectors, demand for cybersecurity professionals is growing rapidly in more specific industry subsectors not typically associated with cybersecurity, including Air Transportation (+221%) and Accommodation (+157%).

Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765 	57%
Finance and Insurance	13%	17,873 	131%
Manufacturing & Defense*	12%	15,968 	57%
Public Administration	7%	9,725 	N/A**
Information	6%	8,522 	65%
Health Care and Social Assistance	6%	7,915 	118%
Retail Trade	3%	3,505 	120%
Other	15%	19,983 	N/A**

*The Manufacturing Sector includes services divisions of a number of defense contractors (e.g. Raytheon) and computer manufacturers (e.g. Hewlett Packard).
 ** Industry growth rates are suppressed for the Public Administration and Other industry sectors because a significant portion of labor market demand in these industries exists offline.

Engineers, Managers, and Analysts Dominate the Field

The cybersecurity workforce covers a range of job types and skills. This includes advanced Engineer and Architect roles, Auditors (which are concentrated in Finance) and Specialists, which typically have lower entry level requirements.

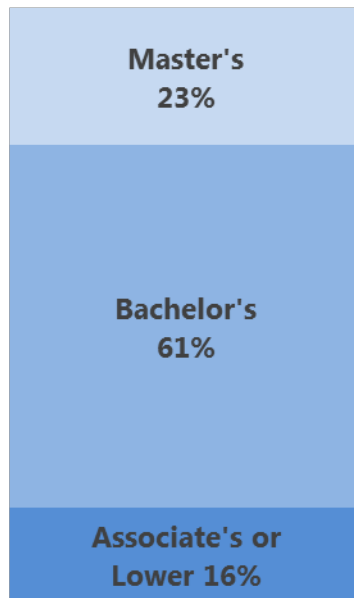
Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355 
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586 
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853 
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289 
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409 
Auditor (e.g. IT Auditor)	5%	7,533 
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294 

Employers Demand More Education, Experience

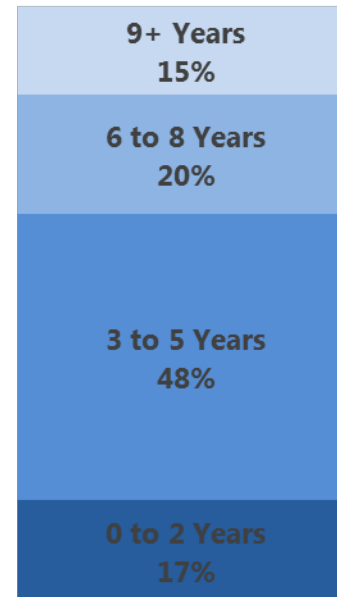
Cybersecurity jobs require significant education and experience. Some 84% of cybersecurity postings specify at least a bachelor's degree, and just as many (83%) require at least 3 years of experience, with an average of 5.4 years.

High education and experience requirements make skills gaps hard to close. Because cybersecurity jobs require years of training and relevant experience, skills gaps cannot easily be resolved through short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

Requested Education Level*



Minimum Experience



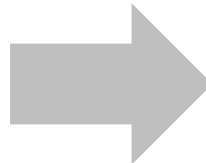
Certification Shapes the Path to Advancement

The cybersecurity job market is shaped by certifications, and job seekers of all experience levels can improve their employment opportunities by obtaining the relevant credentials. Entry-level workers, for example, can obtain foundational certifications such as Security+, which represents an entry point into the field and is by far the largest cybersecurity certification in terms of total holders. Experienced workers can target more advanced certifications such as CISSP, which requires holders to pass a rigorous exam and possess at least five years of information security experience – common requirements among advanced certifications.

Entry-Level Certifications

Typically require less than 3 years of experience

- Security+
- GIAC Security Essentials (GSEC)
- Certified Information Privacy Professional (CIPP)
- Systems Security Certified Practitioner (SSCP)



Advanced Certifications

Typically require at least 3-5 years of experience










- Certified Information Systems Security Professional (CISSP)*
- Certified Information Systems Auditor (CISA)*
- Certified Information Security Manager (CISM)*
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)

*Requires a minimum of 5 years of information security experience.

Certification is More Common in Cybersecurity Jobs

Cybersecurity jobs are highly certificated: More than one in three (35%) of all cybersecurity positions request at least one of the certifications listed below. Only 23% of overall advertised IT jobs request an industry certification.

Certification increases salary: Security+ represents the entry-level certification for cybersecurity roles, and postings requesting it advertise an average salary of \$75,484. This serves as a baseline salary for certified cybersecurity workers, and as workers obtain additional certification they can qualify for ever greater salaries. Postings requesting CISSP, for example, advertised an average salary of \$93,010 – a premium of \$17,526 over the average salary for Security+.

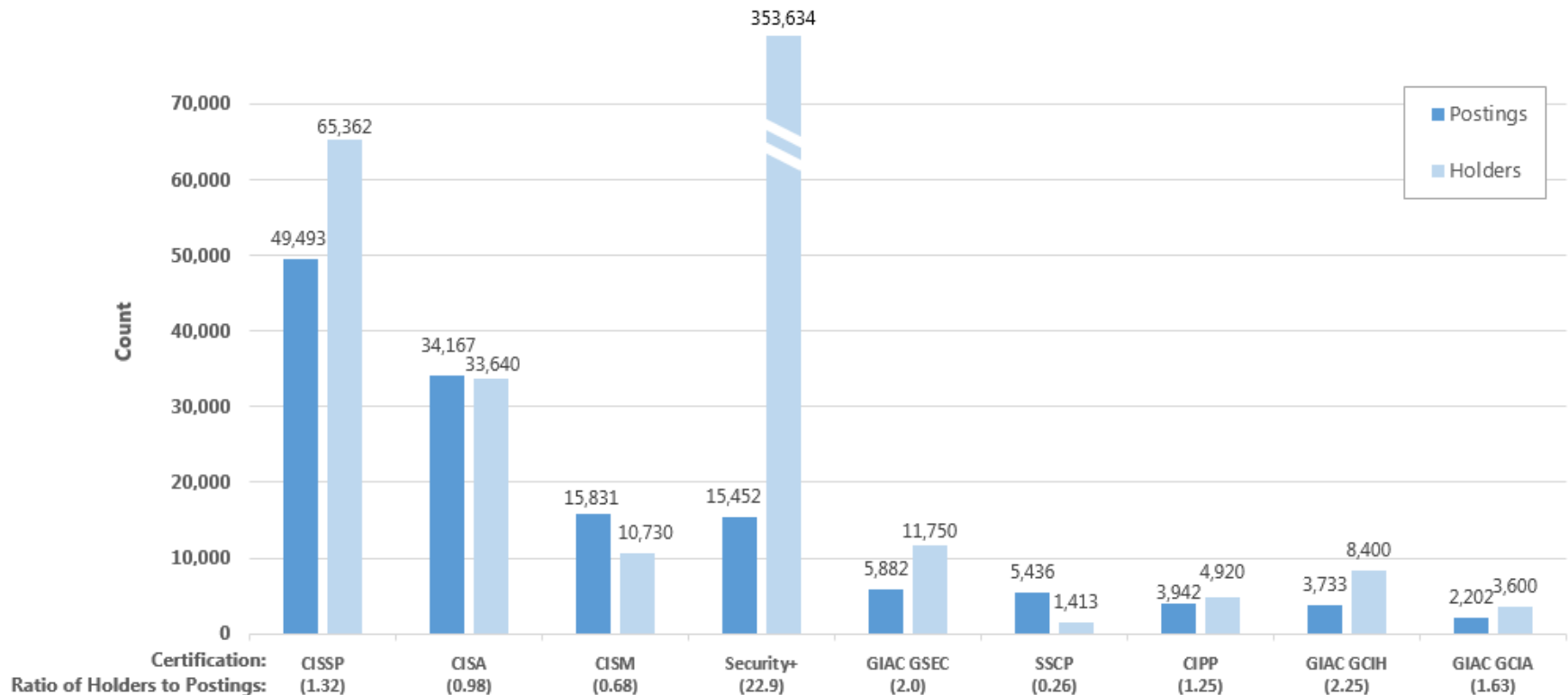
Certification*	% of All Cybersecurity Postings	Number of Cybersecurity Postings (2014)	Average Salary with Certification	Premium Over Security+ Average Salary
CISSP Certified Information Security Professional	21%	49,493 	\$93,010	\$17,526
CISA Certified Information Systems Auditor	14%	34,167 	\$86,238	\$10,754
CISM Certified Information Security Manager	7%	15,831 	\$95,450	\$19,966
Security+ Systems Security Certified Practitioner	6%	15,452 	\$75,484	\$0
GIAC GSEC GIAC Security Essentials	2%	5,882 	\$81,631	\$6,147
SSCP Systems Security Certified Practitioner	2%	5,436 	\$80,718	\$5,234
CIPP Certified Information Privacy Professional	2%	3,942 	\$90,550	\$15,066
GIAC GCIH GIAC Certified Incident Handler	2%	3,733 	\$92,759	\$17,275
GIAC GCIA GIAC Certified Intrusion Analyst	1%	2,202 	\$84,392	\$8,908

*Certification Requirements are not mutually exclusive

Certifications: Too Many Openings Chasing Too Few Workers

Employers prefer workers with cybersecurity certifications, but there can be three or more postings for every certificate holder. When you consider that most of these certificate holders are already employed, the situation looks even better for workers. Even the generous supply of Security + holders is somewhat misleading. Security + is an entry level certificate, so many people with more advanced credentials have one, and the openings that require it are relatively low-level.

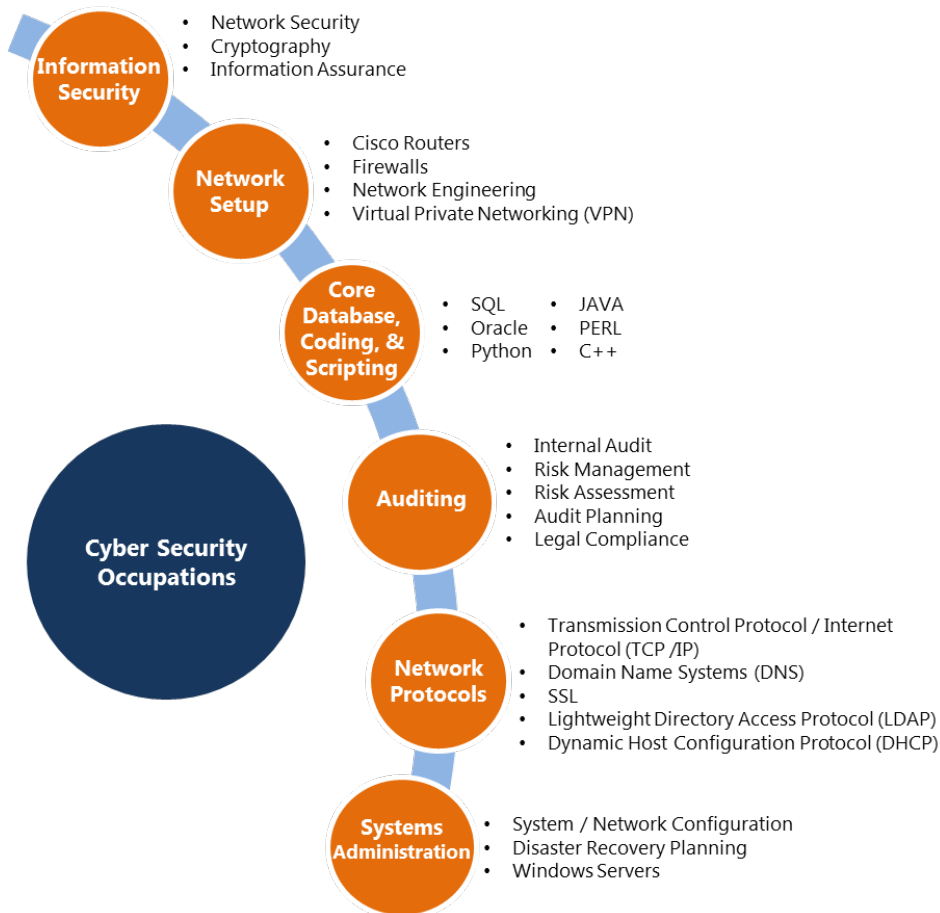
Certification Postings and Holders



Note: Different certifying organizations report slightly different counts of holders. For example, some may report total certifications awarded, while others may report only active certification holders.

Cybersecurity Workers Need to Know IT and Their Industry

The graphic below describes the expertise required for various cybersecurity roles in demand. On top of those skills, job postings often call for additional knowledge in certain information-sensitive industries, such as Health Care; Finance; and Manufacturing and Defense.



Additional Skill and Domain Knowledge Requirements by Industry

Health Care:

Skills:

- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:

- HIPAA
- HITECH
- Payment Card Industry Data Security Standard (PCI DSS)

Finance & Accounting:

Skills:

- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

Manufacturing & Defense:

Compliance & Standards

- JAFAN 6/9 & 6/3, DCID 6/3 and DIACAP
- NERC Reliability Standards

Hybrid Jobs Combining Different Skills are Hardest to Fill

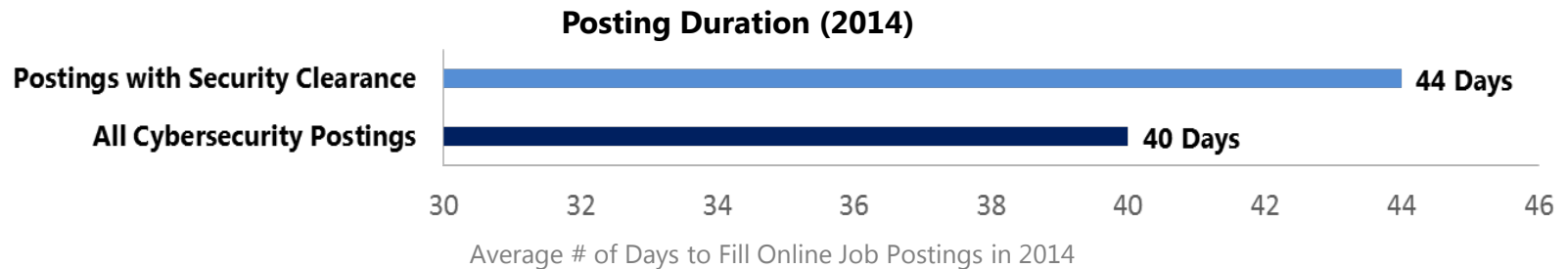
Employers often struggle to fill positions with specialized skill requirements. The fastest-growing skills include industry knowledge areas, such as HIPAA requirements in Health Care and Risk Management, and Accounting in Finance. The hardest-to-fill skills are typically related to finance, such as Information Assurance, Sarbanes-Oxley, and Accounting. **Finding candidates with these unique skill sets can take roughly 17% longer to fill on average than other cybersecurity job openings.**

The difficulties in filling jobs that require a combination of IT security and financial skills reflects a broader trend in the market: hybrid jobs which combine skill sets that are not traditionally trained for together. This often results in skills gaps where employers struggle to find employees that meet these skill needs.

Fastest-Growing Skills in Cybersecurity Job Postings	Five-Year Growth	Hardest to Fill Skills in Cybersecurity Job Postings	Posting Duration	Time to Fill Above Average
Python	309%	Management Information Systems	50 days	+10 days
HIPAA	248%	Information Assurance	47 days	+7 days
Risk Management	209%	Sarbanes-Oxley	47 days	+7 days
Internal Auditing	200%	Accounting	45 days	+5 days
Audit Planning	170%	Python	45 days	+5 days
Risk Assessment	169%	Dynamic Host Configuration Protocol (DHCP)	45 days	+5 days
ITIL	153%	Configuration Management	44 days	+4 days
Management Information Systems	132%	C++	44 days	+4 days
Accounting	121%	Public Accounting	43 days	+3 days
Configuration Management	106%	Internal Auditing	43 days	+3 days

Roles Requiring Security Clearance Take Longer to Fill

Workers with a security clearance—or the ability to get one—have an advantage. In 2014, there were 25,654 cybersecurity postings calling for a government Security Clearance to access classified information, representing 11% of all cybersecurity postings. On average, cybersecurity postings requesting Security Clearance remained open 10% longer than cybersecurity postings overall.



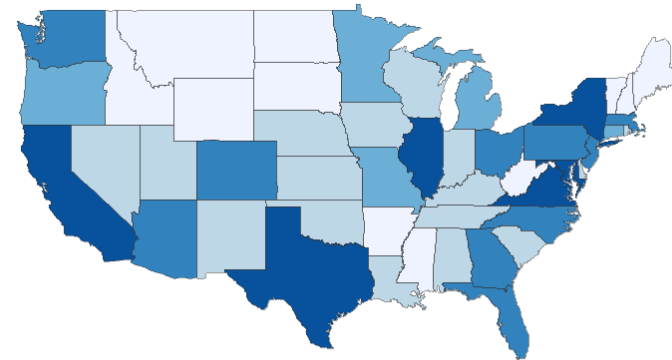
Industry Sector	Percentage of Industry Postings Requesting Security Clearance	Cybersecurity Postings Requesting Security Clearance (2014)
Public Administration	29%	2,793
Manufacturing & Defense*	19%	4,146
Professional Services	18%	10,317
Transportation and Warehousing	7%	107
Information	4%	471
Educational Services	4%	281
Finance and Insurance	2%	499
Healthcare and Social Assistance	1%	128

Cybersecurity Job Postings by State

Top States by Total Postings*

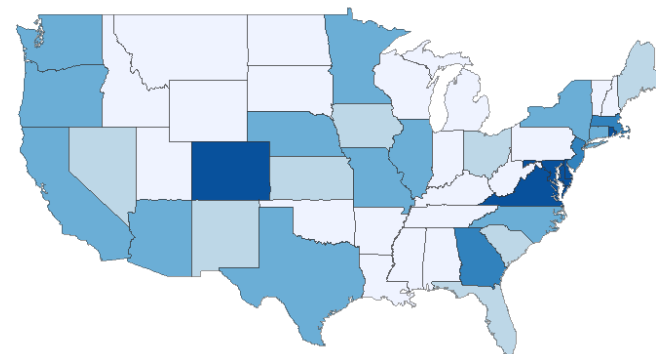
	State	Total Postings	Location Quotient**	% Growth (2010-2014)
1	California	28,744	1.02	75%
2	Virginia	20,276	3.09	38%
3	Texas	18,525	0.92	113%
4	New York	14,089	0.97	104%
5	Illinois	11,428	1.16	163%
6	Maryland	11,406	2.40	39%
7	Florida	9,847	0.67	135%
8	Georgia	8,757	1.22	121%
9	New Jersey	8,268	1.21	80%
10	Massachusetts	7,911	1.45	92%
11	Colorado	7,688	1.77	111%
12	North Carolina	7,503	1.06	127%
13	Ohio	6,281	0.72	141%
14	Pennsylvania	5,745	0.59	69%
15	Arizona	5,502	1.18	87%

Cybersecurity Job Postings in 2014 By State



Cyber Postings 0 to 999 1,000 to 2,499 2,500 to 4,999 5,000 to 10,000 10,000+

Cybersecurity Location Quotient in 2014



Cyber Postings Location Quotients Very Low Low Average High Very High

*See Appendix 1 for state-level data tables on total postings and postings growth.

**Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Cybersecurity Job Postings by City

Top Cities by Total Postings

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Washington, D.C.	27,246	39%
2	New York	17,982	90%
3	San Francisco / San Jose	13,869	88%
4	Chicago	9,623	164%
5	Dallas	8,694	138%
6	Los Angeles	7,654	47%
7	Boston	6,918	99%
8	Atlanta	6,604	128%
9	Denver	4,744	176%
10	Baltimore	4,643	49%

Top Cities by Growth

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Austin	2,937	209%
2	Columbus	1,916	178%
3	Denver	4,744	176%
4	Portland	2,424	175%
5	Chicago	9,623	164%
6	Miami	2,872	158%
7	Charlotte	3,000	147%
8	Tampa	2,606	145%
9	Dallas	8,694	138%
10	Atlanta	6,604	128%

Methodology

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100M worldwide postings collected since 2007. Each day, Burning Glass visits close to 40,000 online jobs sites to collect postings. Using advanced text analytics, over 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials and salary. Postings are then deduplicated and placed in a database for further analysis.

This report classifies cybersecurity jobs as those which have a cybersecurity-related title, require a cybersecurity certification or request cybersecurity-specific skills. Cybersecurity-related titles used to define the roles analyzed in this report include "network security", "information security", "information assurance", and "penetration tester". Cybersecurity skills include information assurance, cryptography, computer forensics, malware analysis, 800-53, and ArcSight.

The data in this report use a broader definition of cybersecurity roles than Burning Glass's 2014 report examining the same topic. That report looked only at those roles with cybersecurity-specific titles, whereas this update includes jobs with cybersecurity titles, certifications or skills.

Appendix 1: State Data

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Alabama	2,159	0.66	31%
2	Alaska	556	1.00	17%
3	Arizona	5,502	1.18	87%
4	Arkansas	989	0.5	117%
5	California	28,744	1.02	75%
6	Colorado	7,688	1.77	111%
7	Connecticut	2,771	0.97	98%
8	Delaware	1,152	1.67	92%
9	Florida	9,847	0.67	135%
10	Georgia	8,757	1.22	121%
11	Hawaii	1,364	1.31	39%
12	Idaho	634	0.53	260%
13	Illinois	11,428	1.16	163%
14	Indiana	2,347	0.48	139%
15	Iowa	1,951	0.74	158%
16	Kansas	1,654	0.71	168%
17	Kentucky	1,753	0.58	209%
18	Louisiana	1,563	0.48	275%
19	Maine	791	0.74	214%
20	Maryland	11,406	2.40	39%
21	Massachusetts	7,911	1.45	92%
22	Michigan	4,225	0.59	117%
23	Minnesota	4,059	0.88	98%
24	Mississippi	827	0.45	161%
25	Missouri	4,004	0.86	88%

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
26	Montana	344	0.43	189%
27	Nebraska	1,603	1.00	68%
28	Nevada	1,462	0.70	89%
29	New Hampshire	581	0.50	134%
30	New Jersey	8,268	1.21	80%
31	New Mexico	1,003	0.72	119%
32	New York	14,089	0.97	104%
33	North Carolina	7,503	1.06	127%
34	North Dakota	322	0.49	341%
35	Ohio	6,281	0.72	141%
36	Oklahoma	1,476	0.53	196%
37	Oregon	2,618	0.89	136%
38	Pennsylvania	5,745	0.59	69%
39	Rhode Island	1,267	1.53	134%
40	South Carolina	2,312	0.69	134%
41	South Dakota	354	0.50	195%
42	Tennessee	2,340	0.51	97%
43	Texas	18,525	0.92	113%
44	Utah	1,371	0.61	146%
45	Vermont	281	0.52	168%
46	Virginia	20,276	3.09	38%
47	Washington	5,119	0.96	94%
48	West Virginia	496	0.41	35%
49	Wisconsin	2,429	0.51	139%
50	Wyoming	176	0.37	245%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Appendix 2: City (MSA) Data

	MSA	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Atlanta	6,604	1.57	128%
2	Austin	2,937	1.88	209%
3	Baltimore	4,643	2.04	49%
4	Boston	6,918	1.52	99%
5	Charlotte	3,000	1.87	147%
6	Chicago	9,623	1.24	164%
7	Columbus	1,916	1.12	178%
8	Dallas	8,694	1.56	138%
9	Denver	4,744	2.03	176%
10	Detroit	2,753	0.84	112%
11	Houston	3,453	0.69	91%
12	Kansas City	1,884	1.06	111%
13	Los Angeles	7,654	0.78	47%
14	Miami	2,872	0.69	158%
15	Minneapolis	3,285	1.02	93%
16	New York	17,982	1.18	90%
17	Philadelphia	4,519	0.95	75%
18	Phoenix	4,044	1.26	101%
19	Portland, OR	2,424	1.30	175%
20	San Diego	3,068	1.32	94%
21	San Francisco / San Jose	13,869	4.89	88%
22	Seattle	4,105	1.32	100%
23	St. Louis	3,248	1.41	95%
24	Tampa	2,606	1.25	145%
25	Washington, D.C.	27,246	5.25	39%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

About Burning Glass

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. Burning Glass is reshaping how the job market works, with data that identify the skill gaps that keep job seekers and employers apart and tools that enable both sides to bridge that gap and connect more easily. The company's artificial intelligence technology analyzes hundreds of millions of job postings and real-life career transitions to provide insight into labor market patterns. This real-time strategic intelligence offers crucial insights, such as which jobs are most in demand, the specific skills employers need, and the career directions that offer the highest potential for workers.

Burning Glass' applications drive practical solutions and are used across the job market: by educators in aligning programs with the market, by employers and recruiters in filling positions more effectively, and by policy makers in shaping strategic workforce decisions. At the same time, Burning Glass' data-driven applications for workers and students help them choose career goals and build the skills they need to get ahead.

Based in Boston, Burning Glass is playing a growing role in informing the global conversation on education and the workforce, and in creating a job market that works for everyone.

For More Information

Dan Restuccia

Chief Analytics Officer

t +1 (617) 227-4800

drestuccia@burning-glass.com

www.burning-glass.com

Job Market Intelligence: Cybersecurity Jobs, 2015



Introduction: Cybersecurity and the Job Market

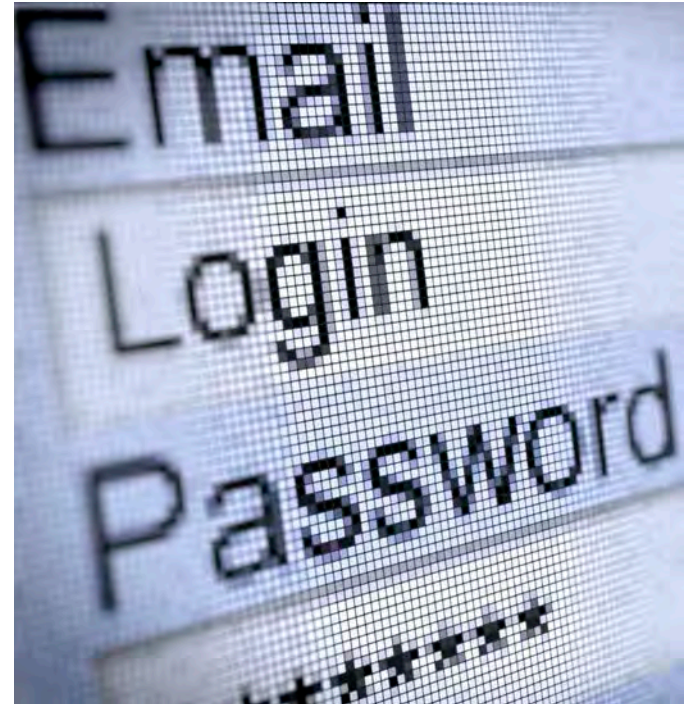
American employers have realized the vital importance of cybersecurity—but that realization has created a near-term shortage of workers that may require long-term solutions.

Cybersecurity was once the province of defense contractors and government agencies, but in this, the third edition of our annual analysis, we find **hiring has boomed in industries like Finance, Health Care, and Retail**. A glance at the headlines is enough to explain why. In addition to the federal Office of Personnel Management, recent cyber breaches have hit major consumer companies like Chase and Target. According to [PwC's 2015 State of US Cybercrime Survey](#), a record 79% of survey respondents said they detected a security incident in the past 12 months. Many incidents go undetected, however, so the real tally is probably much higher.

Yet we are also seeing multiple signs that demand for these workers is outstripping supply. **Job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall** and it takes companies longer to fill cybersecurity positions than other IT jobs. That's bad for employers but good news for **cybersecurity workers, who can command an average salary premium of nearly \$6,500 per year**, or 9% more than other IT workers.

Or put another way, there were nearly 50,000 postings for workers with a CISSP certification in 2014, the primary credential in cybersecurity work. That amounts to three-quarters of all the people who hold that certification in the United States—and presumably most of them already have jobs.

This is a gap that will take time to fill. The skills for some IT positions can be acquired with relatively little training, but cybersecurity isn't one of them. For example, five years of experience are required to even apply for a CISSP certification. That doesn't even consider the rising demand for experience in a specific industry, like finance or health care. This suggests that the shortage of cybersecurity workers is likely to persist, at least until the education and training system catches up.



Key Trends in Cybersecurity Demand

Cybersecurity jobs are in demand and growing across the economy

- The Professional Services, Finance, and Manufacturing/Defense sectors have the highest demand for cybersecurity jobs.
- The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%).

Positions calling for financial skills or a security clearance are even harder to fill than other cybersecurity jobs

- The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of these “hybrid jobs.”
- More than 10% of cybersecurity job postings advertise a security clearance requirement. These jobs, on average, take 10% longer to fill than cybersecurity jobs without a security clearance.

Cybersecurity positions are more likely to require certifications than other IT jobs

- One third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall.

Cybersecurity employers demand a highly educated, highly experienced workforce

- Some 84% of cybersecurity postings specify at least a bachelor’s degree, and 83% require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved through short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

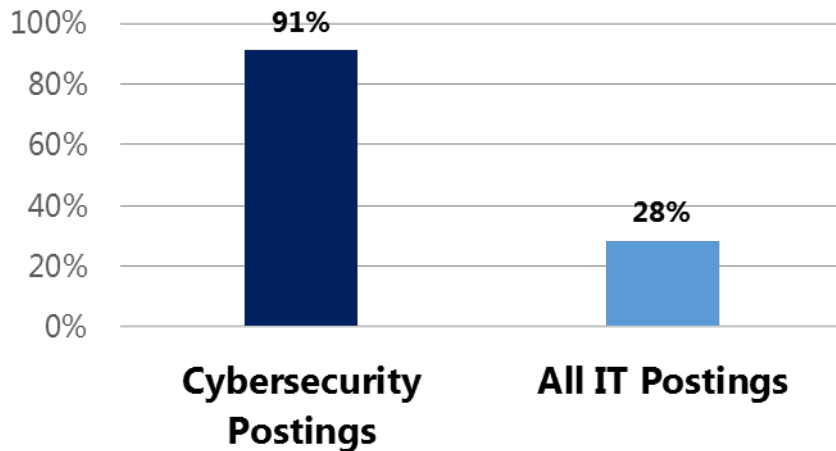
Geographically, cybersecurity jobs are concentrated in government and defense hubs, but are growing most quickly in secondary markets

- On a per capita basis, the leading states are Washington D.C., Virginia, Maryland, and Colorado; all have high concentrations of jobs in the federal government and related contractors.

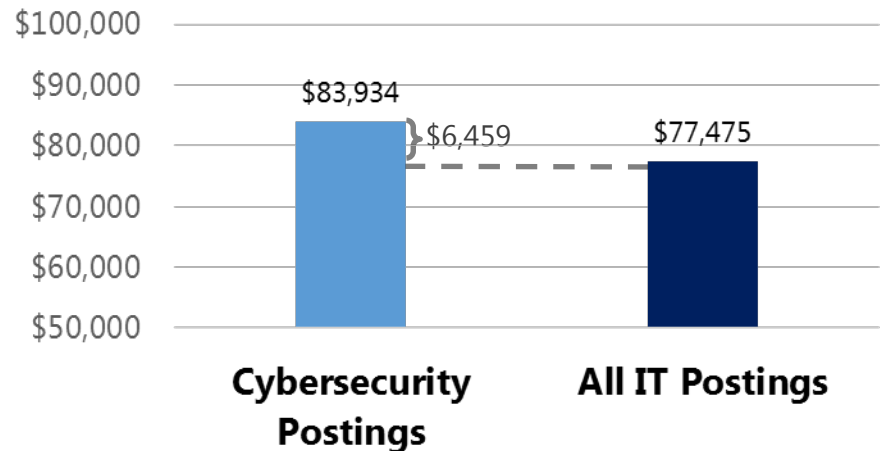
By the Numbers: The Cybersecurity Job Market

- In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for 11% of all IT jobs.**
- Cybersecurity postings have **grown 91%** from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took **8% longer to fill than IT job postings overall.**
- The demand for certificated cybersecurity talent is outstripping supply. In the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.*

Growth in Job Postings (2010-2014)











Cybersecurity Salary Premium



*According to the International Information System Security Certification Consortium, Inc., (ISC)²® membership counts as of July 14, 2015

Cybersecurity Demand Grows in Finance, Professional Services








- **Professional Services, Finance, and Manufacturing & Defense are the leading sectors** for cybersecurity professionals.
- Sectors managing increasing volumes of consumer data such as **Finance, Health Care, and Retail Trade have the fastest increases in demand** for cybersecurity workers.
- Within these sectors, demand for cybersecurity professionals is growing rapidly in more specific industry subsectors not typically associated with cybersecurity, including Air Transportation (+221%) and Accommodation (+157%).

Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765 	57%
Finance and Insurance	13%	17,873 	131%
Manufacturing & Defense*	12%	15,968 	57%
Public Administration	7%	9,725 	N/A**
Information	6%	8,522 	65%
Health Care and Social Assistance	6%	7,915 	118%
Retail Trade	3%	3,505 	120%
Other	15%	19,983 	N/A**

*The Manufacturing Sector includes services divisions of a number of defense contractors (e.g. Raytheon) and computer manufacturers (e.g. Hewlett Packard).
 ** Industry growth rates are suppressed for the Public Administration and Other industry sectors because a significant portion of labor market demand in these industries exists offline.

Engineers, Managers, and Analysts Dominate the Field

The cybersecurity workforce covers a range of job types and skills. This includes advanced Engineer and Architect roles, Auditors (which are concentrated in Finance) and Specialists, which typically have lower entry level requirements.

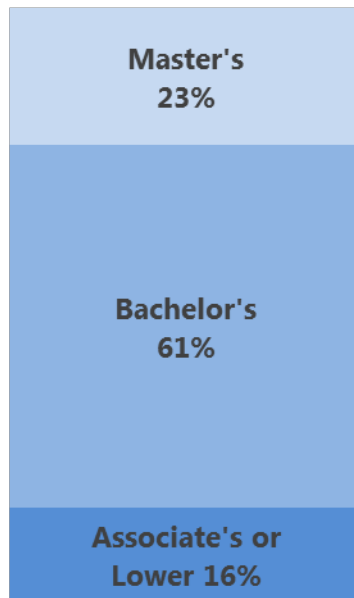
Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355 
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586 
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853 
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289 
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409 
Auditor (e.g. IT Auditor)	5%	7,533 
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294 

Employers Demand More Education, Experience

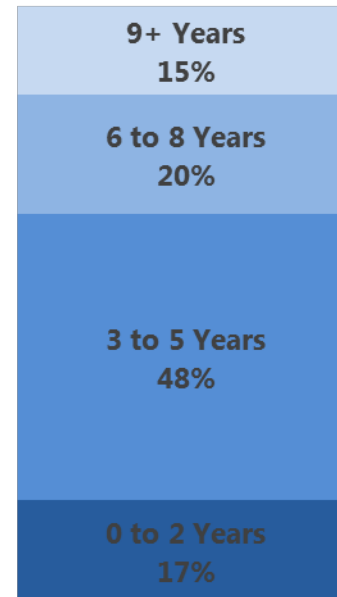
Cybersecurity jobs require significant education and experience. Some 84% of cybersecurity postings specify at least a bachelor's degree, and just as many (83%) require at least 3 years of experience, with an average of 5.4 years.

High education and experience requirements make skills gaps hard to close. Because cybersecurity jobs require years of training and relevant experience, skills gaps cannot easily be resolved through short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

Requested Education Level*



Minimum Experience



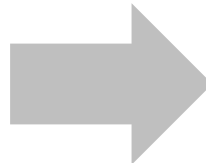
Certification Shapes the Path to Advancement

The cybersecurity job market is shaped by certifications, and job seekers of all experience levels can improve their employment opportunities by obtaining the relevant credentials. Entry-level workers, for example, can obtain foundational certifications such as Security+, which represents an entry point into the field and is by far the largest cybersecurity certification in terms of total holders. Experienced workers can target more advanced certifications such as CISSP, which requires holders to pass a rigorous exam and possess at least five years of information security experience – common requirements among advanced certifications.

Entry-Level Certifications

Typically require less than 3 years of experience

- Security+
- GIAC Security Essentials (GSEC)
- Certified Information Privacy Professional (CIPP)
- Systems Security Certified Practitioner (SSCP)



Advanced Certifications

Typically require at least 3-5 years of experience










- Certified Information Systems Security Professional (CISSP)*
- Certified Information Systems Auditor (CISA)*
- Certified Information Security Manager (CISM)*
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)

*Requires a minimum of 5 years of information security experience.

Certification is More Common in Cybersecurity Jobs

Cybersecurity jobs are highly certificated: More than one in three (35%) of all cybersecurity positions request at least one of the certifications listed below. Only 23% of overall advertised IT jobs request an industry certification.

Certification increases salary: Security+ represents the entry-level certification for cybersecurity roles, and postings requesting it advertise an average salary of \$75,484. This serves as a baseline salary for certified cybersecurity workers, and as workers obtain additional certification they can qualify for ever greater salaries. Postings requesting CISSP, for example, advertised an average salary of \$93,010 – a premium of \$17,526 over the average salary for Security+.

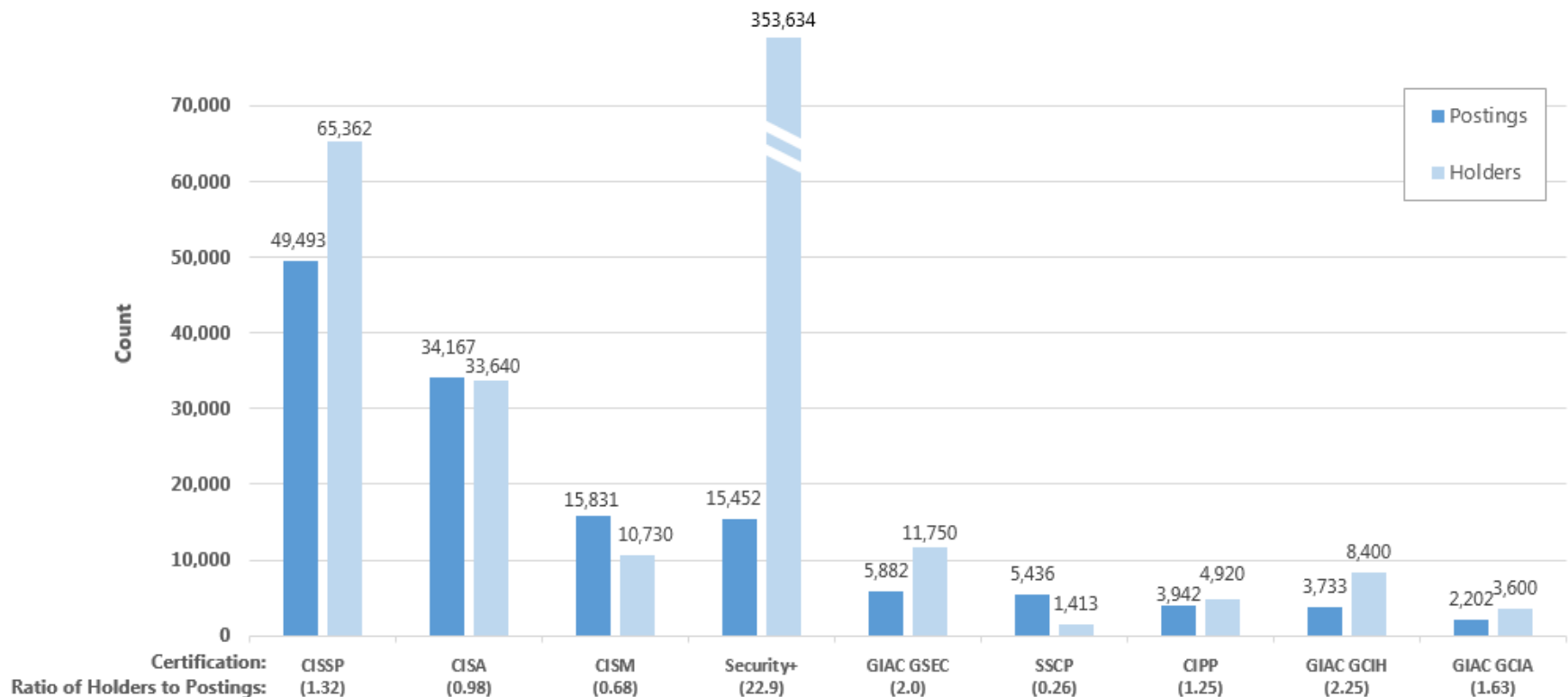
Certification*	% of All Cybersecurity Postings	Number of Cybersecurity Postings (2014)	Average Salary with Certification	Premium Over Security+ Average Salary
CISSP Certified Information Security Professional	21%	49,493 	\$93,010	\$17,526
CISA Certified Information Systems Auditor	14%	34,167 	\$86,238	\$10,754
CISM Certified Information Security Manager	7%	15,831 	\$95,450	\$19,966
Security+ Systems Security Certified Practitioner	6%	15,452 	\$75,484	\$0
GIAC GSEC GIAC Security Essentials	2%	5,882 	\$81,631	\$6,147
SSCP Systems Security Certified Practitioner	2%	5,436 	\$80,718	\$5,234
CIPP Certified Information Privacy Professional	2%	3,942 	\$90,550	\$15,066
GIAC GCIH GIAC Certified Incident Handler	2%	3,733 	\$92,759	\$17,275
GIAC GCIA GIAC Certified Intrusion Analyst	1%	2,202 	\$84,392	\$8,908

*Certification Requirements are not mutually exclusive

Certifications: Too Many Openings Chasing Too Few Workers

Employers prefer workers with cybersecurity certifications, but there can be three or more postings for every certificate holder. When you consider that most of these certificate holders are already employed, the situation looks even better for workers. Even the generous supply of Security + holders is somewhat misleading. Security + is an entry level certificate, so many people with more advanced credentials have one, and the openings that require it are relatively low-level.

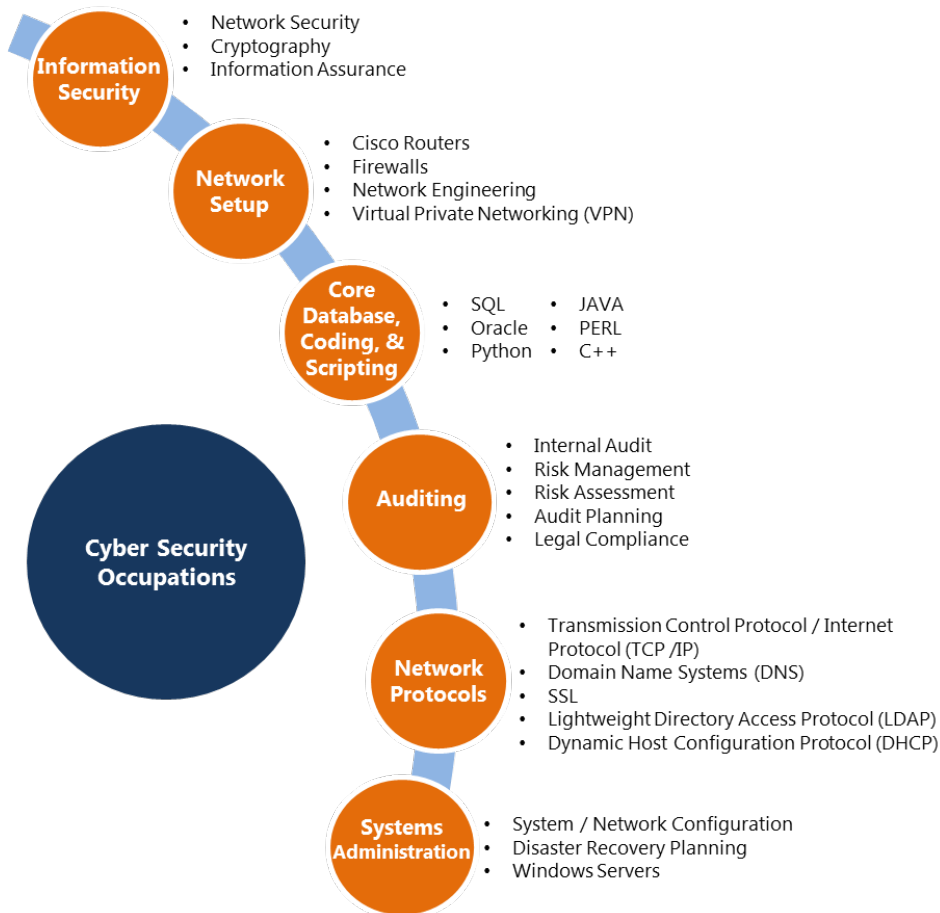
Certification Postings and Holders



Note: Different certifying organizations report slightly different counts of holders. For example, some may report total certifications awarded, while others may report only active certification holders.

Cybersecurity Workers Need to Know IT and Their Industry

The graphic below describes the expertise required for various cybersecurity roles in demand. On top of those skills, job postings often call for additional knowledge in certain information-sensitive industries, such as Health Care; Finance; and Manufacturing and Defense.



Additional Skill and Domain Knowledge Requirements by Industry

Health Care:

Skills:

- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:

- HIPAA
- HITECH
- Payment Card Industry Data Security Standard (PCI DSS)

Finance & Accounting:

Skills:

- Generally Accepted Accounting Principles
- Financial Reporting

Compliance & Standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

Manufacturing & Defense:

Compliance & Standards

- JAFAN 6/9 & 6/3, DCID 6/3 and DIACAP
- NERC Reliability Standards

Hybrid Jobs Combining Different Skills are Hardest to Fill

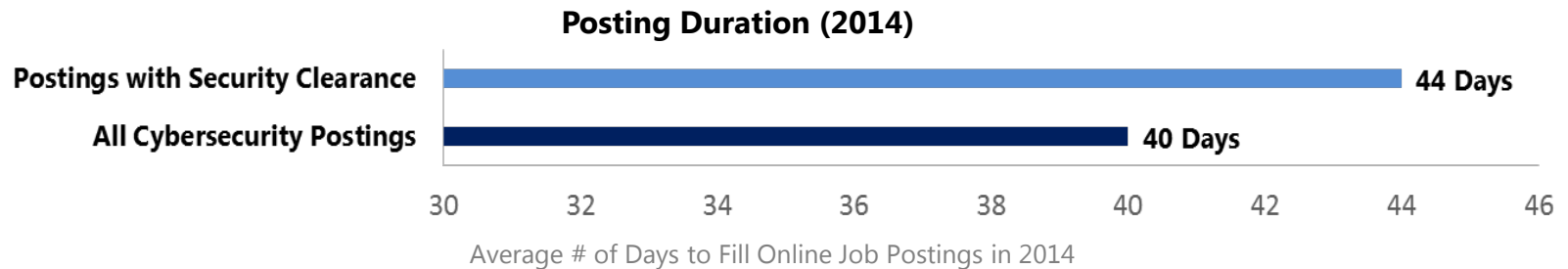
Employers often struggle to fill positions with specialized skill requirements. The fastest-growing skills include industry knowledge areas, such as HIPAA requirements in Health Care and Risk Management, and Accounting in Finance. The hardest-to-fill skills are typically related to finance, such as Information Assurance, Sarbanes-Oxley, and Accounting. **Finding candidates with these unique skill sets can take roughly 17% longer to fill on average than other cybersecurity job openings.**

The difficulties in filling jobs that require a combination of IT security and financial skills reflects a broader trend in the market: hybrid jobs which combine skill sets that are not traditionally trained for together. This often results in skills gaps where employers struggle to find employees that meet these skill needs.

Fastest-Growing Skills in Cybersecurity Job Postings	Five-Year Growth	Hardest to Fill Skills in Cybersecurity Job Postings	Posting Duration	Time to Fill Above Average
Python	309%	Management Information Systems	50 days	+10 days
HIPAA	248%	Information Assurance	47 days	+7 days
Risk Management	209%	Sarbanes-Oxley	47 days	+7 days
Internal Auditing	200%	Accounting	45 days	+5 days
Audit Planning	170%	Python	45 days	+5 days
Risk Assessment	169%	Dynamic Host Configuration Protocol (DHCP)	45 days	+5 days
ITIL	153%	Configuration Management	44 days	+4 days
Management Information Systems	132%	C++	44 days	+4 days
Accounting	121%	Public Accounting	43 days	+3 days
Configuration Management	106%	Internal Auditing	43 days	+3 days

Roles Requiring Security Clearance Take Longer to Fill

Workers with a security clearance—or the ability to get one—have an advantage. In 2014, there were 25,654 cybersecurity postings calling for a government Security Clearance to access classified information, representing 11% of all cybersecurity postings. On average, cybersecurity postings requesting Security Clearance remained open 10% longer than cybersecurity postings overall.



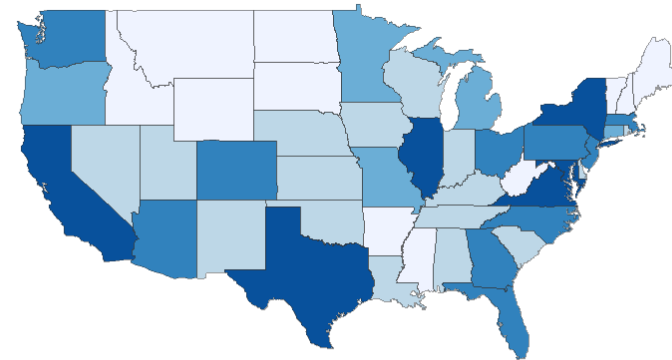
Industry Sector	Percentage of Industry Postings Requesting Security Clearance	Cybersecurity Postings Requesting Security Clearance (2014)
Public Administration	29%	2,793
Manufacturing & Defense*	19%	4,146
Professional Services	18%	10,317
Transportation and Warehousing	7%	107
Information	4%	471
Educational Services	4%	281
Finance and Insurance	2%	499
Healthcare and Social Assistance	1%	128

Cybersecurity Job Postings by State

Top States by Total Postings*

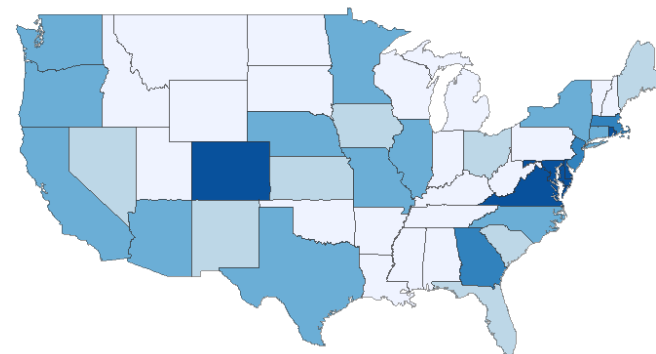
	State	Total Postings	Location Quotient**	% Growth (2010-2014)
1	California	28,744	1.02	75%
2	Virginia	20,276	3.09	38%
3	Texas	18,525	0.92	113%
4	New York	14,089	0.97	104%
5	Illinois	11,428	1.16	163%
6	Maryland	11,406	2.40	39%
7	Florida	9,847	0.67	135%
8	Georgia	8,757	1.22	121%
9	New Jersey	8,268	1.21	80%
10	Massachusetts	7,911	1.45	92%
11	Colorado	7,688	1.77	111%
12	North Carolina	7,503	1.06	127%
13	Ohio	6,281	0.72	141%
14	Pennsylvania	5,745	0.59	69%
15	Arizona	5,502	1.18	87%

Cybersecurity Job Postings in 2014 By State



Cyber Postings 0 to 999 1,000 to 2,499 2,500 to 4,999 5,000 to 10,000 10,000+

Cybersecurity Location Quotient in 2014



Cyber Postings Location Quotients Very Low Low Average High Very High

*See Appendix 1 for state-level data tables on total postings and postings growth.

**Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Cybersecurity Job Postings by City

Top Cities by Total Postings

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Washington, D.C.	27,246	39%
2	New York	17,982	90%
3	San Francisco / San Jose	13,869	88%
4	Chicago	9,623	164%
5	Dallas	8,694	138%
6	Los Angeles	7,654	47%
7	Boston	6,918	99%
8	Atlanta	6,604	128%
9	Denver	4,744	176%
10	Baltimore	4,643	49%

Top Cities by Growth

	City (MSA)	Total Postings	% Growth (2010-2014)
1	Austin	2,937	209%
2	Columbus	1,916	178%
3	Denver	4,744	176%
4	Portland	2,424	175%
5	Chicago	9,623	164%
6	Miami	2,872	158%
7	Charlotte	3,000	147%
8	Tampa	2,606	145%
9	Dallas	8,694	138%
10	Atlanta	6,604	128%

Methodology

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100M worldwide postings collected since 2007. Each day, Burning Glass visits close to 40,000 online jobs sites to collect postings. Using advanced text analytics, over 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials and salary. Postings are then deduplicated and placed in a database for further analysis.

This report classifies cybersecurity jobs as those which have a cybersecurity-related title, require a cybersecurity certification or request cybersecurity-specific skills. Cybersecurity-related titles used to define the roles analyzed in this report include "network security", "information security", "information assurance", and "penetration tester". Cybersecurity skills include information assurance, cryptography, computer forensics, malware analysis, 800-53, and ArcSight.

The data in this report use a broader definition of cybersecurity roles than Burning Glass's 2014 report examining the same topic. That report looked only at those roles with cybersecurity-specific titles, whereas this update includes jobs with cybersecurity titles, certifications or skills.

Appendix 1: State Data

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Alabama	2,159	0.66	31%
2	Alaska	556	1.00	17%
3	Arizona	5,502	1.18	87%
4	Arkansas	989	0.5	117%
5	California	28,744	1.02	75%
6	Colorado	7,688	1.77	111%
7	Connecticut	2,771	0.97	98%
8	Delaware	1,152	1.67	92%
9	Florida	9,847	0.67	135%
10	Georgia	8,757	1.22	121%
11	Hawaii	1,364	1.31	39%
12	Idaho	634	0.53	260%
13	Illinois	11,428	1.16	163%
14	Indiana	2,347	0.48	139%
15	Iowa	1,951	0.74	158%
16	Kansas	1,654	0.71	168%
17	Kentucky	1,753	0.58	209%
18	Louisiana	1,563	0.48	275%
19	Maine	791	0.74	214%
20	Maryland	11,406	2.40	39%
21	Massachusetts	7,911	1.45	92%
22	Michigan	4,225	0.59	117%
23	Minnesota	4,059	0.88	98%
24	Mississippi	827	0.45	161%
25	Missouri	4,004	0.86	88%

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
26	Montana	344	0.43	189%
27	Nebraska	1,603	1.00	68%
28	Nevada	1,462	0.70	89%
29	New Hampshire	581	0.50	134%
30	New Jersey	8,268	1.21	80%
31	New Mexico	1,003	0.72	119%
32	New York	14,089	0.97	104%
33	North Carolina	7,503	1.06	127%
34	North Dakota	322	0.49	341%
35	Ohio	6,281	0.72	141%
36	Oklahoma	1,476	0.53	196%
37	Oregon	2,618	0.89	136%
38	Pennsylvania	5,745	0.59	69%
39	Rhode Island	1,267	1.53	134%
40	South Carolina	2,312	0.69	134%
41	South Dakota	354	0.50	195%
42	Tennessee	2,340	0.51	97%
43	Texas	18,525	0.92	113%
44	Utah	1,371	0.61	146%
45	Vermont	281	0.52	168%
46	Virginia	20,276	3.09	38%
47	Washington	5,119	0.96	94%
48	West Virginia	496	0.41	35%
49	Wisconsin	2,429	0.51	139%
50	Wyoming	176	0.37	245%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

Appendix 2: City (MSA) Data

	MSA	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Atlanta	6,604	1.57	128%
2	Austin	2,937	1.88	209%
3	Baltimore	4,643	2.04	49%
4	Boston	6,918	1.52	99%
5	Charlotte	3,000	1.87	147%
6	Chicago	9,623	1.24	164%
7	Columbus	1,916	1.12	178%
8	Dallas	8,694	1.56	138%
9	Denver	4,744	2.03	176%
10	Detroit	2,753	0.84	112%
11	Houston	3,453	0.69	91%
12	Kansas City	1,884	1.06	111%
13	Los Angeles	7,654	0.78	47%
14	Miami	2,872	0.69	158%
15	Minneapolis	3,285	1.02	93%
16	New York	17,982	1.18	90%
17	Philadelphia	4,519	0.95	75%
18	Phoenix	4,044	1.26	101%
19	Portland, OR	2,424	1.30	175%
20	San Diego	3,068	1.32	94%
21	San Francisco / San Jose	13,869	4.89	88%
22	Seattle	4,105	1.32	100%
23	St. Louis	3,248	1.41	95%
24	Tampa	2,606	1.25	145%
25	Washington, D.C.	27,246	5.25	39%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

About Burning Glass

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. Burning Glass is reshaping how the job market works, with data that identify the skill gaps that keep job seekers and employers apart and tools that enable both sides to bridge that gap and connect more easily. The company's artificial intelligence technology analyzes hundreds of millions of job postings and real-life career transitions to provide insight into labor market patterns. This real-time strategic intelligence offers crucial insights, such as which jobs are most in demand, the specific skills employers need, and the career directions that offer the highest potential for workers.

Burning Glass' applications drive practical solutions and are used across the job market: by educators in aligning programs with the market, by employers and recruiters in filling positions more effectively, and by policy makers in shaping strategic workforce decisions. At the same time, Burning Glass' data-driven applications for workers and students help them choose career goals and build the skills they need to get ahead.

Based in Boston, Burning Glass is playing a growing role in informing the global conversation on education and the workforce, and in creating a job market that works for everyone.

For More Information

Dan Restuccia

Chief Analytics Officer

t +1 (617) 227-4800

drestuccia@burning-glass.com

www.burning-glass.com



Enter school name, location or keyw

X

Go

[Find Schools & Data](#)

[LoginSign Up](#)

[Community College Review](#)

-
- [WHY COMMUNITY COLLEGE](#)
- [CHOOSING A COLLEGE](#)
- [FINANCING](#)
- [STUDENT ISSUES](#)
-

Enter school name, location or keyw

X

Go

[Find Schools & Data](#)

[Home](#) > [Blog](#) > [Career Training](#) > [Science & Technology Careers](#)

Crack into Cyber-Security Training at Community Colleges

By [Grace Chen](#)

0



A career fighting cyber-terror and crimes can begin right at community college. Learn about the demand for cyber-security professionals and how you can obtain training at community colleges.



Associates Degrees	Bachelor's Degrees
Master's Degrees	Health Care
Criminal Justice	Business
Info. Technology	Get Started ▶

As we have come to rely more and more on computer systems for our daily lives, the issue of [security](#) has become a more widespread problem. From the original fear over a "Y2K" bug that could wipe out entire financial records when the calendar changed to the rising

concern over a variety of [terror threats](#), our country is on the search for highly trained cyber-experts that protect our precious computers from whatever ills might befall.

The result is a growing demand for cyber-security training – a challenge that many community colleges across the country have been more than happy to accept.

The Role of Community Colleges

According to a blog on [Bank Info Security](#) last year, community colleges are beginning to offer cyber-security training in hopes of tapping into funds President Obama has released to spend on strengthening [IT security](#). While this blog has voiced concern over the quality of training some students may receive, other reports are attesting to the fact that community college education in this area can be high quality, affordable and practical.

Finding the Best Schools

To help students find the best schools for their needs, the National Security Agency has designated a few institutions as National Centers for Academic Excellence, according to a report in the [Baltimore Business Journal](#). When an institution boasts this label, students can rest assured the cyber-security training program has been sanctioned by federal agencies.

Currently, there are 106 colleges and universities across the country that are Centers for Academic Excellence, including the U.S. Naval Academy and [Anne Arundel Community College](#) in the Baltimore area. Community colleges receive the distinction with a high-quality, two-year Information Assurance program.

What is Cyber Security?

According to the [Department of Homeland Security](#), there are many options for using your cyber-security training, including:

- Vulnerability detection and assessment
- Cyber incident response
- Cyber risk and strategic analysis
- Networks and systems engineering
- Intelligence and investigation

In addition to the various government jobs available in this area, employment in the private sector is also an option. Cyber-security experts might work in the following:

- As security experts for companies that have their own computer networks

- In banks and [health care institutions](#) to protect sensitive information on patients and customers
- As forensic experts that investigate a cyber crime after it occurs and track down the perpetrators

According to an article on [Edu.com](#), some cyber-security experts work as contractors, helping companies safeguard new computer systems or tracking down problems after they arise. In other instances, companies may place a cyber-security guard on staff to protect network systems and the sensitive information they contain.

The [Bureau of Labor Statistics](#) lumps network security experts with network and database administrators, and predicts a faster rate of job growth than the national average over the next few years in this field.

The job is typically handled in a comfortable office environment, although some aspects of the job may take place in other areas as well. The typical cyber-security expert may work more than the standard 40-hour work week in some situations, and he or she may be on call at times to handle emergencies as they arise.

Finding a Program

If cyber-security sounds like the right field for you, there are many training options available. Community colleges across the country are beginning to offer cyber-security training programs, allowing you to earn an [associates degree](#) in just two years. In addition to classes in information security technology, students will gain a background in computer science and program and technical management.

One community college currently offering a cyber-security program is [Herkimer County Community College](#) in Herkimer, New York. This program is available to students who can demonstrate computer literacy and who want to pursue a career in the field, or use the two-year program as a [springboard to a bachelor's degree](#). At Herkimer, the entire training program can be completed [online](#), making it an easy option for working adults and students who live too far away to commute to campus daily.

Cyber-security is a career path that is constantly growing and evolving. When you complete a training program in this field, it opens the door to a job with the federal government or in the private sector in a wide range of industries. The starting salary is competitive, and the job outlook appears to be bright for at least the next few years. Contact the community colleges in your area to find out if a cyber-security program is available, and get started on an exciting career in the area of network security and information management.

[Additional Resources \[+\]](#)

Barracuda for K-12



Put Student Safety First. Protect Your Data & IT Budget. Free Eval!



0 Comments

Community College Review

 Login ▾

 Recommend

 Share

Sort by Best ▾



Start the discussion...

Be the first to comment.

 Subscribe

 Add Disqus to your site

 Privacy

0

```
{"http://www.communitycollegereview.com/blog/crack-into-cyber-security-training-at-community-colleges":{"comments":{"data":[]}}}
```

Enroll in our free mini-course:
"Community College Survival Guide"

Name:

Email:

Submit

We respect your [email privacy](#)

PREVIOUS ARTICLE



[How to Start Your Aquarium Science Career at Community College](#)

NEXT ARTICLE



[Controlling a Career in Robotics](#)

Recent Articles



[Why Four Year Community College Degrees May Be Great for California](#)

Updated July 12, 2015

Recently, a measure passed that allows community colleges in California to offer 4 year degrees. Until now such offerings have been the sole province of other institutions. Now, the game has changed.

[Community College Pathways to a Career in Air Traffic Control](#)

Air traffic controllers enjoy secure, interesting work. Earning a degree in ATC at a community college is an excellent first step to securing a job.

[Community Colleges Offer Online Options](#)

Community colleges have responded to the needs of working adults with online options.

More Articles

[Choosing a School](#), [Student Issues / Attending College](#), [Courses in College](#), [College Policies](#), [Why Community College](#)

Get Your Degree!

Find schools and get information on the program that's right for you. *(It's fast and free!)*

Step 1 of 2

Choose an Area of Study

- Select One -

Highest Education

- Select One -

H.S. Grad Year

- Select One -

Learning Preference

- Select One -



ZIP

NEXT STEP

Powered by: **CAMPUS EXPLORER**

[Privacy Policy](#)

Enroll in our free mini-course:
"Community College Survival
Guide"

Name:

Email:

Submit

We respect your [email privacy](#)

[RSS/XML Feed](#)

Career Training

Science & Technology Careers

Indeed, science and technology careers, ranging from cyber-security to nano-technology, can all start from community college training. Get your feet wet with waterbotics, crack into cyber-security or dive into marine biology at your local community college.



- [Blast Off for Space Studies in Community College!](#)



- [How to Start Your Aquarium Science Career at Community College](#)



- [Crack into Cyber-Security Training at Community Colleges](#)

- More Articles:
- [Read more articles \(11\)](#)

- [Green Careers \(8\)](#)
- [Healthcare Careers \(11\)](#)
- [Culinary Careers \(7\)](#)
- [Business Careers \(1\)](#)
- [Education Careers \(1\)](#)
- [Creative Careers \(6\)](#)
- [Public Service Careers \(3\)](#)
- [Manufacturing Careers \(3\)](#)
- [Lucrative Jobs \(6\)](#)
- [Career Training 101 \(15\)](#)



Most Popular Articles



[Should Community Colleges Require Meningitis Vaccine for Admission?](#)



[What is a Community College?](#)



[Four-Year Degrees at Community College? Many Schools Now Say Yes](#)



[Choosing a Community College](#)



[New Analysis Shows How California Community Colleges Could Cut Millio...](#)

More Articles

[Choosing a School](#)

[Courses in College](#)

[College Policies](#)

[Financing](#)

[Community College News](#)

[Find Us](#)

[Follow Us](#)

X

[Find Schools & Data](#)

Community College Review 244 5th Avenue, # J-229 New York, NY 10001

© 2003-2015 All rights reserved.

[User Agreement](#) | [Privacy Policy](#)

- [Home](#)
- [About us](#)
- [Articles](#)

- [Student Member Area](#)
- [Find Community Colleges](#)
- [Compare Community Colleges](#)

- [College Member Area](#)
- [Feedback](#)

Community College Review

244 5th Avenue, # J-229 New York, NY 10001

© 2003-2015 All rights reserved.

[User Agreement](#) | [Privacy Policy](#)