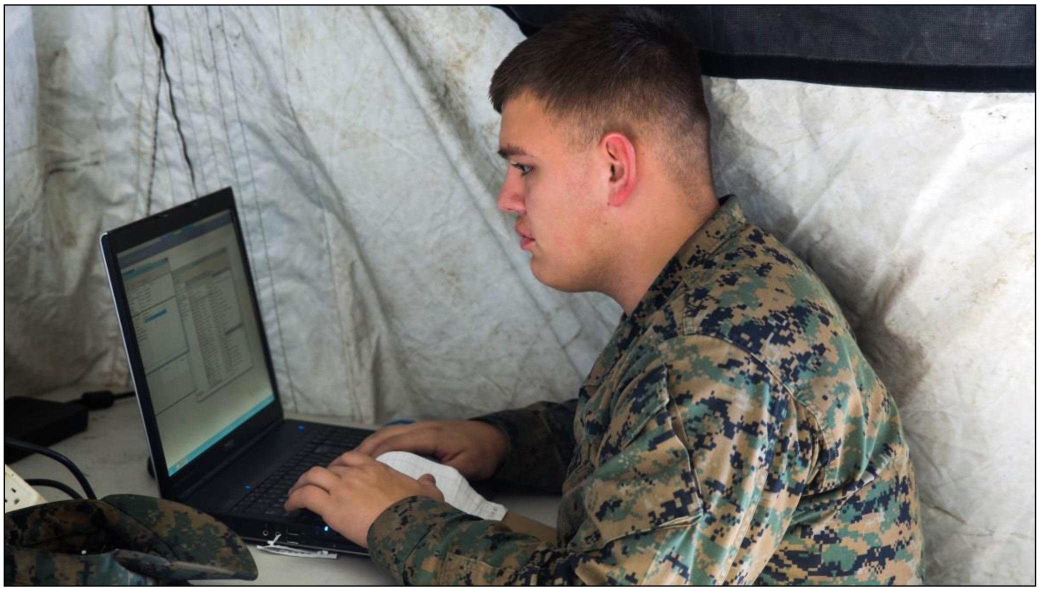
Understanding the Cybersecurity Labor Market: A Primer for CNA Analysts

Thomas Geraghty, Justin Ladner, Rikesh Nana, and Jeff Peterson

August 2016



Distribution Unlimited

CNA
ANALYSIS & SOLUTIONS

This document contains the best opinion of CNA at the time of issue.
It does not necessarily reflect the views of CNA or the Department of the Navy.

Distribution

Approved for Public Release; Distribution Unlimited. Specific authority: N00014-16-D-5003.

Photography Credit: PFC Alec Rivera, a cyber-network specialist with Headquarters Company, Combat Logistics Regiment 25, works on a computer during a command post exercise at Camp Lejeune, N.C., on Feb. 2, 2016. Photo by Cpl Paul S. Martinez. (http://www.marines.mil/Photos/igphoto/2001340296/).

Approved by: **August 2016**

Anita Hattiangadi

Anita U. Hattiangadi - Research Team Leader
Marine Corps Manpower Team
Resource Analysis Division

Abstract

This CNA-initiated study creates a primer for CNA analysts who are doing cybersecurity workforce analyses for the Department of Defense and the services. It is intended as a starting point to accelerate an analyst's understanding of the cybersecurity labor market, employment and training opportunities for cybersecurity professionals, key private-sector companies that provide cybersecurity services and/or employ cybersecurity professionals, and the certifications that cybersecurity personnel can earn. This work also includes a "big data" analysis (focused on current cybersecurity employment openings across the United States) that shows how state-of-the-art data analysis techniques can be used to analyze a rapidly changing labor market such as the one for cybersecurity professionals.

This page intentionally left blank.

Executive Summary

As cybersecurity threats proliferate and the corresponding demand for cybersecurity professionals grows, the Navy and Marine Corps increasingly are asking CNA to examine the population of civilians with cybersecurity skills and training. Although we know what it takes to become a cybersecurity Marine or Sailor, we generally do not have a good understanding of where civilian cybersecurity technicians are being produced, in what numbers, and what their comparable skills are.

In this CNA-initiated study, we pull together publicly available information on the following topics:

- Aspects of the **cybersecurity labor market**, including employment and wage trends, education, skill, and experience requirements, and the geographic location of major areas of cybersecurity analyst demand in the United States. These resources are intended to provide researchers with a starting point for conducting cybersecurity labor market analyses.
- The **education and training** opportunities available to cybersecurity professionals in both the military and the private sector. These sources cover procedures for training, certification, and management of DOD cybersecurity specialists, model curricula for cybersecurity training programs, lists of institutions of higher education that provide cybersecurity degree programs, and some information on which degree programs are considered to be high quality.
- Which **companies** are important players in the cybersecurity services sector, either as cybersecurity service providers, and/or as significant employers of cybersecurity professionals.
- The various **certifications** that can be earned by cybersecurity professionals, including information about the type of the certification, the experience level that is recommended as a prerequisite for those applying for the certification, and the number of professionals who hold that certification.

In addition, we include an example of a "big data" analysis focused on current cybersecurity employment openings across the United States. In a rapidly changing sector, such as cybersecurity, the labor market evolves rapidly, and traditional data sources cannot be revised quickly enough to provide an up-to-date view of the

market. Big-data tools can be used to provide up-to-the-minute information on labor market conditions. Specifically, we explore the use of online job forums as a tool for understanding a specific market, with cybersecurity jobs being the test case. We describe a methodology, "web-scraping," for extracting data from job forums, and we then use data gathered from one particular job forum website to provide insight into several details about the current cybersecurity labor market.

This work is intended as a primer for CNA analysts who are conducting cyber-related workforce analyses—particularly analyses related to recruiting existing cyber-trained personnel—and to provide analysts with a richer understanding of the cybersecurity landscape, which can inform business development with various sponsors. Increasing our understanding of the resources that characterize the cybersecurity technician civilian labor market will improve CNA's ability to help the Navy and Marine Corps to develop and evaluate cybersecurity recruiting, retention, and other related workforce policies. Because the cybersecurity world is rapidly evolving, and previous literature reviews may quickly become outdated, this resource should be periodically updated, perhaps as part of the CNA-initiated study process.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

Glossary

API	Application Programming Interface
CIPP	Certified Information Privacy Professional
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CND	Computer Network Defense
CONUS	Continental (or Contiguous) United States
COOL	Credentialing Opportunities Online
DHS	Department of Homeland Security
DOD	Department of Defense
GCIA	G Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
GSEC	GIAC Security Essentials Certification
IA	Information Assurance
IAM	Information Assurance Manager
IAT	Information Assurance Technical
IS	Information Security
IT	Information Technology
NSA	National Security Agency
SSCP	Systems Security Certified Practitioner
TIA	Technology Industry Association

This page intentionally left blank.

Introduction

CNA continues to be asked by the Department of Defense (DOD) and the services for analysis of the cybersecurity labor market [1]. Cybersecurity is a growth industry, and DOD must either compete for or develop cybersecurity technicians who can defend its networks and attack those of its adversaries. The curricula, certifications, and labor market features for cybersecurity technicians continue to rapidly evolve, and the timelines for manpower researchers to answer critical cybersecurity workforce questions are becoming shorter [2]. This primer is intended to accelerate analyst learning about the cybersecurity education/training and labor markets. Although it may not answer every specific question, it provides a robust array of information that we have pulled from various internet-based sources. Increasing our understanding of the resources that characterize the cybersecurity technician civilian education/training/labor market will improve CNA's ability to help the Navy and Marine Corps to develop and evaluate cybersecurity recruiting, retention, and other related workforce policies.

This report provides short summaries of the information that can be found at each accompanying internet link for the below-listed topical areas:

- Cybersecurity labor market
- Cybersecurity education and training
- Cybersecurity companies
- Cybersecurity certifications
- Cybersecurity "big data" opportunities

In the associated appendixes, we provide screenshots of the information to give analysts additional insights into the kinds of information that they will find at these links.

Cybersecurity Labor Market

Following are selected resources that will assist analysts in understanding aspects of the cybersecurity labor market (including employment and wage trends, education, skill, and experience requirements) and the geographic location of major areas of cybersecurity analyst demand in the United States. These resources are intended to provide researchers with a starting point for conducting cybersecurity labor market analyses. Appendix A provides selected screen shots of the information available from these sources.

Burning Glass Technologies. (2015). *Job Market Intelligence: Cybersecurity Jobs, 2015.*

http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

This is a brief report summarizing the state of the job market for cybersecurity professionals with data through 2014. It covers demand trends for cybersecurity workers, job types and skills, experience and educational requirements, and certifications in the sector. It also includes information on the geographic distribution of job opportunities by state and city.

Bureau of Labor Statistics, Employment Projections. (2014). Information Security.

http://data.bls.gov/projections/occupationProj

This resource provides information, by occupation, on current (2014) and projected (2024) employment, median annual wage, and education, work experience, and training requirements.

Bureau of Labor Statistics, National Employment Matrix (2015). Industries Where Information Security Analysts Are Employed.

http://data.bls.gov/projections/nationalMatrix?queryParams=15-1122-405&ioType=o

For industries in which Information Security Analysts are employed, this resource provides information on current and projected employment by sector (computer systems design and related services, management of companies and enterprises, depository credit intermediation, etc.).

Bureau of Labor Statistics, Occupational Outlook Handbook (2015). Information Security Analysts.

http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

For the Information Security Analyst occupation, this resource provides information on typical tasks and responsibilities, work environment, skill, education, experience, training requirements, pay, and projected employment growth. It includes links to state, area, and similar occupation data.

Bureau of Labor Statistics, Occupational Employment Statistics (2014). Occupational Employment and Wages, May 2014. 15-1122 Information Security Analysts.

http://www.bls.gov/oes/current/oes151122.htm

For Information Security Analysts, this resource provides information on wages and pay, both overall and by sector, and a geographic profile of the occupation highlighting employment, job concentration, and average wages by state and metropolitan area.

O*Net Online (2015). Summary Report for: 15-1122.00 - Information Security Analysts.

http://www.onetonline.org/link/summary/15-1122.00

This resource provides a summary report for the Information Security Analyst occupation. It provides information on job tasks and work activities, tools and technologies used in the occupation, and skill and ability, education, experience, and training requirements. It also provides links to related occupations and wage and employment trend information.

PayScale, Inc. (2016). Information Security Analyst Salary (United States). http://www.payscale.com/research/US/Job=Information_Security_Analyst/Salary

For Information Security Analysts, this resource provides information on pay (including variation by experience and location and salaries of related jobs), job descriptions, skill requirements, common career paths, and some employer-specific information, including salary ranges.

Sargent, John F., Jr. (2014). *The U.S. Science and Engineering Workforce: Recent, Current, and Projected Employment, Wages, and Unemployment*. Congressional Research Service. https://www.fas.org/sgp/crs/misc/R43061.pdf

This report summarizes information on employment and current pay levels, recent trends, and future projections for the U.S. science and engineering workforce. It provides useful information for comparing information security analysts with those in other computer science and science/engineering-related occupations.

Cybersecurity Education and Training

The following are selected resources that will assist analysts with understanding the education and training opportunities available to cybersecurity professionals in both the military and the private sector. These sources cover procedures for training, certification, and management of DOD cybersecurity specialists, model curricula for cybersecurity training programs, lists of institutions of higher education that provide cybersecurity degree programs, and some information on which degree programs are considered to be high quality. Appendix B provides selected screenshots of the information available from these resources.

Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Chief Information Officer (2015). Information Assurance Workforce Improvement Program. DOD 8570.01-M.

http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.

This DOD manual provides guidance and procedures for the training, certification, and management of the DOD workforce that conducts Information Assurance (IA) functions in assigned duty positions. It also provides information and guidance on reporting metrics and the implementation schedule for DOD Directive 8140.01, “Cyberspace Workforce Management,” August 11, 2015.

ISACA. (2012). *ISACA® Model Curriculum for Information Security Management*, 2nd Edition.

http://www.isaca.org/Knowledge-Center/Academia/Pages/Model-Curriculum-for-Information-Security-Management.aspx

This document provides information on academic institutions with a basic educational framework required to make students employable in the Information Security Management profession. The topics covered by the model are grouped into four domains: (1) Information Security Governance, (2) Information Risk Management and Compliance, (3) Information Security Program Development and Management, and (4) Information Security Incident Management. These domains are broken into major topic areas, and subtopics are provided within each topic area, along with the number of contact hours needed to adequately cover the topic.

ISACA. (2012). *ISACA® Model Curriculum for IS Audit and Control*, 3rd Edition.

http://www.isaca.org/Knowledge-Center/Academia/Pages/Model-Curriculum-for-IS-Audit-and-Control-3rd-Edition.aspx

This report identifies the fundamental course components of Information Security (IS) audit and control so that universities can educate students for careers in the IS audit and assurance profession and assist students in becoming marketable in the field. The topics identified in the model have been selected to provide graduates with entry-level skills and capabilities for the profession. The model matches academic offerings with the needs of the profession and provides a framework for universities and professional associations to develop new courses or redesign existing course offerings. The topics covered by the model are grouped into the following five content domains: (1) Process of Auditing Information Systems, (2) Governance and Management of IT, (3) Information Systems Acquisition, Development, and Implementation, (4) Information Systems Operations, Maintenance, and Support, and (5) Protection of Information Assets.

U.S. News and World Report (2015). "Online Cybersecurity Bachelor's Degree."

http://www.usnews.com/education/online-education/cyber-security-bachelors-degree

This article provides information about online cybersecurity degree programs, including coursework and job outlook and salary information for graduates.

Nana, Rikesh (2015). Cybersecurity Program Database.

https://public.tableau.com/profile/rikesh#!/vizhome/CybersecurityPrograms/Dashboard1[1]

This resource provides an interactive U.S. map that allows the user to click on a state and obtain a list of colleges and universities offering cybersecurity degree programs. The user can filter the list by degree type and whether the program is highly ranked and/or National Security Agency (NSA) certified.[2]

[1] To ensure link functionality, please copy and paste this link into a web browser (as opposed to clicking on it).

[2] One of the goals of this work was to identify student enrollments in these programs. Unfortunately, we were unable to locate resources that provided enrollment numbers.

Ponemon Institute LLC. (2014). *2014 Best Schools for Cybersecurity*. Ponemon Institute Research Report sponsored by HP Enterprise Security.

http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf

This report summarizes the results of a survey of subject matter experts who were asked to identify educational institutions that are achieving a high level of excellence in academics, the practical relevance of their programs, the experience and expertise of program faculty, the experience and background of students and alumni, and the institution's professional reputation in the cybersecurity community. According to the report, characteristics of highly rated educational programs in cybersecurity include being interdisciplinary (combining the disciplines of computer science, engineering, and management), having a curriculum that addresses both technical and theoretical issues, and developing a hands-on learning environment where students and faculty work together on projects that address real-life cybersecurity threats.

National Security Agency, Central Security Service. (2015). Centers of Academic Excellence Institutions

https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

This resource lists, by state, institutions of higher education offering programs in IA rated by the NSA as "National Centers of Excellence" in two-year education, four-year education, or research.

Cybersecurity Companies and Civilian Career Opportunities

In what follows, we present selected resources that will assist analysts with understanding which companies are important players in the cybersecurity services sector and which companies are significant employers of cybersecurity professionals. Appendix C provides selected screenshots of the information available.

Cybersecurity Ventures (2015). Top 25 Cybersecurity Companies to Watch in 2016.

> http://www.itbusinessedge.com/slideshows/top-25-cybersecurity-companies-to-watch-in-2015.html
>
> Cybersecurity Ventures is a research and marketing information firm focused on cybersecurity companies. Its list of "companies to watch" is based on feedback from Chief Information Security Officers (CISOs) and end-user security practitioners and on research gleaned from security events and news sources. Companies are evaluated on such criteria as their security market category, problems solved, customer base, venture capital funding, company growth, and published reviews.

CareerBuilder, Cybersecurity Jobs.

> http://www.careerbuilder.com/jobs/keyword/cybersecurity
>
> This resource lists cybersecurity job openings across the country, providing information on which industries and companies have how many current listings and which cities and states have the most listings. Other sites, such as LinkedIn and Glassdoor, also have information on individual companies, including type of company (private, public, etc.), revenue category, and average salaries.

Cybersecurity Certifications

Table 1 and Table 2 provide information on some of the important entry-level and advanced certifications that can be earned by cybersecurity professionals, including the type or level of the certification, the experience level that is recommended as a prerequisite for those applying for the certification, and the number of professionals who hold that certification in 2015. Entry-level certifications typically can be earned by individuals with 0 to 2 years of experience, while advanced certifications often require 5 or more years of experience as a prerequisite.

To provide some explanation for the terminology in the tables, the IA level of a certification refers to the scale of the computer system environment:[3]

- Level I: Computing Environment (i.e., environment the size of an office/shop)
- Level II: Networking Environment (i.e., environment the size of a command/ship-wide)
- Level III: Enclave (i.e., Naval Computer and Telecommunications Area Master Station (NCTAMS), Global Network Operations Center, global environment)

Computer Network Defense (CND)-A (Analyst) personnel use data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze and evaluate events that occur within their environment.

CND-IR (Incident Responder) personnel investigate and analyze all response activities related to computer security incidents within the Networking Environment or Enclave. These tasks include, but are not limited to, creating and maintaining incident tracking information; planning, coordinating, and directing recovery activities; and incident analysis tasks, including examining all available information and supporting information or artifacts related to an incident or event.[4]

[3] See Navy Credential Opportunities Online (COOL) Information Assurance Technician Flow Chart, http://www.cool.navy.mil/usn/ia_documents/ia_iat_flow.htm.

[4] See Navy COOL Computer Network Defense Flow Chart (http://www.cool.navy.mil/usn/ia_documents/ia_cnd_flow.htm).

Table 1. Common entry-level cybersecurity certifications

Entry-Level Certifications	Computing Environment Type/Level	Recommended Experience as Prerequisite for Certification	Holders (2015)
Security+	IAM Level I[a]	CompTIA[a] Network+ certification and 2 years of technical networking experience, with an emphasis on security	353,634
GIAC Security Essentials (GSEC)	IAT Level II[a]	No specific training/experience is required	11,750
Certified Information Privacy Professional (CIPP)	N/A	N/A	4,920
Systems Security Certified Practitioner (SSCP)	IAT Level II[a]	Minimum of 1 year of cumulative paid full-time work experience in 1 or more of 7 domains (Access Controls, Security Operations and Administration, Risk Identification Monitoring and Analysis, Incident Response and Recovery, Cryptography, Network and Communications Security, and Systems and Application Security)	1,413

Sources: Burning Glass Technologies, "Job Market Intelligence: Cybersecurity Jobs, 2015," Transcender (http://www.transcender.com/gen.aspx?pf=page&sn=tra_dod8570.1_sec)

[a] IAM is "Information Assurance Manager," IAT is "Information Assurance Technical," and TIA is "Technology Industry Association."

Table 2. Common advanced cybersecurity certifications

Advanced Certifications	Computing Environment Type/Level	Recommended Experience as Prerequisite for Certification	Holders (2015)
Certified Information Systems Security Professional (CISSP)	IAT Level III[a]	Minimum of 5 years of cumulative paid full-time work experience in 2 or more of 8 domains (Security and Risk Management, Asset Security, Security Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security)	65,362
Certified Information Systems Auditor (CISA)	IAT Level III[a]	Minimum of 5 years of professional information systems auditing, control, or security work experience	33,640
Certified Information Security Manager (CISM)	IAM Level II[a]	Minimum of 5 years of IS work experience, with a minimum of 3 years of IS management work experience in 3 or more job practice analysis areas (IS Governance, Information Risk Management and Compliance, IS Program Development and Management, and IS Incident Management)	10,730
GIAC-Certified Incident Handler (GCIH)	CND[a] Incident Responder	No specific training/experience is required	8,400
GIAC-Certified Intrusion Analyst (GCIA)	CND[a] Analyst	No specific training/experience is required	3,600

Sources: Burning Glass Technologies, "Job Market Intelligence: Cybersecurity Jobs, 2015;" Transcender (http://www.transcender.com/gen.aspx?pf=page&sn=tra_dod8570.1_sec).

[a]. IAT is "Information Assurance Technical," IAM is "Information Assurance Manager," and CND is "Computer Network Defense."

Appendix D provides a list of additional certification types.

A Big-Data Approach to Understanding the Cybersecurity Labor Market

CNA is continuing to find opportunities to incorporate big-data techniques into its analyses. Here, we provide an example of "web-scraping," a method for autonomously gathering content from webpages. Although this tool does not always (or even commonly) involve all of the characteristics associated with big data (i.e., high volume, high velocity, and variety), it can be used to collect many forms of unstructured data[5] and, consequently, represents a powerful new tool in modern empirical research.

Up to this point, we have focused on understanding the cybersecurity labor market using data and/or reports from agencies that one would traditionally turn to when conducting research. Of course, these sources have significant value, but they also have limitations. For example, labor markets often evolve rapidly, so data produced from official surveys cannot be compiled and published fast enough to provide the researcher with an up-to-date view of the market. Given that the cybersecurity job market is particularly dynamic, one might be especially concerned that formal survey data fail to capture current conditions.

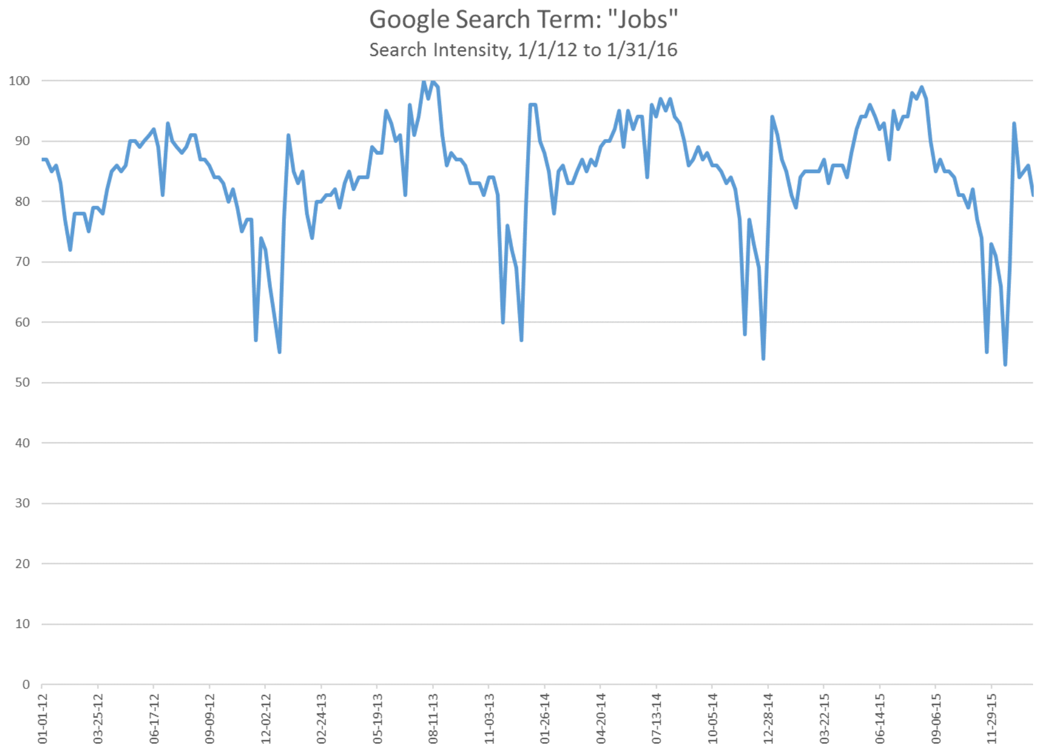
To illustrate this point, consider Figure 1 and Figure 2, which were produced using search intensity data from Google Trends.[6] In both cases, these figures plot the relative frequency of different search terms on Google between January 1, 2012, and January 31, 2016. In the first case, the keyword is *jobs,* a term that was chosen to capture the intensity with which internet users searched for any kind of employment during the period. Figure 2, however, reports results obtained for the key phrase

[5] In this sense, web-scraping exemplifies the "variety" characteristic associated with big data.

[6] Google Trends is a service offered by Google. Among other features, it allows users to track the popularity of search terms across time and at different geographical locations, using archived data from the Google search engine. For any given search term, Google Trends produces an index reflecting the relative popularity of the term over time; the value 100 always represents the most popular point in the chosen date range.

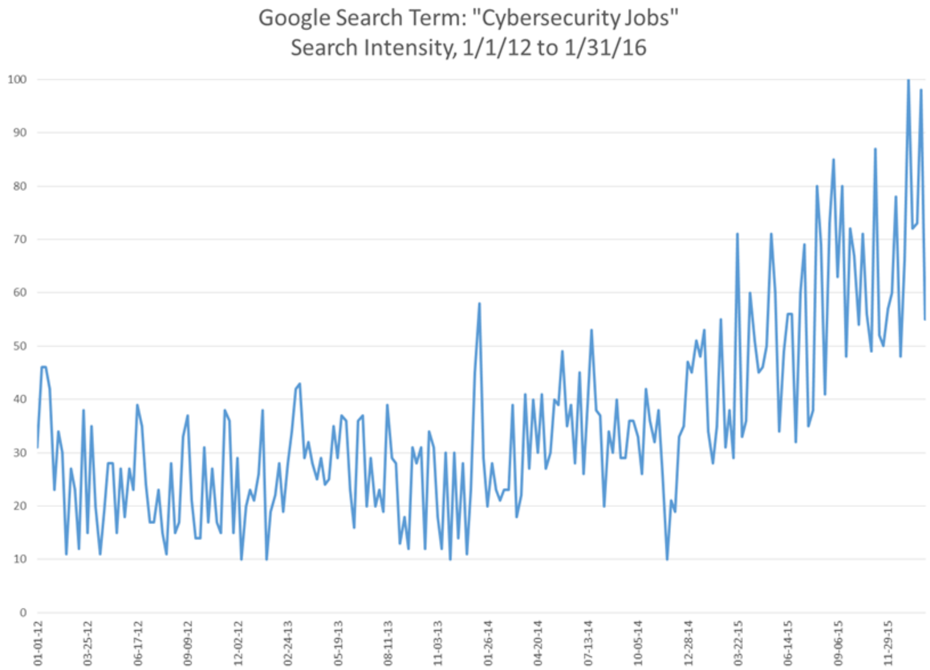
cybersecurity jobs. The difference between the two plots is striking: whereas average search intensity for *jobs* was fairly flat (with clear seasonal variation) during the entire period, the popularity of *cybersecurity jobs* as a search term grew dramatically (especially starting in 2014). This growth suggests that this industry is evolving rapidly, which makes an up-to-date view of the cybersecurity labor market particularly desirable.

Figure 1. Number of Google searches for the term *jobs,* January 2012 through January 2016



Source: Google Trends.

Figure 2. Number of Google searches for the term *cybersecurity jobs,* January 2012 through January 2016



Source: Google Trends.

Until relatively recently, the limitations of survey-based labor market data were a fact of life for researchers; after all, only a handful of large (usually government) organizations had the resources necessary to conduct nationally representative surveys, and even efficiently run surveys take a long time to complete when implemented on that scale. Fortunately, the internet provides many novel avenues through which labor markets can operate, creating new opportunities for data collection. In particular, the proliferation of online job boards has made it possible to view tens of thousands of current job postings from companies all over the world. Aside from facilitating employer-employee matching, these forums represent publicly available labor market databases that (with the right tools) can be used to ascertain up-to-the-minute labor market conditions.

Next, we explore the use of online job forums as a tool for understanding a specific market, with cybersecurity jobs being the test case. In the subsections that follow, we describe a methodology for extracting data from job forums, and we use data gathered from two websites to highlight several details about the current cybersecurity labor market. After reviewing our findings, we offer some concluding remarks about the viability of these techniques for future research efforts.

Methodology: Web-scraping

In a broad sense, web-scraping is simply the collection of online content for the purpose of building a dataset. Manual copying/pasting is the crudest example, but in practice the term is almost exclusively used to describe automated computer programs that systematically visit webpages and extract content. The value of such programs becomes obvious when one wishes to collect data that are spread over thousands of pages: it would be nearly impossible for a single person to manually visit every page, and attempting to do so would represent an enormous waste of labor. In this study, we collect job posts from an online job forum using a free browser add-on called iMacros. This tool allowed us to download thousands of job board webpages as text files, which we then used to build a dataset for analysis. A 2015 CNA report discusses the mechanics of web-scraping in more detail [3].

The first step in any web-scraping exercise is to determine where to look for data. Recall that we want to collect data from online job boards; specifically, we would like to extract information from job advertisements that employers post. There are many websites to choose from, but two websites (USAJOBS and Glassdoor) stand out as the best options for our purposes.

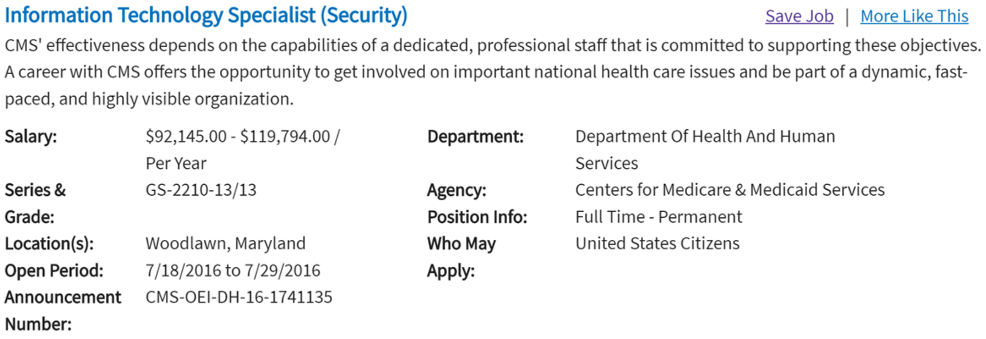
USAJOBS is an online job forum specifically dedicated to employment in federal agencies of the United States government. This focus has a number of advantages for our research, but also suffers from an important limitation. On the positive side, the individual posts on USAJOBS generally have more consistent information about the position and provide greater detail than is typically available on sites dedicated to private-sector employment. For example, nearly every post on USAJOBS provides salary information (in the form of a pay range), a relative rarity for job posts on websites focused on the private sector. Furthermore, since almost every federal entity must use USAJOBS, the site's job posts provide an accurate picture of the federal government current employment demands.[7] The primary drawback of USAJOBS is that it focuses on a narrow slice of the labor market (i.e., federal jobs) and therefore does a poor job of describing some aspects of labor demand in the country as a whole. In particular, the geographic distribution of federal jobs is biased heavily toward certain locations (e.g., Washington, D.C.), so data from USAJOBS may fail to capture where demand for cybersecurity employment is highest.

[7] In contrast, sites focusing on private-sector employment invariably suffer from a selection issue since different types of private-sector employers are more or less likely to use online job boards to search for workers.

Fortunately, comprehensive private-sector information on the geographic distribution of cybersecurity jobs is available from Glassdoor, a company that hosts one of the largest and most popular online job boards in use today. Although directly scraping job posts from Glassdoor's website is prohibited, limited types of aggregated data are available through the company's public-use Application Programming Interface (API). Using these data, we are able to more accurately depict the distribution of cybersecurity employment in the United States.

After determining which websites to use, we scraped USAJOBS during the afternoon of July 27, 2016. This process visited hundreds of webpages and gathered data on just over 14,800 unique job posts. Crucially, every post shares the same general format, an example of which is given in Figure 3. For each post, it is possible to extract 10 items, including job location, hiring department/agency, and salary range. All 10 of these fields can be retrieved for the vast majority of posts, though in a significant minority of cases (approximately 11 percent[8]) the job location cannot be identified.[9]

Figure 3. Format of a typical job posting on USAJOBS



Information Technology Specialist (Security) Save Job | More Like This

CMS' effectiveness depends on the capabilities of a dedicated, professional staff that is committed to supporting these objectives. A career with CMS offers the opportunity to get involved on important national health care issues and be part of a dynamic, fast-paced, and highly visible organization.

Salary:	$92,145.00 - $119,794.00 / Per Year	**Department:**	Department Of Health And Human Services
Series & Grade:	GS-2210-13/13	**Agency:**	Centers for Medicare & Medicaid Services
Location(s):	Woodlawn, Maryland	**Position Info:**	Full Time - Permanent
Open Period:	7/18/2016 to 7/29/2016	**Who May Apply:**	United States Citizens
Announcement Number:	CMS-OEI-DH-16-1741135		

Source: USAJOBS.

The data we collected from USAJOBS were gathered in several separate scrapes. In the first, we attempted to download every job post available on the site, regardless of its specific characteristics. Having done so, we then completed two additional scrapes, which identified job posts using search terms specific to cybersecurity positions. In the first additional scrape (second overall), we limited our attention to

[8] The job location could not be identified in 1,649 out of 14,841 posts.

[9] These missing values occur because some job posts on USAJOBS are advertising multiple locations, in which case the term *Multiple Locations* is inserted into the field that would normally contain the specific location.

posts containing the exact phrase *information security;* in the second (third overall), we only scraped posts containing the term *infosec.* In the context of federal employment, *information security* appears to be the most popular term used when referring to cybersecurity positions, and *infosec* is a standard abbreviation. After collecting job posts in the manner described above, we merged the data from all scrapes into a single, unified dataset. Job posts captured in the second and/or third scrape were identified as cybersecurity jobs (251 posts, or 1.69 percent), and all remaining posts were classified as non-cybersecurity jobs (14,583 posts, or 98.31 percent).[10, 11] In total, the dataset contains 14,841 unique job posts.

To understand the geographic distribution of private-sector cybersecurity jobs, we turned to the Glassdoor API mentioned earlier. Web-scraping was also used to collect data from this service, though the process differed significantly. Rather than directly collecting job posts, we used a web-scraping program to repeatedly submit queries to Glassdoor's API, which returned results that we then downloaded as text files. The queries we submitted specified one or more of the following characteristics: (1) job title, (2) job category, (3) age of job post, and (4) geographic aggregation level. For example, we might want to know how many jobs with the title of "security analyst" in the job category of "software development/IT" were posted on Glassdoor's website in the last year in each state.

Identifying cybersecurity job posts in the Glassdoor API is more complicated than the process we described for USAJOBS, mostly because there is much more diversity in the private sector with regard to cybersecurity job titles. Using a 2014 report from the SANS Institute, we identified the 24 most common job titles in the cybersecurity industry and submitted a state-level query for each [4].[12] Since several of the titles in our list are vague enough to appear in many different contexts (e.g., "security officer"), every query specified the job category as "software development/IT." After collecting these data, we defined the total number of cybersecurity jobs posts in each state to be the sum of posts across all 24 job titles. Finally, an additional state-level

[10] The terms *information security* and *infosec* often appear together in the same job post, so there was significant overlap in the jobs captured in the second and third scrapes.

[11] Our identification of cybersecurity jobs is fairly conservative, in the sense that we are unlikely to have misidentified many non-cybersecurity positions as being cybersecurity positions. This is because the terms *information security* and *infosec* are essentially never used in federal employment except to refer to cybersecurity jobs. However, this conservative approach probably fails to capture some cybersecurity positions since some job posts may fail to include either term.

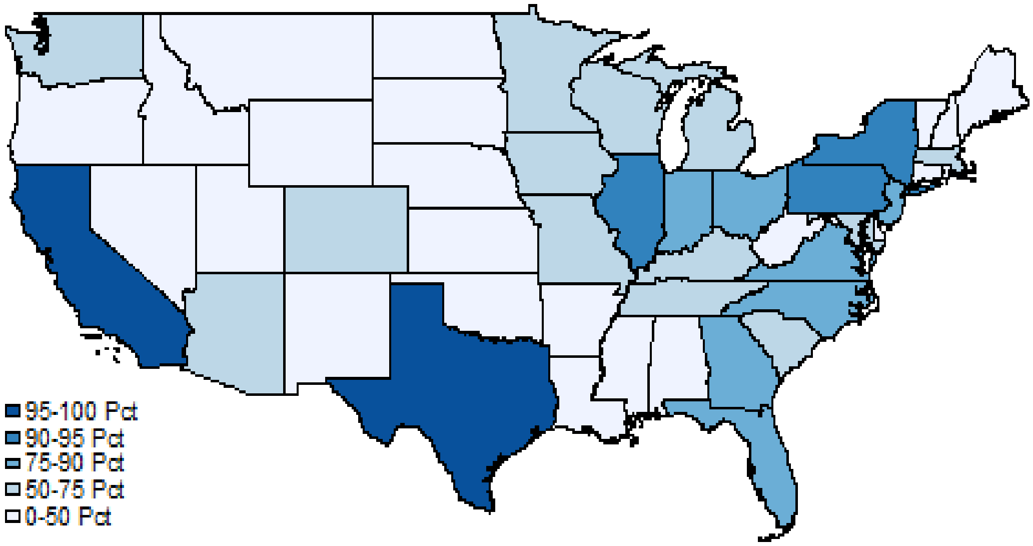
[12] See https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615 for the SANS Institute report. The table of common job titles is on page 4; we added the title of "information security analyst" (very similar to the top-ranked title of "security analyst") because it also shows up frequently.

query was conducted with no specified job title or category, yielding the total number of job posts (of all kinds) in each state. In every case, we only counted jobs that had been posted on Glassdoor within a year of the date the data were collected (July 20, 2016).

Results: Geographic distribution of jobs

Recall that, given its exclusive focus on federal employment, our USAJOBS dataset is poorly suited for examining the geographic distribution of cybersecurity jobs, so in this subsection we use data from our Glassdoor API dataset (described earlier). These results begin with Figure 4, which displays the geographic distribution of all non-cybersecurity job posts in the contiguous United States (CONUS). This figure was created by first ranking all states (and D.C.) by the absolute number of posts for all job types and then sorting these states into groups based on their percentile ranking.[13] Table 3 lists the top 15 states in terms of total non-cybersecurity job posts.

Figure 4. Geographic distribution of all non-cybersecurity job posts within CONUS, July 20, 2016 (percentile ranking of states)



Source: Glassdoor API.

[13] In what follows, each map uses five colors to distinguish five different percentile ranking categories. For example, states colored in the darkest shade of blue are at or above the 95th percentile, which effectively means that these states rank either first or second in whatever value is being measured (total non-cybersecurity job posts in the case of Figure 4).

Table 3. Top 15 states, total non-cybersecurity job posts within CONUS, July 20, 2016

	State	# Posts		State	# Posts		State	# Posts
1	California	901,540	6	Florida	412,075	11	New Jersey	264,633
2	Texas	659,584	7	Ohio	377,895	12	Indiana	252,695
3	Illinois	456,342	8	Virginia	306,445	13	Michigan	238,447
4	Pennsylvania	420,287	9	Georgia	290,338	14	Massachusetts	233,840
5	New York	413,042	10	North Carolina	272,655	15	Missouri	223,993

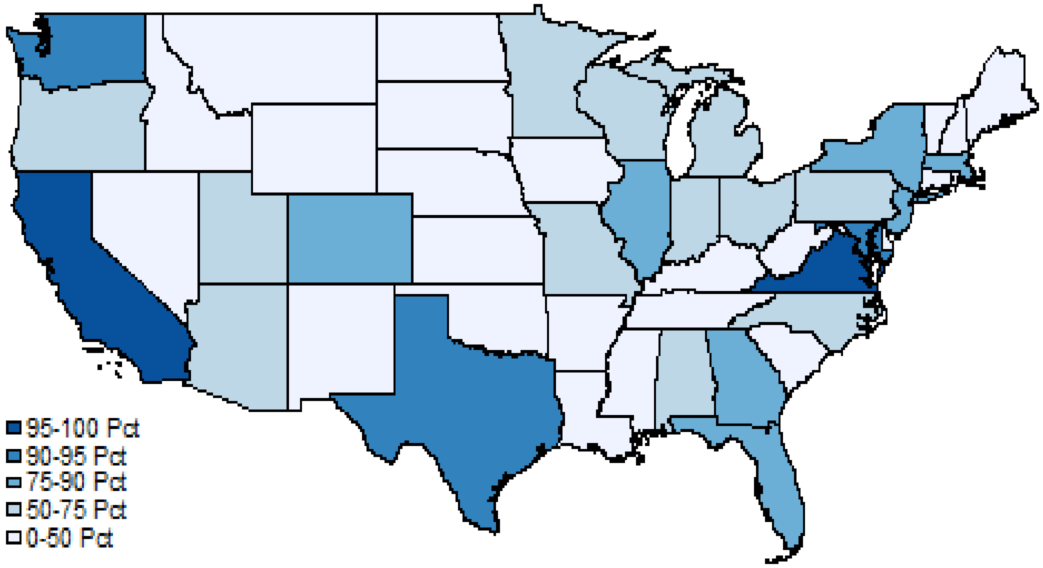
Source: Glassdoor API.

It is not surprising that the states with the most job postings tend to be those with the largest populations. California is in first place with over 900,000 non-cybersecurity posts during the year leading up to July 20, 2016 (when the data were collected), with Texas being a distant second at just under 660,000. Illinois rounds out the top three with about 450,000 posts.

Figure 5 and Table 4 repeat the same exercise for the case of cybersecurity job posts. Once again, California has the most posts, but thereafter the rankings depart significantly from those shown above (for non-cybersecurity posts). Virginia moves from 8th place to 2nd, and Maryland and Washington move from being ranked outside the top 15 to 3rd and 5th (respectively). In contrast, Illinois drops from 3rd to 10th, and Pennsylvania falls outside the top 15. All of these comparisons point to the fact that cybersecurity jobs in the U.S. exhibit a unique geographic distribution.

Although these counts provide some interesting insights, they also obscure important details. For example, one might want to know how important cybersecurity jobs are to a local area's economy, in which case the absolute number of posts may be a poor metric. An alternative would be to look at what percentage of all job posts are for cybersecurity positions since areas where cybersecurity is a bigger part of the local economy are likely to have a relatively high fraction of job posts in this field.

Figure 5. Geographic distribution of all cybersecurity job posts within CONUS, July 20, 2016 (percentile ranking of states)



Source: Glassdoor API.

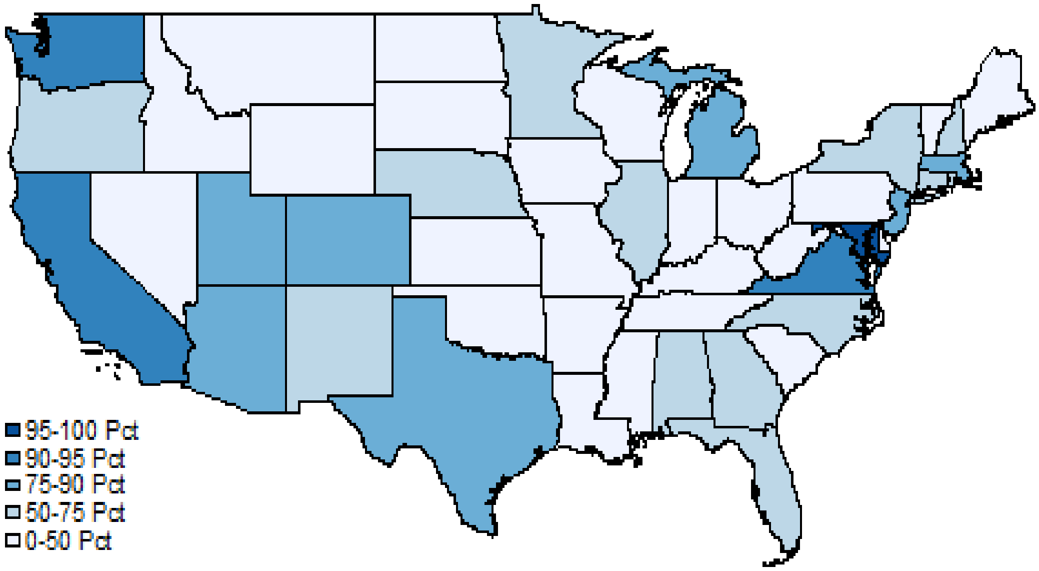
Table 4. Top 15 states, total cybersecurity job posts within CONUS, July 20, 2016

	State	# Posts		State	# Posts		State	# Posts
1	California	25,431	6	New York	5,504	11	Georgia	4,080
2	Virginia	17,641	7	Florida	5,448	12	New Jersey	4,077
3	Maryland	12,994	8	Massachusetts	5,392	13	DC	3,941
4	Texas	9,312	9	Colorado	5,291	14	Michigan	3,518
5	Washington	8,568	10	Illinois	4,778	15	North Carolina	3,432

Source: Glassdoor API.

As Figure 6 and Table 5 make clear, the set of states with a relatively high percentage of cybersecurity job posts differs markedly from the absolute rankings discussed above. For example, in the District of Columbia, 7.7 percent of all job posts are for cybersecurity positions, a full percentage point ahead of the nearest competitor (Maryland). In fact, these data clearly point to the fact that cybersecurity is a dominant industry in the D.C. metropolitan area (including most of Maryland and Northern Virginia), much more so than any other part of the country.

Figure 6. Cybersecurity job posts as a percentage of all job posts, by state within CONUS, July 20, 2016 (percentile ranking of states)



Source: Glassdoor API.

Table 5. Top 15 states, cybersecurity job posts as a percentage of all posts, by state within CONUS, July 20, 2016 (percentile ranking of states)

	State	% Cyber		State	% Cyber		State	% Cyber
1	DC	7.7	6	Colorado	2.5	11	Utah	1.5
2	Maryland	6.7	7	Hawaii	2.5	12	Michigan	1.5
3	Virginia	5.8	8	Massachusetts	2.3	13	TX	1.4
4	Washington	3.9	9	Arizona	1.6	14	Georgia	1.4
5	California	2.8	10	New Jersey	1.5	15	Nebraska	1.3

Source: Glassdoor API.

Results: Top federal departments by cybersecurity job posts

Although the Glassdoor API is a good resource for understanding the geographic distribution of private-sector jobs, it is not equipped to address other questions of interest. From the USAJOBS, however, we built a dataset that can be used to investigate several topics, including which federal departments are trying to hire cybersecurity employees. In Table 6, we list the top 10 departments in our data, ranked according to how many unique cybersecurity postings they had placed on USAJOBS.

Table 6. Rank of federal departments by cybersecurity job posts, July 27, 2016

Rank	Department	Cyber-security Posts	All Posts	Percentage Cyber
1	Army	67	2,692	2.43
2	Air Force	63	1,247	4.81
3	Homeland Security	45	498	8.29
4	Navy	38	804	4.51
5	Veterans Affairs	23	3,670	0.62
6	Defense	19	766	2.42
7	Transportation	10	338	2.87
8	Commerce	10	201	4.74
9	Interior	8	699	1.13
10	Health and Human Services	6	1,113	0.54

Source: USAJOBS.

This table is interesting for several reasons. First, it shows that cybersecurity employees are in high demand across the military, as well as the Department of Homeland Security (DHS). This is not surprising since one can easily imagine why these organizations would be concerned with computer and network security. However, cybersecurity also appears to be important to the Department of Veterans Affairs (VA)—no doubt because it has millions of medical records, which must be securely managed.

Table 6 also reveals that these departments vary considerably in terms of how important cybersecurity is relative to other hiring needs. For example, the Army appears to be the largest cybersecurity employer in the federal government, yet less than 2.5 percent of its job posts are for positions in this area. Conversely, well over 8 percent of all job posts sponsored by DHS are for cybersecurity positions, suggesting that the latter department views cybersecurity as a much higher priority relative to its other hiring needs.

Results: Pay and other job characteristics

Several other useful variables can be generated from the data we scraped from USAJOBS, particularly relating to pay, job status (full-time, part-time, etc.), and job schedule (permanent, temporary etc.). As we show in this subsection, these data reveal fundamental differences between the characteristics of cybersecurity jobs and the remainder of the federal labor market.

Table 7 compares cybersecurity jobs and non-cybersecurity jobs in three distinct categories: pay characteristics, job status, and job schedule. With regard to the first category, it is clear that significantly more cybersecurity positions are advertised as salaried positions (99.6 percent vs. 85.3 percent), and significantly more non-cybersecurity positions offer hourly pay (14.5 percent vs. 0.4 percent). In fact, only 1 of the 251 cybersecurity jobs in the data offers an hourly wage.

Comparing pay levels with the USAJOBS data is somewhat more complicated because every post reports a pay *range*, as opposed to a single value. There is no way of knowing which amount within the reported pay range will actually be the true salary since that number depends in part on the characteristics of the person who is ultimately hired. In light of this, we take the midpoint[14] of each pay range as the best available signal of expected salary and use those data to make the comparisons that follow.

Among salaried workers, we find that cybersecurity jobs in the federal government pay almost $8,000/year more on average, a highly significant difference. Since there is only one cybersecurity job reporting an hourly wage, we cannot make a similar formal comparison for hourly wages. Figure 7 provides greater detail with regard to the distribution of pay for cybersecurity jobs and non-cybersecurity jobs. In these histograms, the jobs included are limited to salaried, full-time workers. For cybersecurity jobs, the bulk of positions seem to be clustered around the $100,000 mark, whereas the non-cybersecurity histogram displays much more density below $100,000. Furthermore, the cybersecurity distribution is much “tighter,” in the sense that there is less salary variation. Also, the non-cybersecurity distribution is less symmetric, due to a pronounced long right tail.

[14] Suppose a given job post advertises a pay range of $80,000 - $100,000. In this case, the midpoint is $\frac{\$80,000+\$100,000}{2}$ = $90,000 (i.e., the point equidistant from both extremes of the range).

Table 7. Pay and other job characteristics for cybersecurity jobs and non-cybersecurity jobs posted on USAJOBS, July 27, 2016[a]

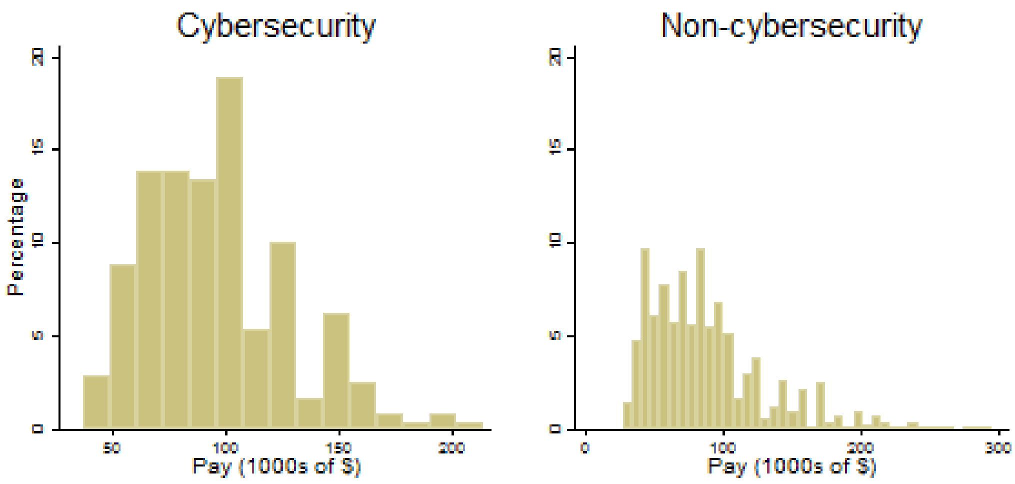
	Non-Cybersecurity	Cybersecurity	Difference	Statistical significance[b]
Wage Characteristics				
Percentage Salaried	85.3	99.6	14.3	***
Average Salary	$88,468	$96,370	$7,902	***
Percentage Hourly	14.5	0.4	-14.1	***
Average Wage	$20.60	$21.80	$1.20	n/a
Job Status				
Full-time	87.7	95.2	7.5	***
Part-time	3.4	0.8	-2.6	**
Other/Unspecified	8.8	4	-4.8	***
Job Schedule				
Permanent	75	81.7	6.6	**
Temporary	7.6	7.2	-0.4	
Intermittent	3.8	0.8	-3	**
Other/Unspecified	14.9	11.6	-3.3	

Source: USAJOBS.

[a] A formal comparison of means could not be made for the average hourly wage because only one cybersecurity job in the data reports an hourly wage.

[b] Levels of significance: ** = 0.05, *** = 0.01.

Figure 7. Histograms of full-time salaries for cybersecurity jobs and non-cybersecurity jobs posted on USAJOBS, July 27, 2016



Source: USAJOBS.

Another dimension in which cybersecurity and non-cybersecurity jobs differ is job-status, as shown in Table 7. Specifically, although full-time employment is far-and-away the most common option in both groups, cybersecurity jobs are 7.5 percentage points more likely to be full-time (95.2 percent vs. 87.7 percent). Correspondingly, non-cybersecurity jobs are more likely to be part-time or "other/unspecified," a group that includes jobs that have flexible hours.

The final category in which we compare cybersecurity and non-cybersecurity jobs is job schedules, a term referring to the duration of the position. In most cases, a job is "permanent," meaning that the position is expected to exist for the foreseeable future. According to our results, cybersecurity positions are significantly more likely to fall into this category (81.7 percent vs. 75 percent). However, a non-trivial minority of jobs in both groups are advertised as "temporary" or "not to exceed" employment, which includes positions that come to a definite end in a specified time period.[15] About 7.6 percent of non-cybersecurity jobs have this schedule, only slightly more than what we see for cybersecurity positions (7.2 percent). Still other positions on USAJOBS are listed as "intermittent," meaning that the position will only be used as needed (e.g., during high-demand periods).[16] Approximately 3.8 percent of non-cybersecurity jobs are intermittent positions, whereas this type of schedule is almost unheard of in cybersecurity (0.8 percent). Finally, a significant minority of jobs in the data have no definite schedule, either because the advertisement was unclear, or because more than one schedule type was available. For the non-cybersecurity group, 14.9 percent of jobs fall into this category; this is 3.3 percentage points higher than what we see for the cybersecurity set (11.6 percent), though the difference is not statistically significant.

Summary

We have applied rather rudimentary data-scraping techniques to two online job forums to produce datasets that shed light on various characteristics of the cybersecurity labor market. CNA researchers should consider other applications of web-scraping of available cybersecurity population information to complement research using more traditional data and methods.

[15] For example, a position might be listed as "full-time, not to exceed 2 years."

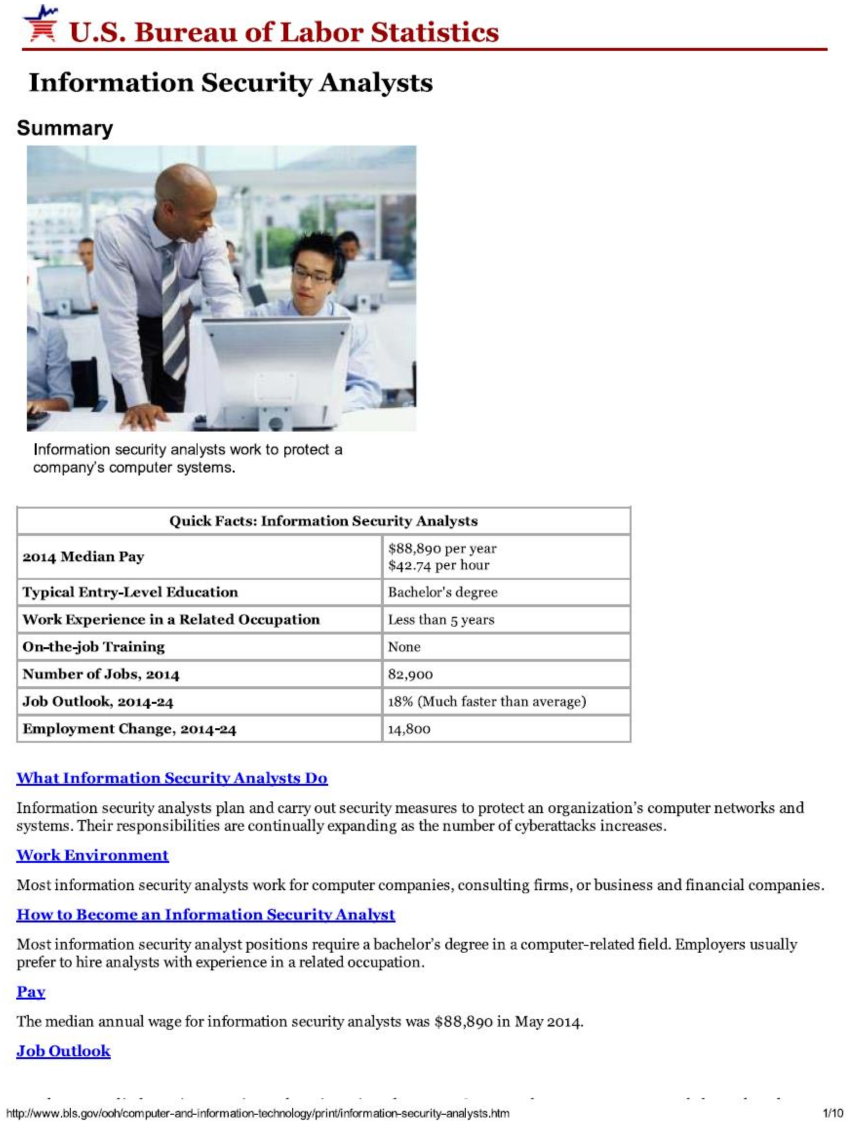
[16] Intermittent should not be confused with "seasonal," another (rare) possibility on USAJOBS. The major difference is that seasonal employment varies in a predictable way, whereas with intermittent employment there are no predefined periods where work will be demanded.

Conclusion

This CNA-initiated study provides CNA analysts with a primer for understanding key aspects of the cybersecurity technician labor market, training and education opportunities, certification levels, and methods for using big data to search for selected cybersecurity technician information. The cybersecurity world is rapidly evolving, and previous literature reviews may quickly become outdated. This resource is intended to help analysts find the most current information about the cybersecurity workforce and should be periodically updated, perhaps as part of the CNA-initiated study process.

Appendix A: Cybersecurity Labor Market

Bureau of Labor Statistics, Employment Projections. (2014). Information Security.



U.S. Bureau of Labor Statistics

Information Security Analysts

Summary

Information security analysts work to protect a company's computer systems.

Quick Facts: Information Security Analysts	
2014 Median Pay	$88,890 per year $42.74 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2014	82,900
Job Outlook, 2014-24	18% (Much faster than average)
Employment Change, 2014-24	14,800

What Information Security Analysts Do

Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increases.

Work Environment

Most information security analysts work for computer companies, consulting firms, or business and financial companies.

How to Become an Information Security Analyst

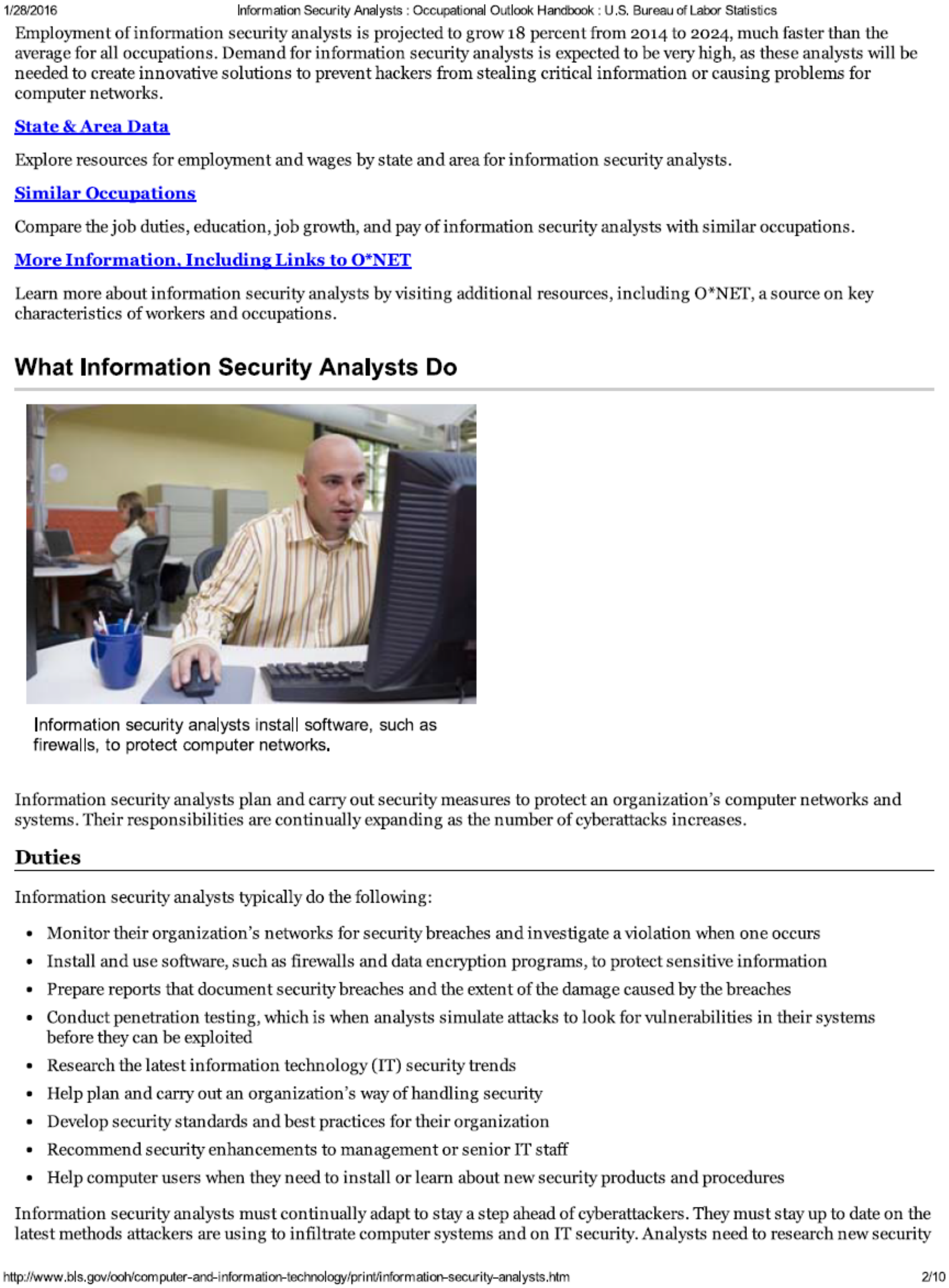
Most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer to hire analysts with experience in a related occupation.

Pay

The median annual wage for information security analysts was $88,890 in May 2014.

Job Outlook

http://www.bls.gov/ooh/computer-and-information-technology/print/information-security-analysts.htm 1/10



1/28/2016 Information Security Analysts : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics

Employment of information security analysts is projected to grow 18 percent from 2014 to 2024, much faster than the average for all occupations. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks.

State & Area Data

Explore resources for employment and wages by state and area for information security analysts.

Similar Occupations

Compare the job duties, education, job growth, and pay of information security analysts with similar occupations.

More Information, Including Links to O*NET

Learn more about information security analysts by visiting additional resources, including O*NET, a source on key characteristics of workers and occupations.

What Information Security Analysts Do

Information security analysts install software, such as firewalls, to protect computer networks.

Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increases.

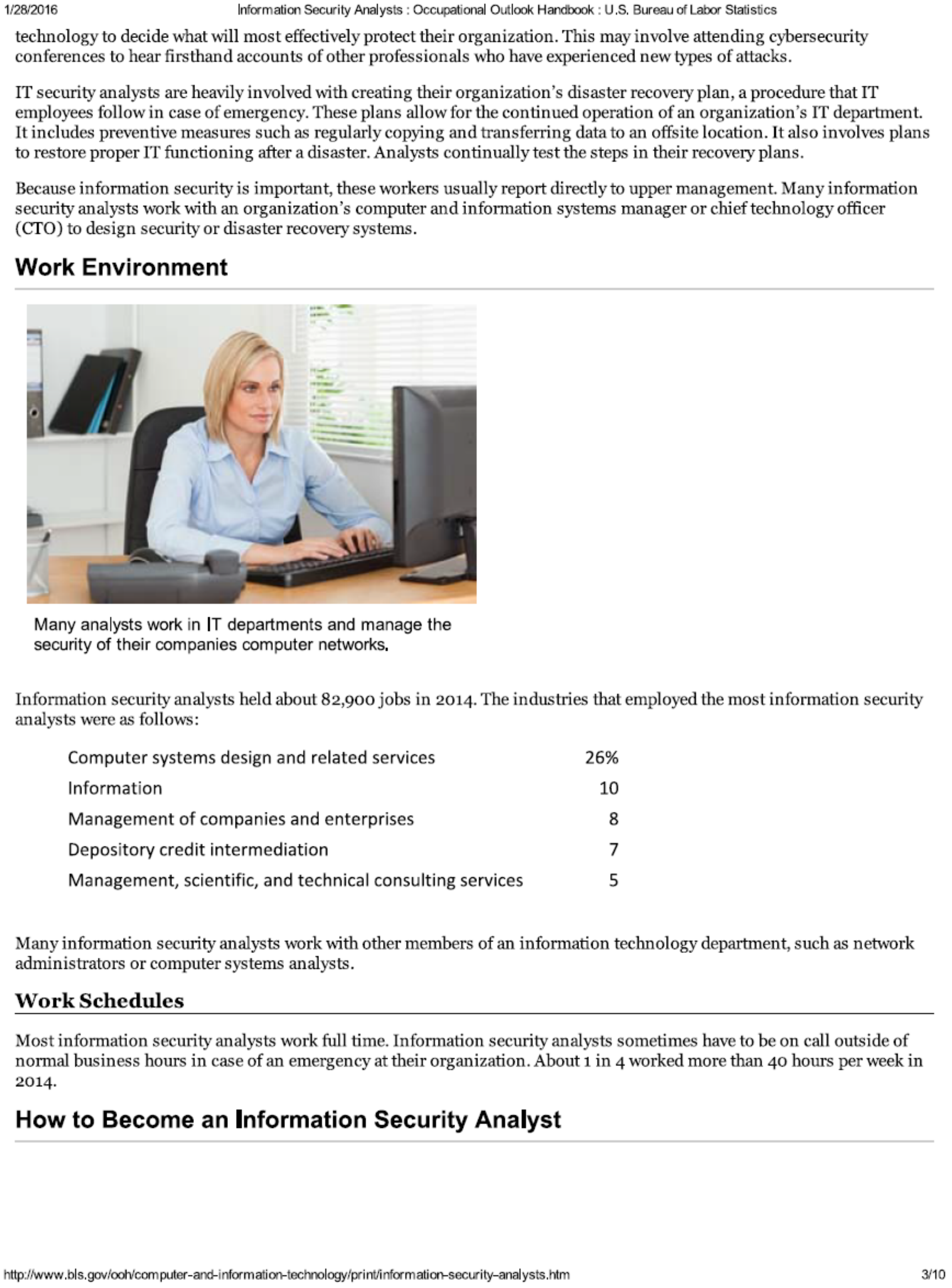
Duties

Information security analysts typically do the following:

- Monitor their organization's networks for security breaches and investigate a violation when one occurs
- Install and use software, such as firewalls and data encryption programs, to protect sensitive information
- Prepare reports that document security breaches and the extent of the damage caused by the breaches
- Conduct penetration testing, which is when analysts simulate attacks to look for vulnerabilities in their systems before they can be exploited
- Research the latest information technology (IT) security trends
- Help plan and carry out an organization's way of handling security
- Develop security standards and best practices for their organization
- Recommend security enhancements to management or senior IT staff
- Help computer users when they need to install or learn about new security products and procedures

Information security analysts must continually adapt to stay a step ahead of cyberattackers. They must stay up to date on the latest methods attackers are using to infiltrate computer systems and on IT security. Analysts need to research new security

http://www.bls.gov/ooh/computer-and-information-technology/print/information-security-analysts.htm 2/10



technology to decide what will most effectively protect their organization. This may involve attending cybersecurity conferences to hear firsthand accounts of other professionals who have experienced new types of attacks.

IT security analysts are heavily involved with creating their organization's disaster recovery plan, a procedure that IT employees follow in case of emergency. These plans allow for the continued operation of an organization's IT department. It includes preventive measures such as regularly copying and transferring data to an offsite location. It also involves plans to restore proper IT functioning after a disaster. Analysts continually test the steps in their recovery plans.

Because information security is important, these workers usually report directly to upper management. Many information security analysts work with an organization's computer and information systems manager or chief technology officer (CTO) to design security or disaster recovery systems.

Work Environment

Many analysts work in IT departments and manage the security of their companies computer networks.

Information security analysts held about 82,900 jobs in 2014. The industries that employed the most information security analysts were as follows:

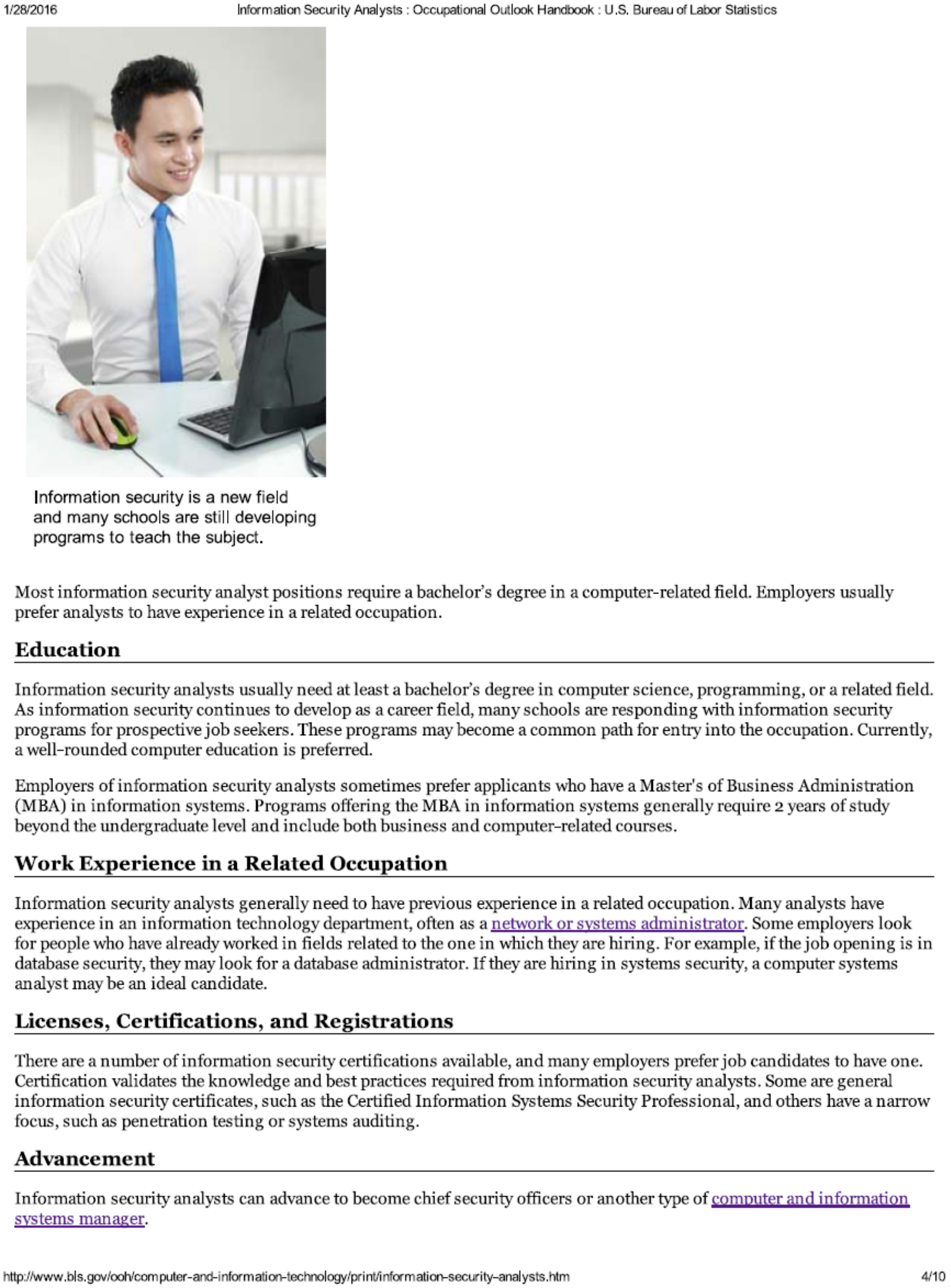
Computer systems design and related services	26%
Information	10
Management of companies and enterprises	8
Depository credit intermediation	7
Management, scientific, and technical consulting services	5

Many information security analysts work with other members of an information technology department, such as network administrators or computer systems analysts.

Work Schedules

Most information security analysts work full time. Information security analysts sometimes have to be on call outside of normal business hours in case of an emergency at their organization. About 1 in 4 worked more than 40 hours per week in 2014.

How to Become an Information Security Analyst



Information security is a new field and many schools are still developing programs to teach the subject.

Most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer analysts to have experience in a related occupation.

Education

Information security analysts usually need at least a bachelor's degree in computer science, programming, or a related field. As information security continues to develop as a career field, many schools are responding with information security programs for prospective job seekers. These programs may become a common path for entry into the occupation. Currently, a well-rounded computer education is preferred.

Employers of information security analysts sometimes prefer applicants who have a Master's of Business Administration (MBA) in information systems. Programs offering the MBA in information systems generally require 2 years of study beyond the undergraduate level and include both business and computer-related courses.

Work Experience in a Related Occupation

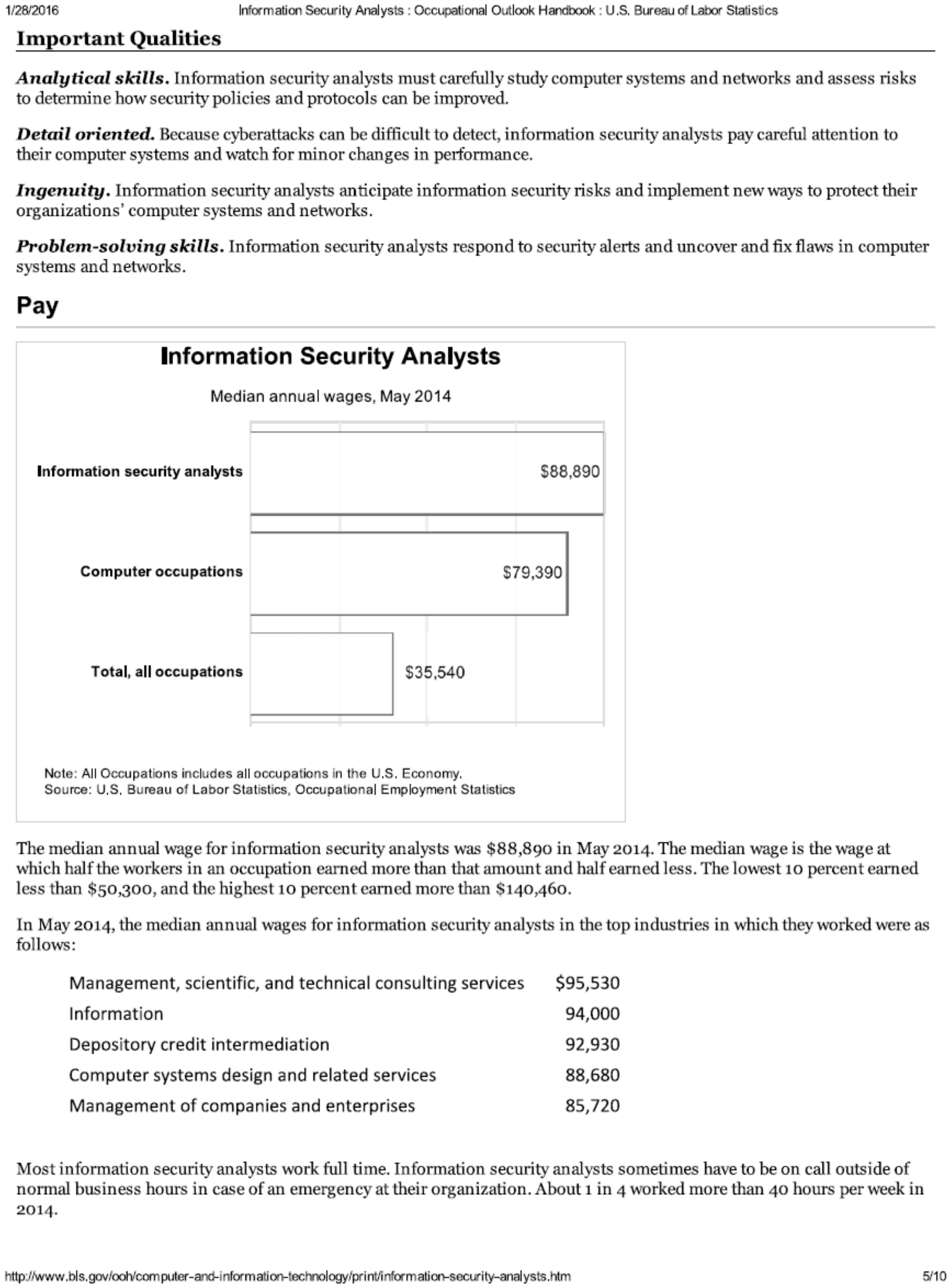
Information security analysts generally need to have previous experience in a related occupation. Many analysts have experience in an information technology department, often as a network or systems administrator. Some employers look for people who have already worked in fields related to the one in which they are hiring. For example, if the job opening is in database security, they may look for a database administrator. If they are hiring in systems security, a computer systems analyst may be an ideal candidate.

Licenses, Certifications, and Registrations

There are a number of information security certifications available, and many employers prefer job candidates to have one. Certification validates the knowledge and best practices required from information security analysts. Some are general information security certificates, such as the Certified Information Systems Security Professional, and others have a narrow focus, such as penetration testing or systems auditing.

Advancement

Information security analysts can advance to become chief security officers or another type of computer and information systems manager.



Important Qualities

Analytical skills. Information security analysts must carefully study computer systems and networks and assess risks to determine how security policies and protocols can be improved.

Detail oriented. Because cyberattacks can be difficult to detect, information security analysts pay careful attention to their computer systems and watch for minor changes in performance.

Ingenuity. Information security analysts anticipate information security risks and implement new ways to protect their organizations' computer systems and networks.

Problem-solving skills. Information security analysts respond to security alerts and uncover and fix flaws in computer systems and networks.

Pay

Information Security Analysts

Median annual wages, May 2014

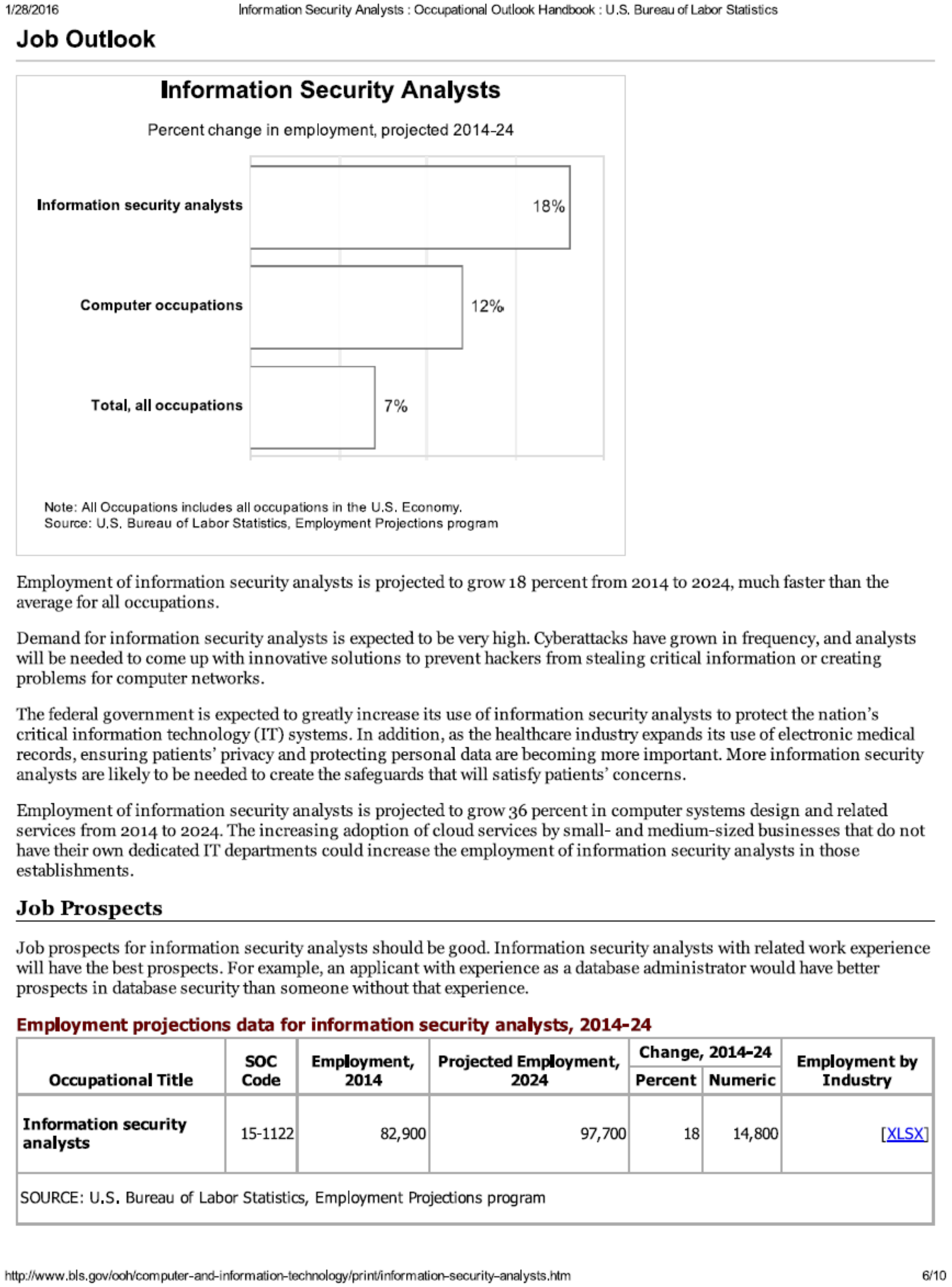
Note: All Occupations includes all occupations in the U.S. Economy.
Source: U.S. Bureau of Labor Statistics, Occupational Employment Statistics

The median annual wage for information security analysts was $88,890 in May 2014. The median wage is the wage at which half the workers in an occupation earned more than that amount and half earned less. The lowest 10 percent earned less than $50,300, and the highest 10 percent earned more than $140,460.

In May 2014, the median annual wages for information security analysts in the top industries in which they worked were as follows:

Management, scientific, and technical consulting services	$95,530
Information	94,000
Depository credit intermediation	92,930
Computer systems design and related services	88,680
Management of companies and enterprises	85,720

Most information security analysts work full time. Information security analysts sometimes have to be on call outside of normal business hours in case of an emergency at their organization. About 1 in 4 worked more than 40 hours per week in 2014.



1/28/2016 Information Security Analysts : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics

Job Outlook

Information Security Analysts
Percent change in employment, projected 2014-24
Information security analysts
18%
Computer occupations
12%
Total, all occupations
7%

Note: All Occupations includes all occupations in the U.S. Economy.
Source: U.S. Bureau of Labor Statistics, Employment Projections program

Employment of information security analysts is projected to grow 18 percent from 2014 to 2024, much faster than the average for all occupations.

Demand for information security analysts is expected to be very high. Cyberattacks have grown in frequency, and analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating problems for computer networks.

The federal government is expected to greatly increase its use of information security analysts to protect the nation's critical information technology (IT) systems. In addition, as the healthcare industry expands its use of electronic medical records, ensuring patients' privacy and protecting personal data are becoming more important. More information security analysts are likely to be needed to create the safeguards that will satisfy patients' concerns.

Employment of information security analysts is projected to grow 36 percent in computer systems design and related services from 2014 to 2024. The increasing adoption of cloud services by small- and medium-sized businesses that do not have their own dedicated IT departments could increase the employment of information security analysts in those establishments.

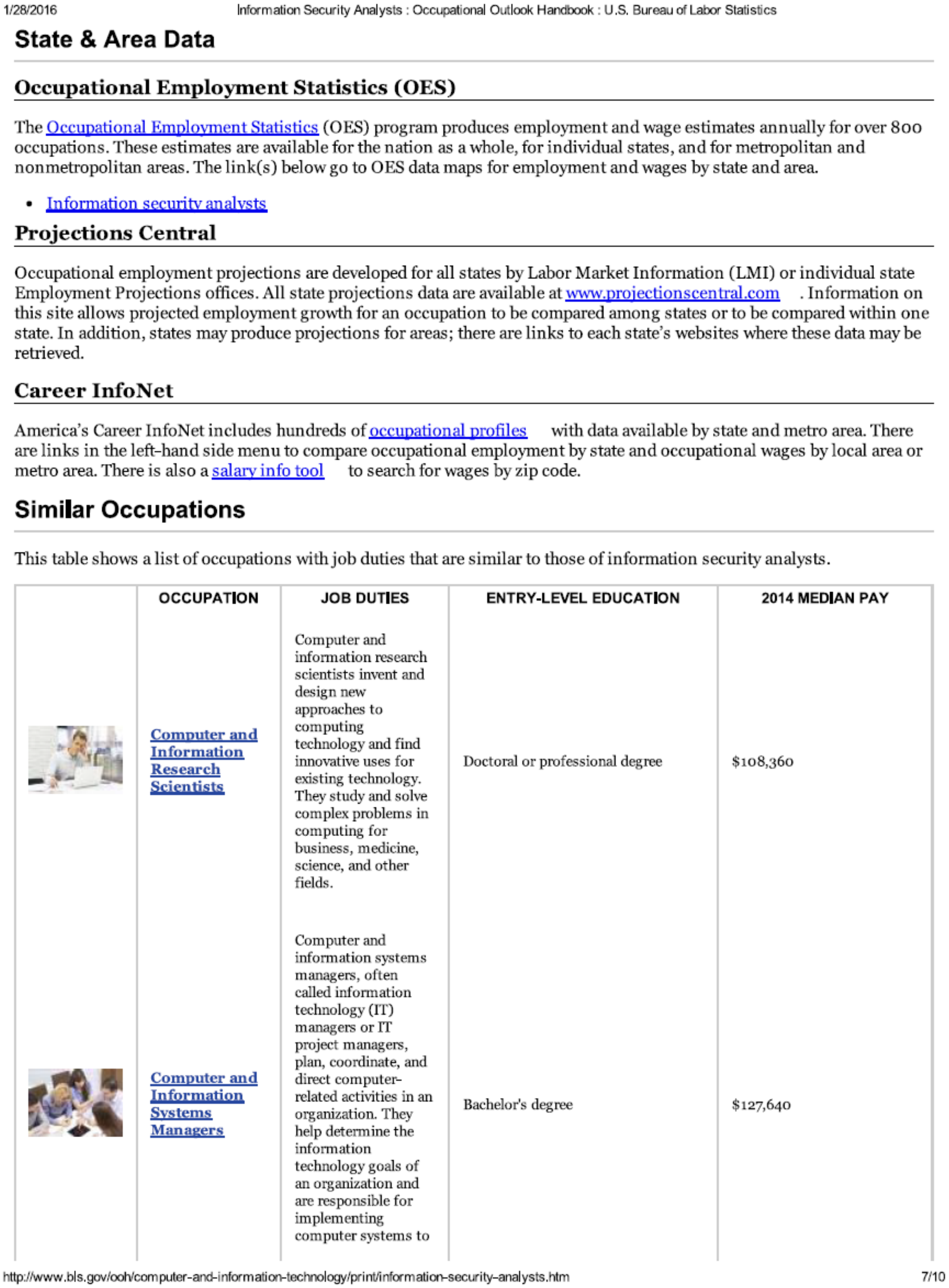
Job Prospects

Job prospects for information security analysts should be good. Information security analysts with related work experience will have the best prospects. For example, an applicant with experience as a database administrator would have better prospects in database security than someone without that experience.

Employment projections data for information security analysts, 2014-24

Occupational Title	SOC Code	Employment, 2014	Projected Employment, 2024	Change, 2014-24		Employment by Industry
				Percent	Numeric	
Information security analysts	15-1122	82,900	97,700	18	14,800	[XLSX]
SOURCE: U.S. Bureau of Labor Statistics, Employment Projections program						

http://www.bls.gov/ooh/computer-and-information-technology/print/information-security-analysts.htm 6/10



State & Area Data

Occupational Employment Statistics (OES)

The Occupational Employment Statistics (OES) program produces employment and wage estimates annually for over 800 occupations. These estimates are available for the nation as a whole, for individual states, and for metropolitan and nonmetropolitan areas. The link(s) below go to OES data maps for employment and wages by state and area.

- Information security analysts

Projections Central

Occupational employment projections are developed for all states by Labor Market Information (LMI) or individual state Employment Projections offices. All state projections data are available at www.projectionscentral.com . Information on this site allows projected employment growth for an occupation to be compared among states or to be compared within one state. In addition, states may produce projections for areas; there are links to each state's websites where these data may be retrieved.

Career InfoNet

America's Career InfoNet includes hundreds of occupational profiles with data available by state and metro area. There are links in the left-hand side menu to compare occupational employment by state and occupational wages by local area or metro area. There is also a salary info tool to search for wages by zip code.

Similar Occupations

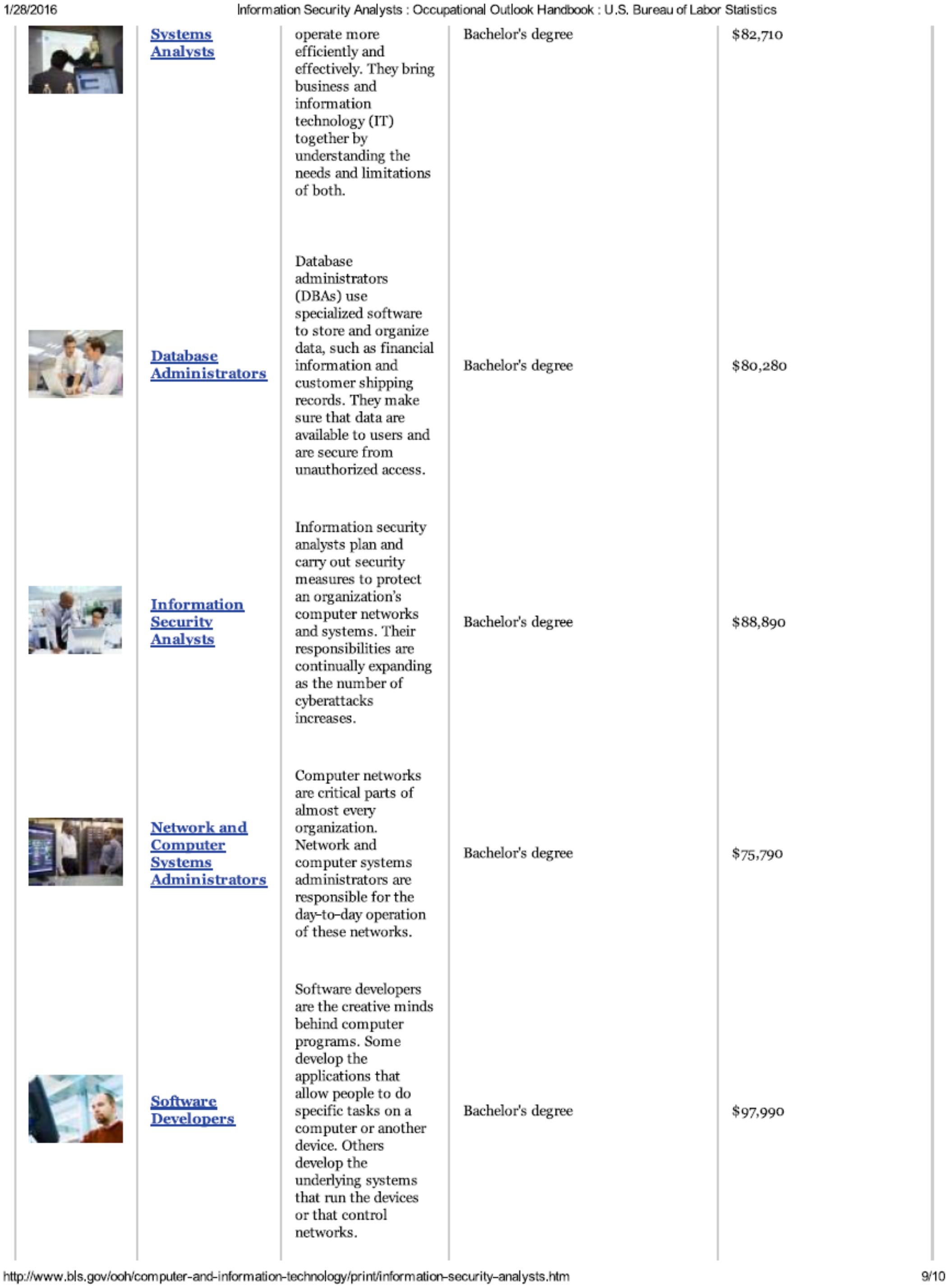
This table shows a list of occupations with job duties that are similar to those of information security analysts.

	OCCUPATION	JOB DUTIES	ENTRY-LEVEL EDUCATION	2014 MEDIAN PAY
	Computer and Information Research Scientists	Computer and information research scientists invent and design new approaches to computing technology and find innovative uses for existing technology. They study and solve complex problems in computing for business, medicine, science, and other fields.	Doctoral or professional degree	$108,360
	Computer and Information Systems Managers	Computer and information systems managers, often called information technology (IT) managers or IT project managers, plan, coordinate, and direct computer-related activities in an organization. They help determine the information technology goals of an organization and are responsible for implementing computer systems to	Bachelor's degree	$127,640

1/28/2016 Information Security Analysts : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics

		meet those goals.		
	Computer Network Architects	Computer network architects design and build data communication networks, including local area networks (LANs), wide area networks (WANs), and intranets. These networks range from small connections between two offices to next-generation networking capabilities such as a cloud infrastructure that serves multiple customers.	Bachelor's degree	$98,430
	Computer Programmers	Computer programmers write and test code that allows computer applications and software programs to function properly. They turn the program designs created by software developers and engineers into instructions that a computer can follow.	Bachelor's degree	$77,550
	Computer Support Specialists	Computer support specialists provide help and advice to people and organizations using computer software or equipment. Some, called computer network support specialists, support information technology (IT) employees within their organization. Others, called computer user support specialists, assist non-IT users who are having computer problems.	See How to Become One	$50,380
	Computer	Computer systems analysts study an organization's current computer systems and procedures and design information systems solutions to help the organization		

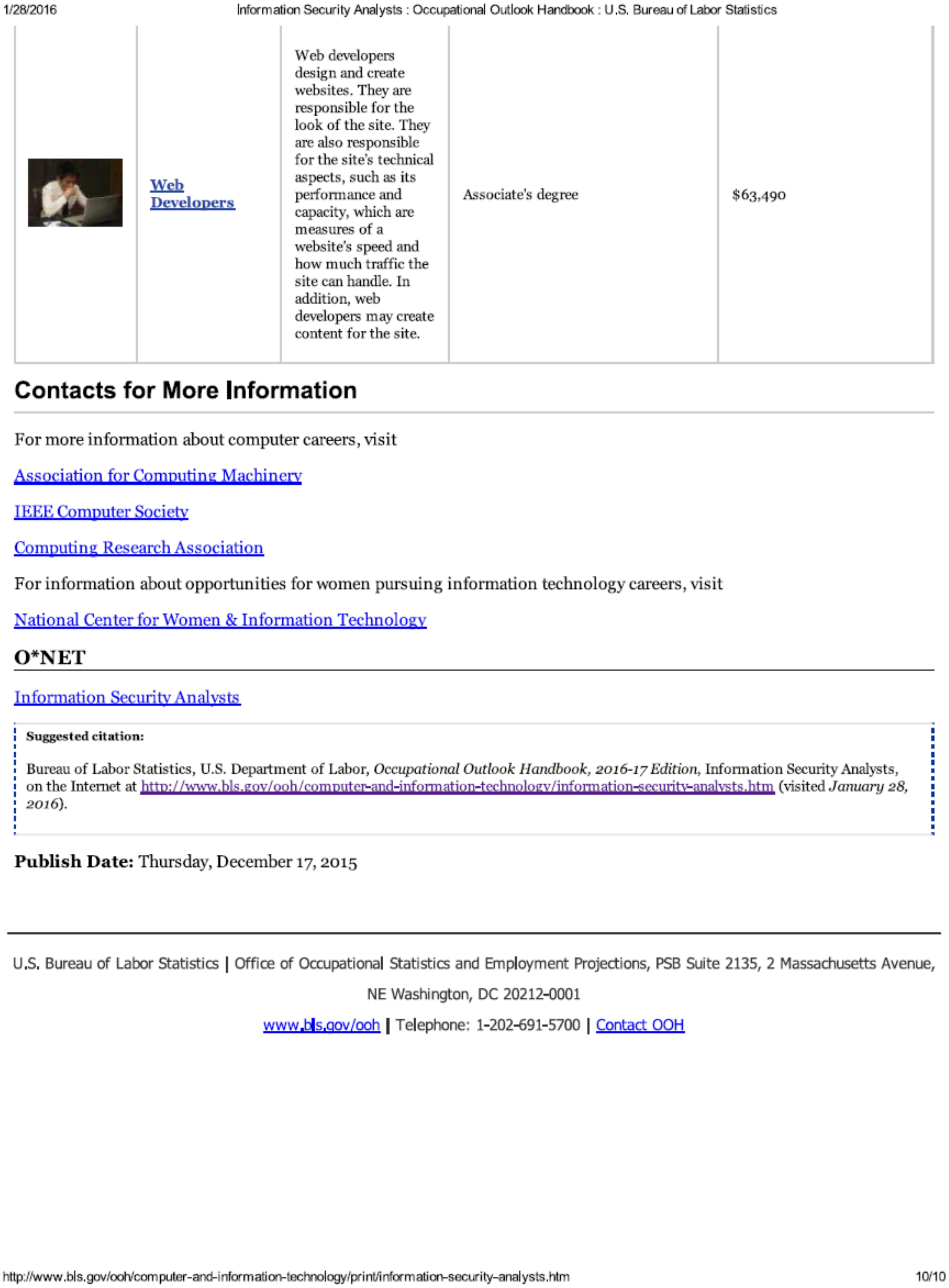
http://www.bls.gov/ooh/computer-and-information-technology/print/information-security-analysts.htm 8/10



1/28/2016 Information Security Analysts : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics

	Systems Analysts	operate more efficiently and effectively. They bring business and information technology (IT) together by understanding the needs and limitations of both.	Bachelor's degree	$82,710
	Database Administrators	Database administrators (DBAs) use specialized software to store and organize data, such as financial information and customer shipping records. They make sure that data are available to users and are secure from unauthorized access.	Bachelor's degree	$80,280
	Information Security Analysts	Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increases.	Bachelor's degree	$88,890
	Network and Computer Systems Administrators	Computer networks are critical parts of almost every organization. Network and computer systems administrators are responsible for the day-to-day operation of these networks.	Bachelor's degree	$75,790
	Software Developers	Software developers are the creative minds behind computer programs. Some develop the applications that allow people to do specific tasks on a computer or another device. Others develop the underlying systems that run the devices or that control networks.	Bachelor's degree	$97,990

http://www.bls.gov/ooh/computer-and-information-technology/print/information-security-analysts.htm 9/10



	Web Developers	Web developers design and create websites. They are responsible for the look of the site. They are also responsible for the site's technical aspects, such as its performance and capacity, which are measures of a website's speed and how much traffic the site can handle. In addition, web developers may create content for the site.	Associate's degree	$63,490

Contacts for More Information

For more information about computer careers, visit

Association for Computing Machinery

IEEE Computer Society

Computing Research Association

For information about opportunities for women pursuing information technology careers, visit

National Center for Women & Information Technology

O*NET

Information Security Analysts

Suggested citation:

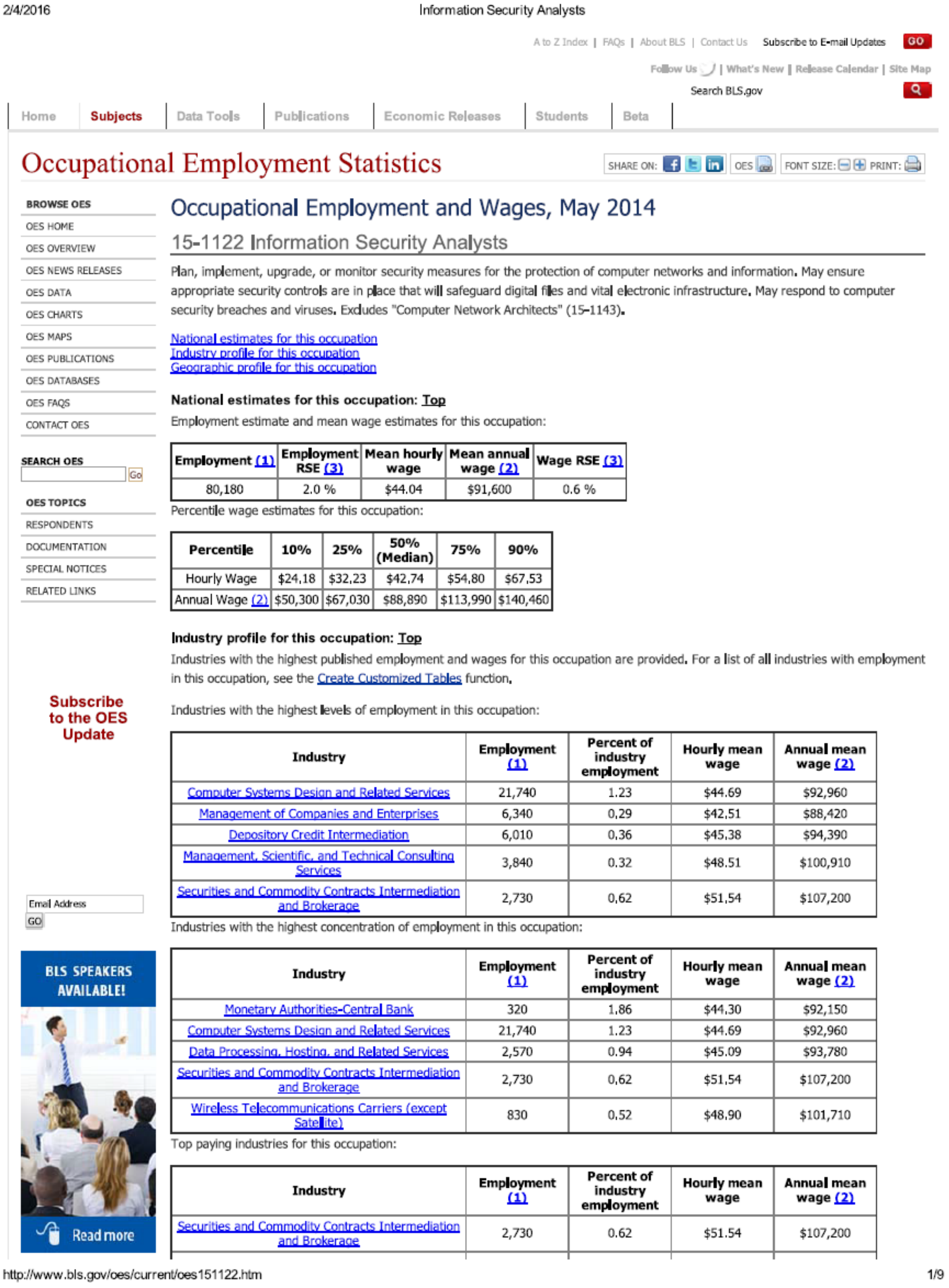
Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook, 2016-17 Edition*, Information Security Analysts, on the Internet at http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visited *January 28, 2016*).

Publish Date: Thursday, December 17, 2015

U.S. Bureau of Labor Statistics | Office of Occupational Statistics and Employment Projections, PSB Suite 2135, 2 Massachusetts Avenue, NE Washington, DC 20212-0001

www.bls.gov/ooh | Telephone: 1-202-691-5700 | Contact OOH

Bureau of Labor Statistics , Occupational Employment Statistics (2014). Occupational Employment and Wages, May 2014. 15-1122 Information Security Analysts.



Occupational Employment Statistics

Occupational Employment and Wages, May 2014

15-1122 Information Security Analysts

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).

National estimates for this occupation
Industry profile for this occupation
Geographic profile for this occupation

National estimates for this occupation: Top

Employment estimate and mean wage estimates for this occupation:

Employment (1)	Employment RSE (3)	Mean hourly wage	Mean annual wage (2)	Wage RSE (3)
80,180	2.0 %	$44.04	$91,600	0.6 %

Percentile wage estimates for this occupation:

Percentile	10%	25%	50% (Median)	75%	90%
Hourly Wage	$24,18	$32,23	$42,74	$54,80	$67,53
Annual Wage (2)	$50,300	$67,030	$88,890	$113,990	$140,460

Industry profile for this occupation: Top

Industries with the highest published employment and wages for this occupation are provided. For a list of all industries with employment in this occupation, see the Create Customized Tables function.

Industries with the highest levels of employment in this occupation:

Industry	Employment (1)	Percent of industry employment	Hourly mean wage	Annual mean wage (2)
Computer Systems Design and Related Services	21,740	1.23	$44.69	$92,960
Management of Companies and Enterprises	6,340	0,29	$42,51	$88,420
Depository Credit Intermediation	6,010	0,36	$45,38	$94,390
Management, Scientific, and Technical Consulting Services	3,840	0.32	$48.51	$100,910
Securities and Commodity Contracts Intermediation and Brokerage	2,730	0,62	$51,54	$107,200

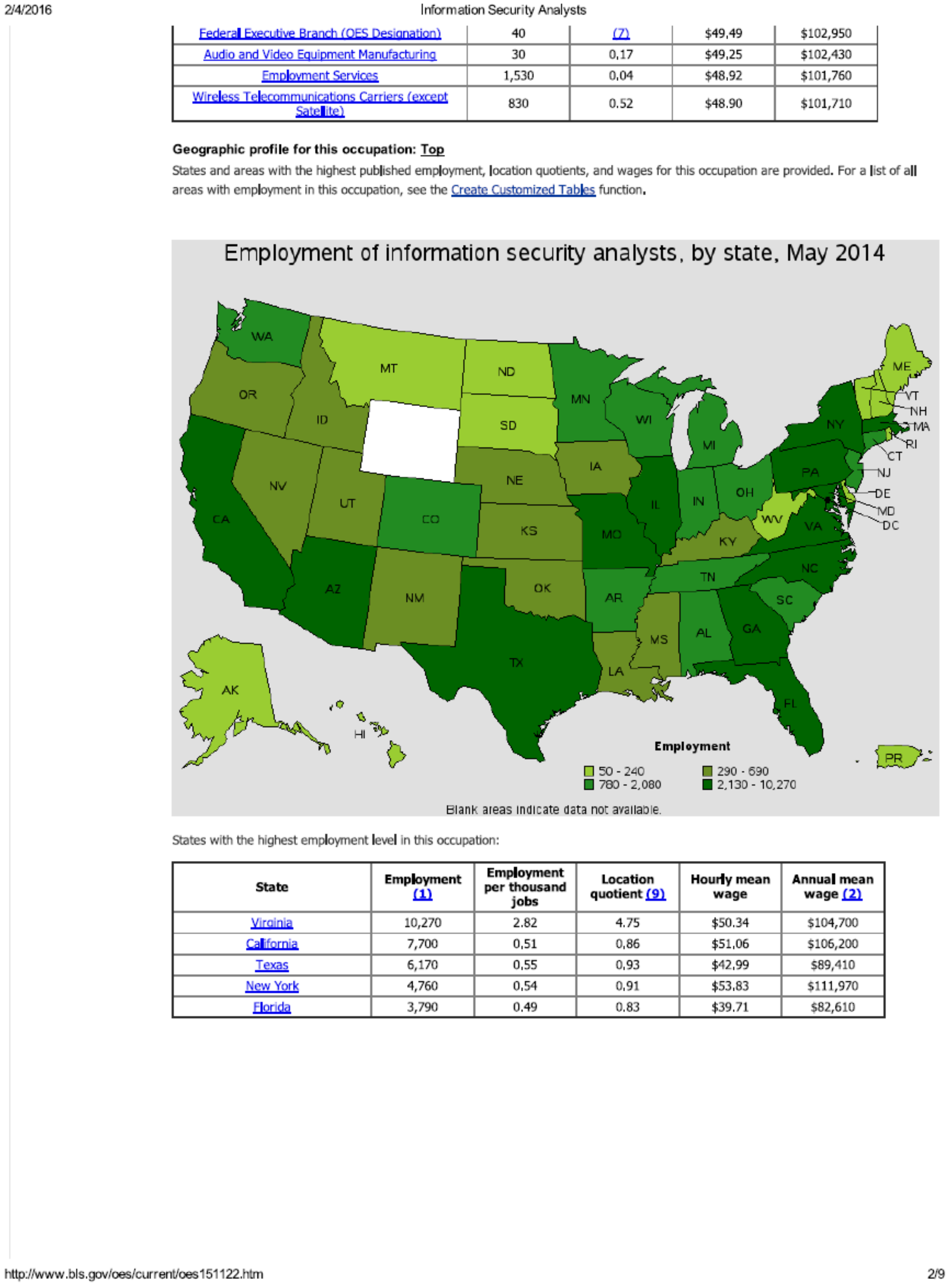
Industries with the highest concentration of employment in this occupation:

Industry	Employment (1)	Percent of industry employment	Hourly mean wage	Annual mean wage (2)
Monetary Authorities-Central Bank	320	1,86	$44,30	$92,150
Computer Systems Design and Related Services	21,740	1.23	$44.69	$92,960
Data Processing, Hosting, and Related Services	2,570	0.94	$45.09	$93,780
Securities and Commodity Contracts Intermediation and Brokerage	2,730	0,62	$51,54	$107,200
Wireless Telecommunications Carriers (except Satellite)	830	0,52	$48,90	$101,710

Top paying industries for this occupation:

Industry	Employment (1)	Percent of industry employment	Hourly mean wage	Annual mean wage (2)
Securities and Commodity Contracts Intermediation and Brokerage	2,730	0.62	$51.54	$107,200

http://www.bls.gov/oes/current/oes151122.htm 1/9



Federal Executive Branch (OES Designation)	40	(7)	$49.49	$102,950
Audio and Video Equipment Manufacturing	30	0.17	$49.25	$102,430
Employment Services	1,530	0.04	$48.92	$101,760
Wireless Telecommunications Carriers (except Satellite)	830	0.52	$48.90	$101,710

Geographic profile for this occupation: Top

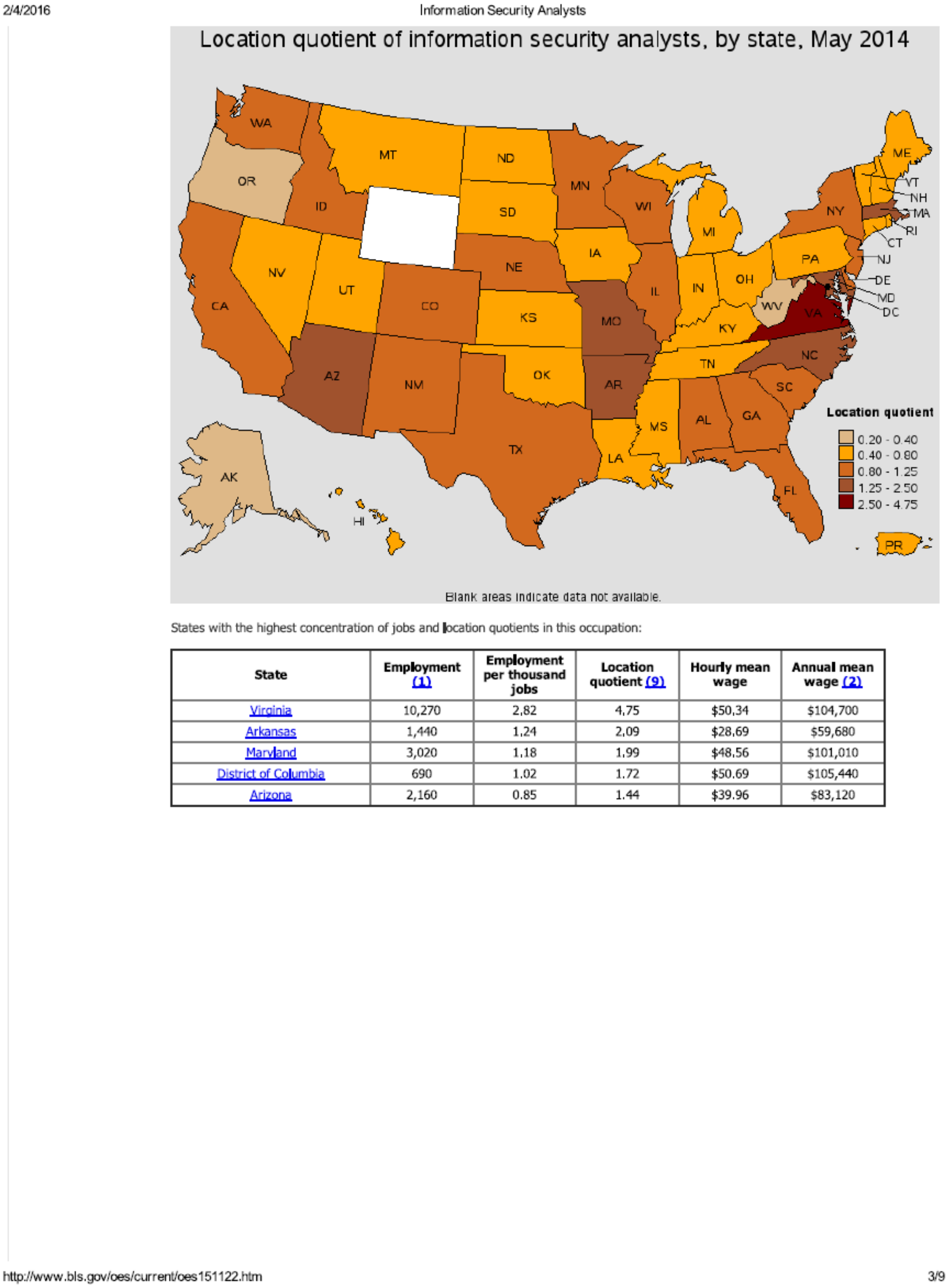
States and areas with the highest published employment, location quotients, and wages for this occupation are provided. For a list of all areas with employment in this occupation, see the Create Customized Tables function.

Employment of information security analysts, by state, May 2014

Blank areas indicate data not available.

States with the highest employment level in this occupation:

State	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
Virginia	10,270	2.82	4.75	$50.34	$104,700
California	7,700	0.51	0.86	$51.06	$106,200
Texas	6,170	0.55	0.93	$42.99	$89,410
New York	4,760	0.54	0.91	$53.83	$111,970
Florida	3,790	0.49	0.83	$39.71	$82,610



2/4/2016 Information Security Analysts

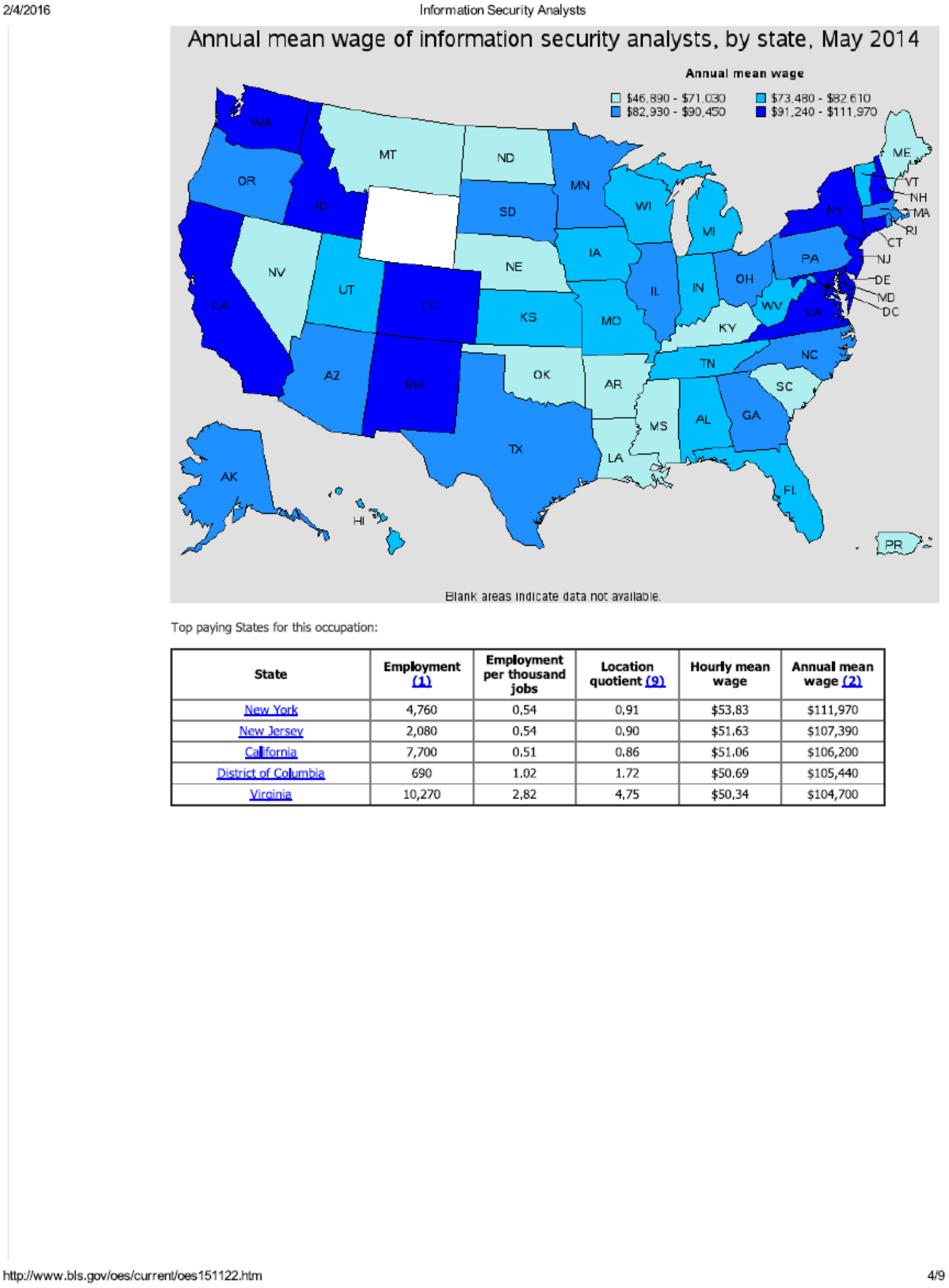
Location quotient of information security analysts, by state, May 2014

Blank areas indicate data not available.

States with the highest concentration of jobs and location quotients in this occupation:

State	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
Virginia	10,270	2,82	4,75	$50,34	$104,700
Arkansas	1,440	1,24	2,09	$28,69	$59,680
Maryland	3,020	1,18	1,99	$48,56	$101,010
District of Columbia	690	1.02	1.72	$50.69	$105,440
Arizona	2,160	0.85	1.44	$39.96	$83,120

http://www.bls.gov/oes/current/oes151122.htm 3/9



2/4/2016 Information Security Analysts

Annual mean wage of information security analysts, by state, May 2014

Annual mean wage

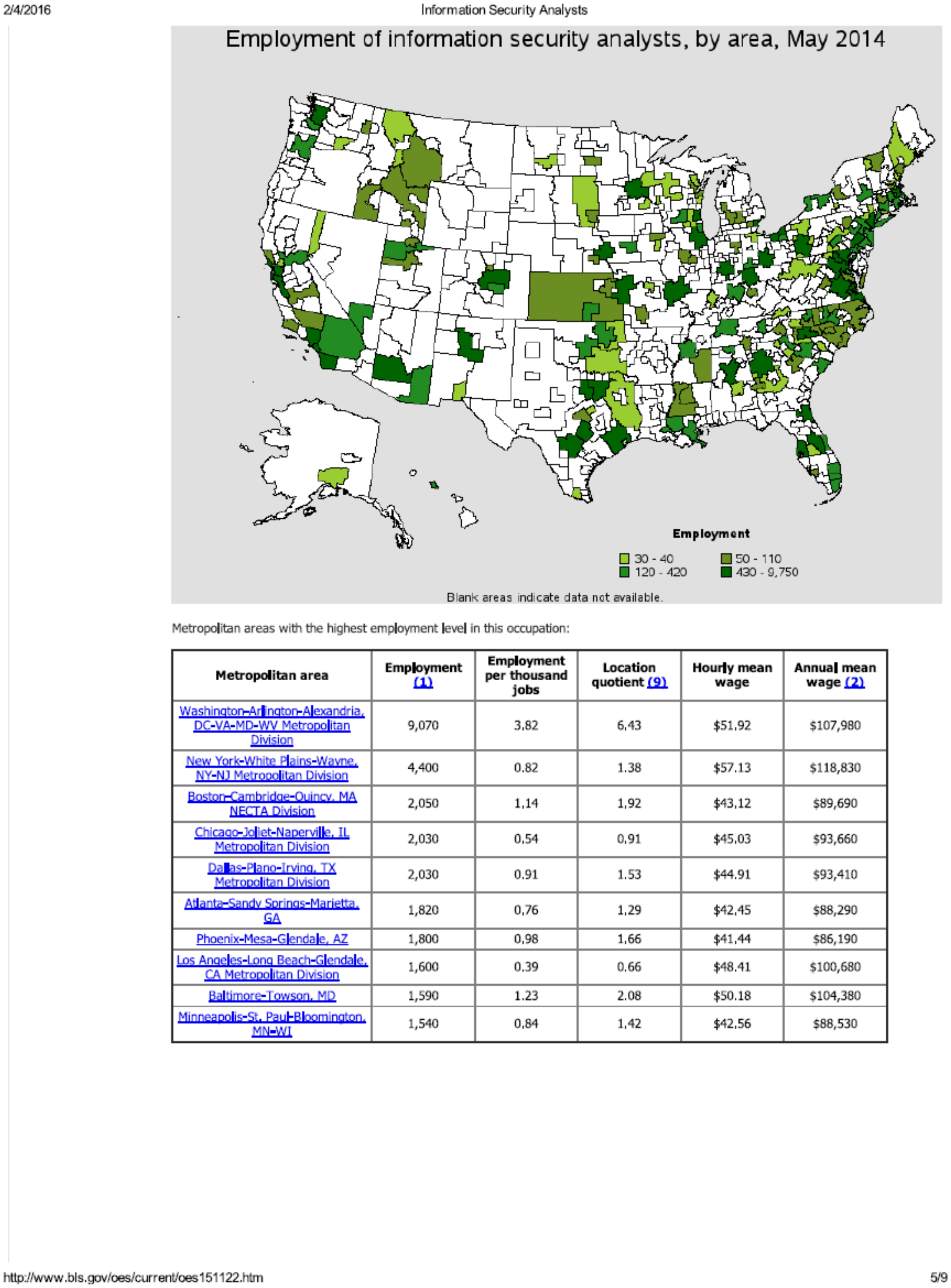
□ $46,890 - $71,030	▨ $73,480 - $82,610
▨ $82,930 - $90,450	■ $91,240 - $111,970

Blank areas indicate data not available.

Top paying States for this occupation:

State	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
New York	4,760	0.54	0.91	$53.83	$111,970
New Jersey	2,080	0.54	0.90	$51.63	$107,390
California	7,700	0.51	0.86	$51.06	$106,200
District of Columbia	690	1.02	1.72	$50.69	$105,440
Virginia	10,270	2.82	4.75	$50.34	$104,700

http://www.bls.gov/oes/current/oes151122.htm 4/9



2/4/2016 Information Security Analysts

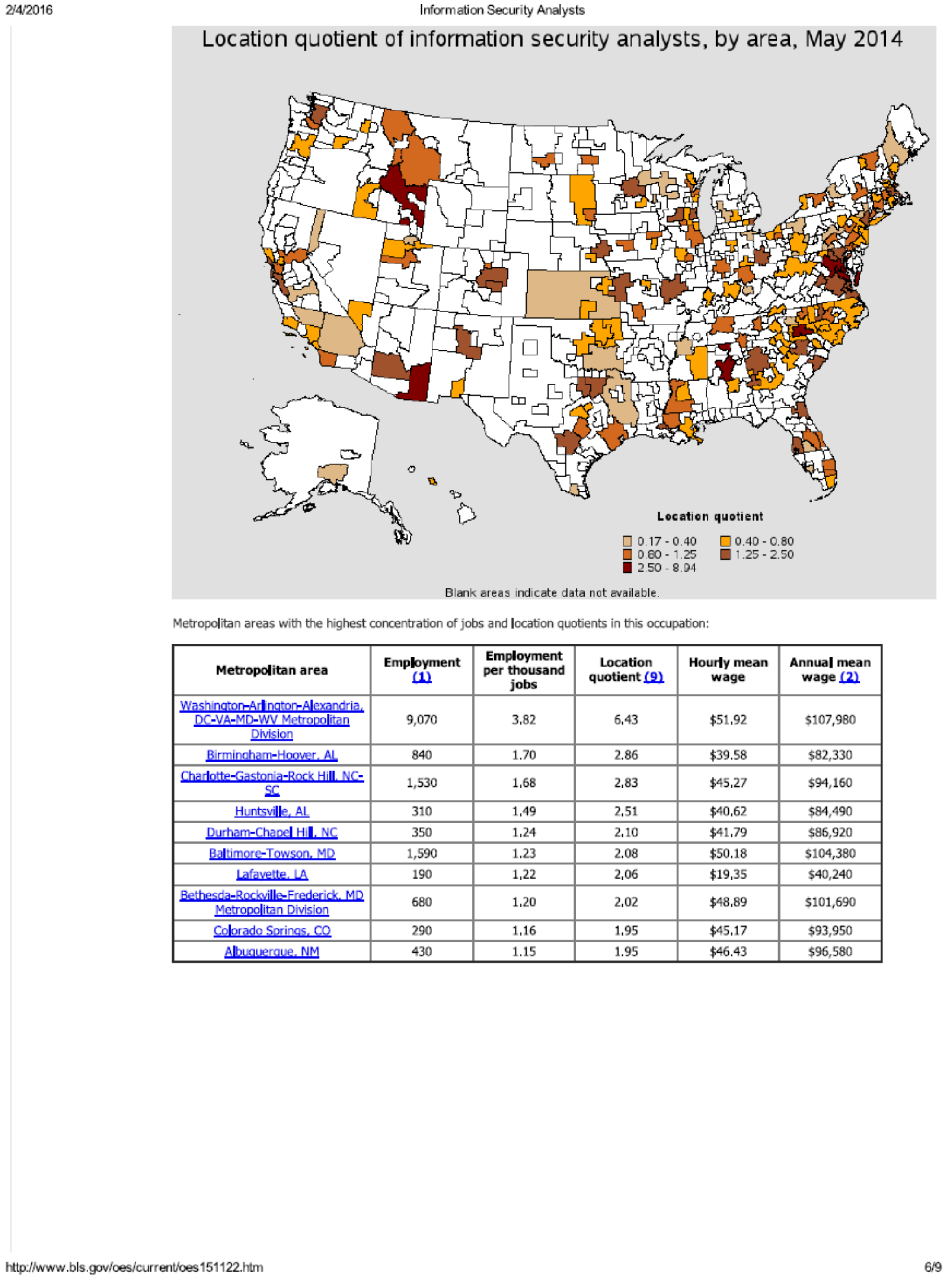
Employment of information security analysts, by area, May 2014

Blank areas indicate data not available.

Metropolitan areas with the highest employment level in this occupation:

Metropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
Washington-Arlington-Alexandria, DC-VA-MD-WV Metropolitan Division	9,070	3.82	6.43	$51.92	$107,980
New York-White Plains-Wayne, NY-NJ Metropolitan Division	4,400	0.82	1.38	$57.13	$118,830
Boston-Cambridge-Quincy, MA NECTA Division	2,050	1.14	1.92	$43.12	$89,690
Chicago-Joliet-Naperville, IL Metropolitan Division	2,030	0.54	0.91	$45.03	$93,660
Dallas-Plano-Irving, TX Metropolitan Division	2,030	0.91	1.53	$44.91	$93,410
Atlanta-Sandy Springs-Marietta, GA	1,820	0.76	1.29	$42.45	$88,290
Phoenix-Mesa-Glendale, AZ	1,800	0.98	1.66	$41.44	$86,190
Los Angeles-Long Beach-Glendale, CA Metropolitan Division	1,600	0.39	0.66	$48.41	$100,680
Baltimore-Towson, MD	1,590	1.23	2.08	$50.18	$104,380
Minneapolis-St. Paul-Bloomington, MN-WI	1,540	0.84	1.42	$42.56	$88,530

http://www.bls.gov/oes/current/oes151122.htm 5/9



2/4/2016 Information Security Analysts

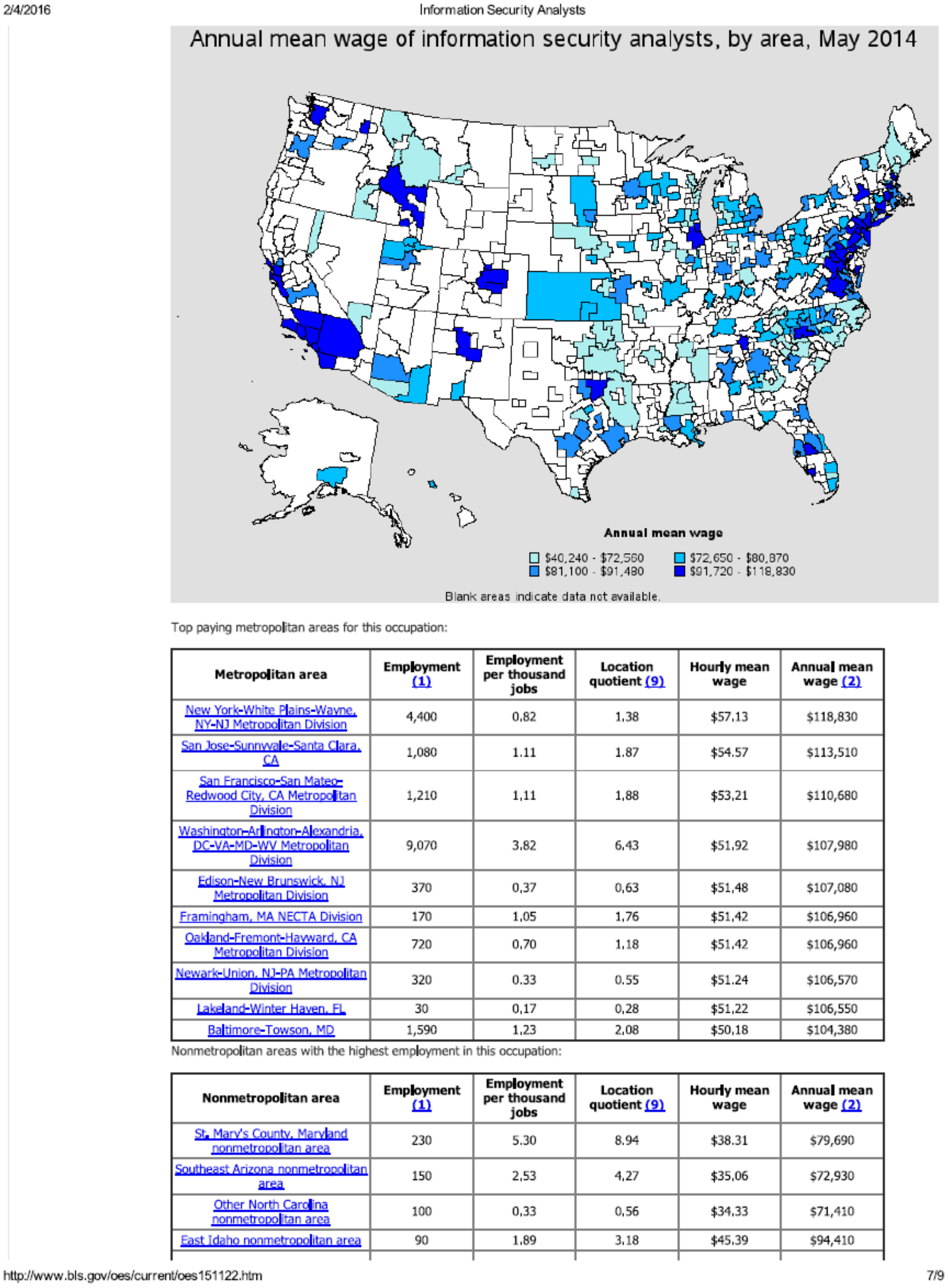
Location quotient of information security analysts, by area, May 2014

Blank areas indicate data not available.

Metropolitan areas with the highest concentration of jobs and location quotients in this occupation:

Metropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
Washington-Arlington-Alexandria, DC-VA-MD-WV Metropolitan Division	9,070	3.82	6.43	$51.92	$107,980
Birmingham-Hoover, AL	840	1.70	2.86	$39.58	$82,330
Charlotte-Gastonia-Rock Hill, NC-SC	1,530	1.68	2.83	$45.27	$94,160
Huntsville, AL	310	1.49	2.51	$40.62	$84,490
Durham-Chapel Hill, NC	350	1.24	2.10	$41.79	$86,920
Baltimore-Towson, MD	1,590	1.23	2.08	$50.18	$104,380
Lafayette, LA	190	1.22	2.06	$19.35	$40,240
Bethesda-Rockville-Frederick, MD Metropolitan Division	680	1.20	2.02	$48.89	$101,690
Colorado Springs, CO	290	1.16	1.95	$45.17	$93,950
Albuquerque, NM	430	1.15	1.95	$46.43	$96,580

http://www.bls.gov/oes/current/oes151122.htm 6/9



2/4/2016 Information Security Analysts

Annual mean wage of information security analysts, by area, May 2014

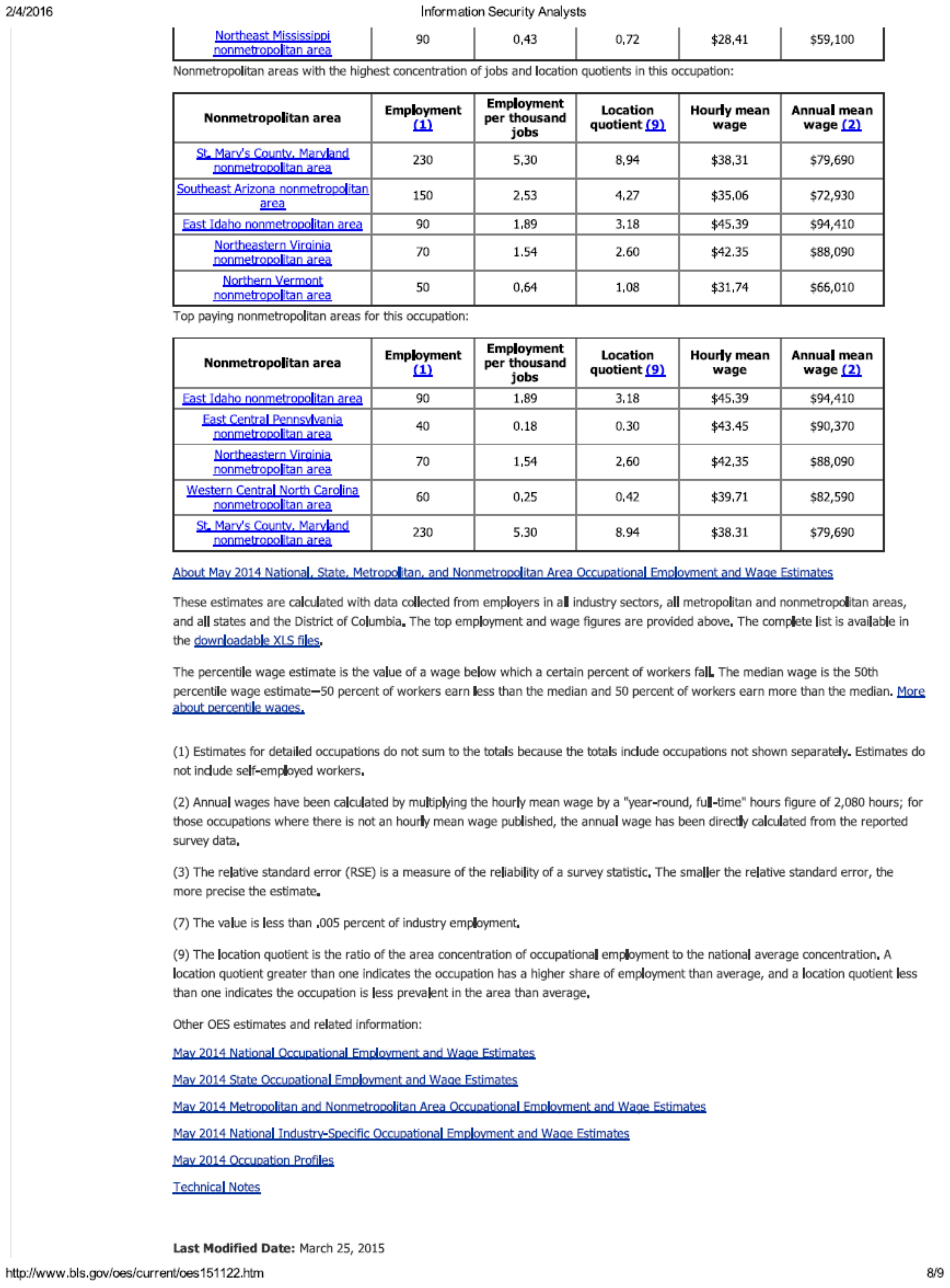
Top paying metropolitan areas for this occupation:

Metropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
New York-White Plains-Wayne, NY-NJ Metropolitan Division	4,400	0.82	1.38	$57.13	$118,830
San Jose-Sunnyvale-Santa Clara, CA	1,080	1.11	1.87	$54.57	$113,510
San Francisco-San Mateo-Redwood City, CA Metropolitan Division	1,210	1.11	1.88	$53.21	$110,680
Washington-Arlington-Alexandria, DC-VA-MD-WV Metropolitan Division	9,070	3.82	6.43	$51.92	$107,980
Edison-New Brunswick, NJ Metropolitan Division	370	0.37	0.63	$51.48	$107,080
Framingham, MA NECTA Division	170	1.05	1.76	$51.42	$106,960
Oakland-Fremont-Hayward, CA Metropolitan Division	720	0.70	1.18	$51.42	$106,960
Newark-Union, NJ-PA Metropolitan Division	320	0.33	0.55	$51.24	$106,570
Lakeland-Winter Haven, FL	30	0.17	0.28	$51.22	$106,550
Baltimore-Towson, MD	1,590	1.23	2.08	$50.18	$104,380

Nonmetropolitan areas with the highest employment in this occupation:

Nonmetropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
St. Mary's County, Maryland nonmetropolitan area	230	5.30	8.94	$38.31	$79,690
Southeast Arizona nonmetropolitan area	150	2.53	4.27	$35.06	$72,930
Other North Carolina nonmetropolitan area	100	0.33	0.56	$34.33	$71,410
East Idaho nonmetropolitan area	90	1.89	3.18	$45.39	$94,410

http://www.bls.gov/oes/current/oes151122.htm 7/9



2/4/2016 Information Security Analysts

Northeast Mississippi nonmetropolitan area	90	0.43	0.72	$28.41	$59,100

Nonmetropolitan areas with the highest concentration of jobs and location quotients in this occupation:

Nonmetropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
St. Mary's County, Maryland nonmetropolitan area	230	5.30	8.94	$38.31	$79,690
Southeast Arizona nonmetropolitan area	150	2.53	4.27	$35.06	$72,930
East Idaho nonmetropolitan area	90	1.89	3.18	$45.39	$94,410
Northeastern Virginia nonmetropolitan area	70	1.54	2.60	$42.35	$88,090
Northern Vermont nonmetropolitan area	50	0.64	1.08	$31.74	$66,010

Top paying nonmetropolitan areas for this occupation:

Nonmetropolitan area	Employment (1)	Employment per thousand jobs	Location quotient (9)	Hourly mean wage	Annual mean wage (2)
East Idaho nonmetropolitan area	90	1.89	3.18	$45.39	$94,410
East Central Pennsylvania nonmetropolitan area	40	0.18	0.30	$43.45	$90,370
Northeastern Virginia nonmetropolitan area	70	1.54	2.60	$42.35	$88,090
Western Central North Carolina nonmetropolitan area	60	0.25	0.42	$39.71	$82,590
St. Mary's County, Maryland nonmetropolitan area	230	5.30	8.94	$38.31	$79,690

About May 2014 National, State, Metropolitan, and Nonmetropolitan Area Occupational Employment and Wage Estimates

These estimates are calculated with data collected from employers in all industry sectors, all metropolitan and nonmetropolitan areas, and all states and the District of Columbia. The top employment and wage figures are provided above. The complete list is available in the downloadable XLS files.

The percentile wage estimate is the value of a wage below which a certain percent of workers fall. The median wage is the 50th percentile wage estimate—50 percent of workers earn less than the median and 50 percent of workers earn more than the median. More about percentile wages.

(1) Estimates for detailed occupations do not sum to the totals because the totals include occupations not shown separately. Estimates do not include self-employed workers.

(2) Annual wages have been calculated by multiplying the hourly mean wage by a "year-round, full-time" hours figure of 2,080 hours; for those occupations where there is not an hourly mean wage published, the annual wage has been directly calculated from the reported survey data.

(3) The relative standard error (RSE) is a measure of the reliability of a survey statistic. The smaller the relative standard error, the more precise the estimate.

(7) The value is less than .005 percent of industry employment.

(9) The location quotient is the ratio of the area concentration of occupational employment to the national average concentration. A location quotient greater than one indicates the occupation has a higher share of employment than average, and a location quotient less than one indicates the occupation is less prevalent in the area than average.

Other OES estimates and related information:

May 2014 National Occupational Employment and Wage Estimates

May 2014 State Occupational Employment and Wage Estimates

May 2014 Metropolitan and Nonmetropolitan Area Occupational Employment and Wage Estimates

May 2014 National Industry-Specific Occupational Employment and Wage Estimates

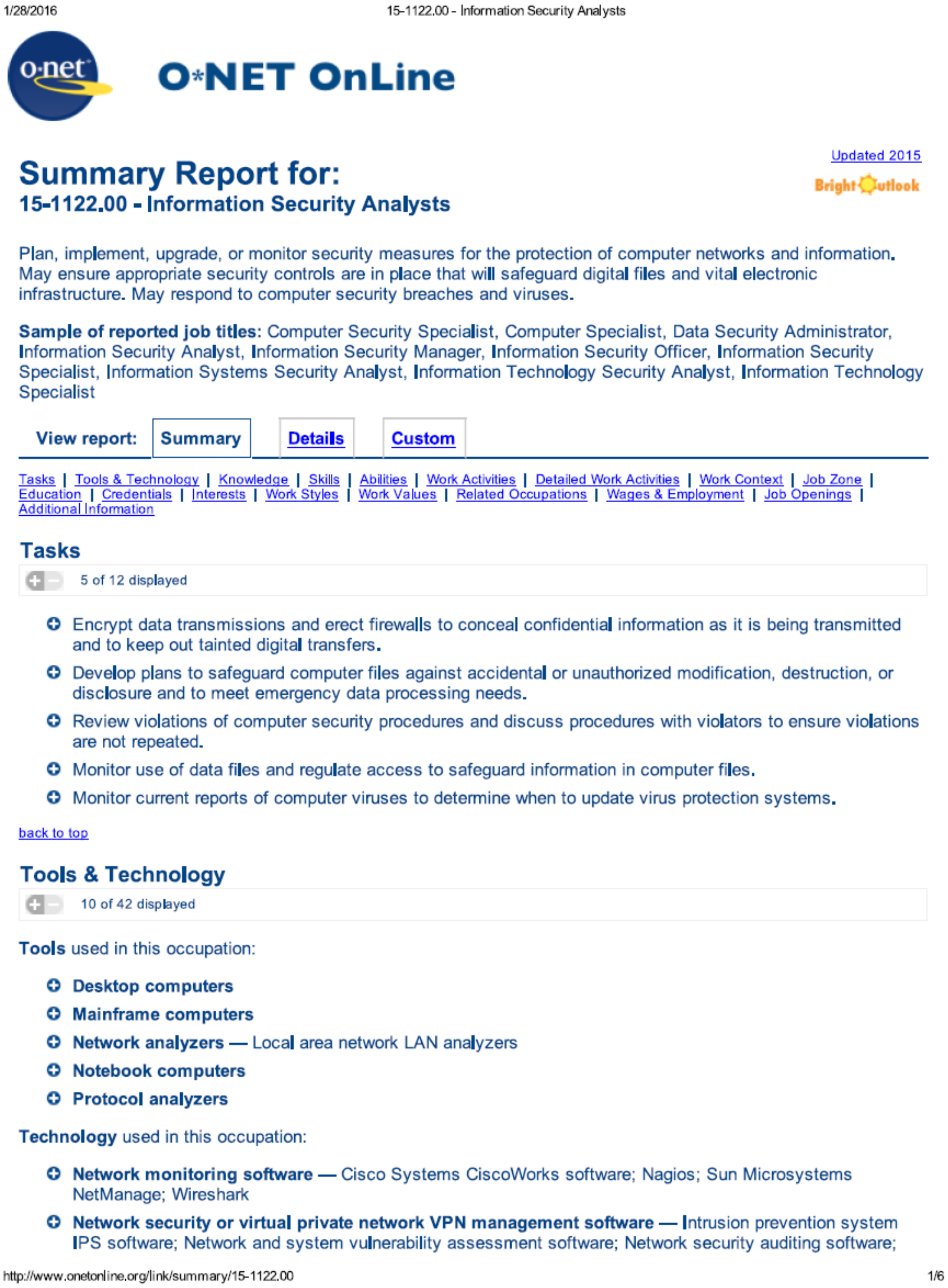
May 2014 Occupation Profiles

Technical Notes

Last Modified Date: March 25, 2015

http://www.bls.gov/oes/current/oes151122.htm 8/9

O*Net Online (2015). Summary Report for: 15-1122.00 - Information Security Analysts



1/28/2016 15-1122.00 - Information Security Analysts

Summary Report for:

15-1122.00 - Information Security Analysts

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.

Sample of reported job titles: Computer Security Specialist, Computer Specialist, Data Security Administrator, Information Security Analyst, Information Security Manager, Information Security Officer, Information Security Specialist, Information Systems Security Analyst, Information Technology Security Analyst, Information Technology Specialist

View report: Summary Details Custom
Tasks | Tools & Technology | Knowledge | Skills | Abilities | Work Activities | Detailed Work Activities | Work Context | Job Zone | Education | Credentials | Interests | Work Styles | Work Values | Related Occupations | Wages & Employment | Job Openings | Additional Information

Tasks

5 of 12 displayed

- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated.
- Monitor use of data files and regulate access to safeguard information in computer files.
- Monitor current reports of computer viruses to determine when to update virus protection systems.

back to top

Tools & Technology

10 of 42 displayed

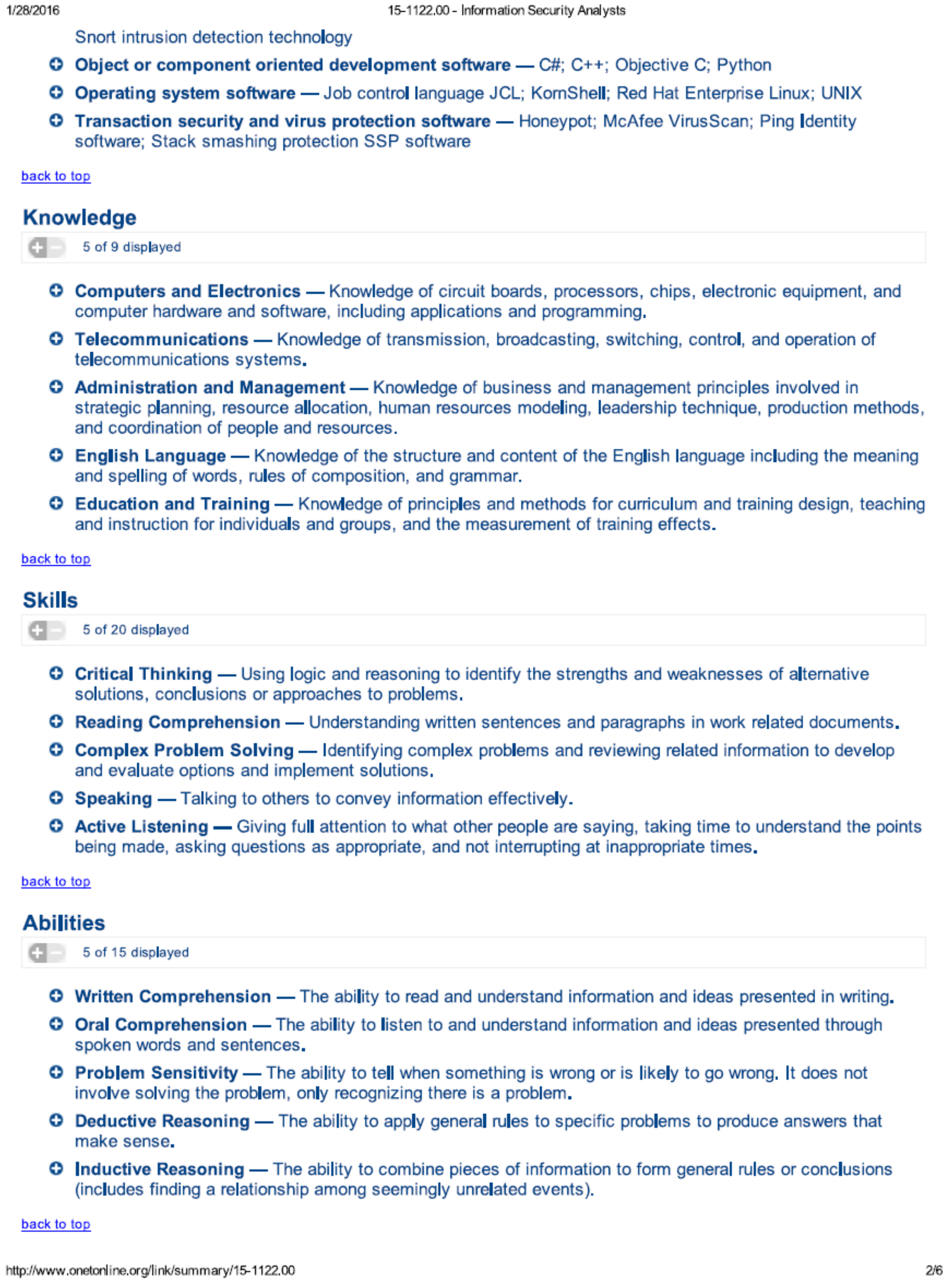
Tools used in this occupation:

- **Desktop computers**
- **Mainframe computers**
- **Network analyzers** — Local area network LAN analyzers
- **Notebook computers**
- **Protocol analyzers**

Technology used in this occupation:

- **Network monitoring software** — Cisco Systems CiscoWorks software; Nagios; Sun Microsystems NetManage; Wireshark
- **Network security or virtual private network VPN management software** — Intrusion prevention system IPS software; Network and system vulnerability assessment software; Network security auditing software;

http://www.onetonline.org/link/summary/15-1122.00 1/6



1/28/2016 15-1122.00 - Information Security Analysts

Snort intrusion detection technology

- **Object or component oriented development software** — C#; C++; Objective C; Python
- **Operating system software** — Job control language JCL; KornShell; Red Hat Enterprise Linux; UNIX
- **Transaction security and virus protection software** — Honeypot; McAfee VirusScan; Ping Identity software; Stack smashing protection SSP software

back to top

Knowledge

5 of 9 displayed

- **Computers and Electronics** — Knowledge of circuit boards, processors, chips, electronic equipment, and computer hardware and software, including applications and programming.
- **Telecommunications** — Knowledge of transmission, broadcasting, switching, control, and operation of telecommunications systems.
- **Administration and Management** — Knowledge of business and management principles involved in strategic planning, resource allocation, human resources modeling, leadership technique, production methods, and coordination of people and resources.
- **English Language** — Knowledge of the structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.
- **Education and Training** — Knowledge of principles and methods for curriculum and training design, teaching and instruction for individuals and groups, and the measurement of training effects.

back to top

Skills

5 of 20 displayed

- **Critical Thinking** — Using logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.
- **Reading Comprehension** — Understanding written sentences and paragraphs in work related documents.
- **Complex Problem Solving** — Identifying complex problems and reviewing related information to develop and evaluate options and implement solutions.
- **Speaking** — Talking to others to convey information effectively.
- **Active Listening** — Giving full attention to what other people are saying, taking time to understand the points being made, asking questions as appropriate, and not interrupting at inappropriate times.

back to top

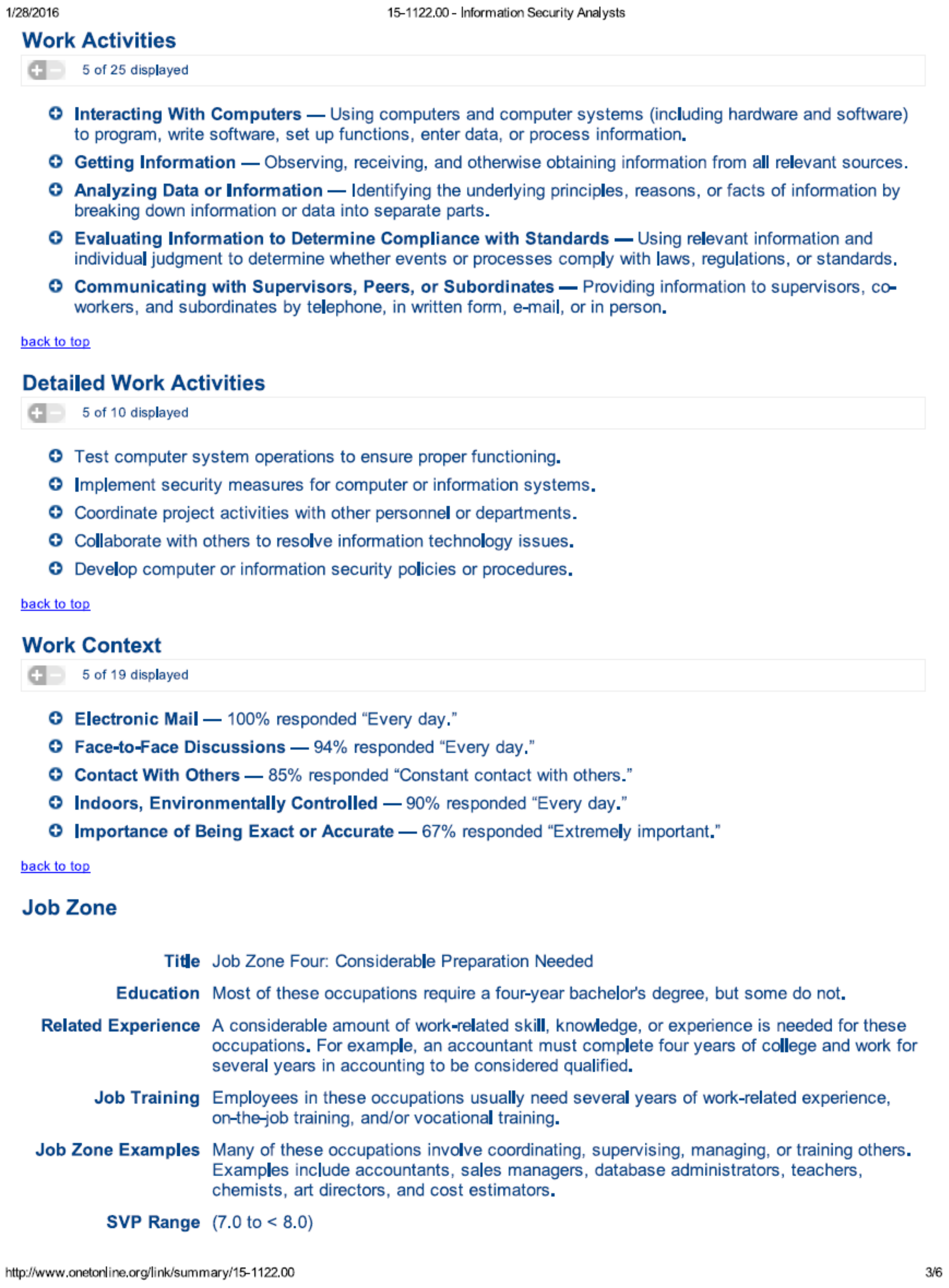
Abilities

5 of 15 displayed

- **Written Comprehension** — The ability to read and understand information and ideas presented in writing.
- **Oral Comprehension** — The ability to listen to and understand information and ideas presented through spoken words and sentences.
- **Problem Sensitivity** — The ability to tell when something is wrong or is likely to go wrong. It does not involve solving the problem, only recognizing there is a problem.
- **Deductive Reasoning** — The ability to apply general rules to specific problems to produce answers that make sense.
- **Inductive Reasoning** — The ability to combine pieces of information to form general rules or conclusions (includes finding a relationship among seemingly unrelated events).

back to top

http://www.onetonline.org/link/summary/15-1122.00 2/6



Work Activities

⊕ ⊖ 5 of 25 displayed

- **Interacting With Computers —** Using computers and computer systems (including hardware and software) to program, write software, set up functions, enter data, or process information.
- **Getting Information —** Observing, receiving, and otherwise obtaining information from all relevant sources.
- **Analyzing Data or Information —** Identifying the underlying principles, reasons, or facts of information by breaking down information or data into separate parts.
- **Evaluating Information to Determine Compliance with Standards —** Using relevant information and individual judgment to determine whether events or processes comply with laws, regulations, or standards.
- **Communicating with Supervisors, Peers, or Subordinates —** Providing information to supervisors, co-workers, and subordinates by telephone, in written form, e-mail, or in person.

back to top

Detailed Work Activities

⊕ ⊖ 5 of 10 displayed

- Test computer system operations to ensure proper functioning.
- Implement security measures for computer or information systems.
- Coordinate project activities with other personnel or departments.
- Collaborate with others to resolve information technology issues.
- Develop computer or information security policies or procedures.

back to top

Work Context

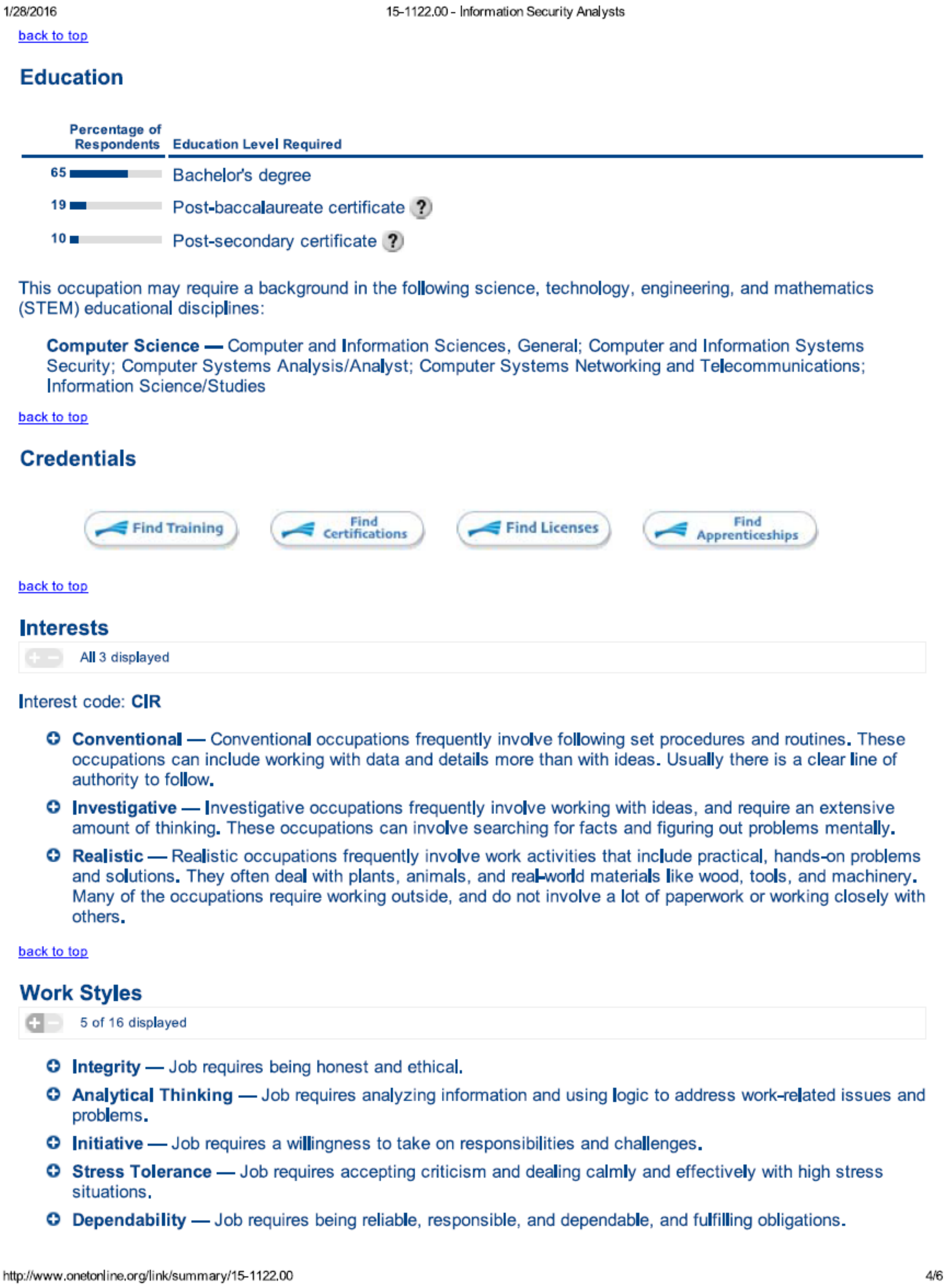
⊕ ⊖ 5 of 19 displayed

- **Electronic Mail —** 100% responded "Every day."
- **Face-to-Face Discussions —** 94% responded "Every day."
- **Contact With Others —** 85% responded "Constant contact with others."
- **Indoors, Environmentally Controlled —** 90% responded "Every day."
- **Importance of Being Exact or Accurate —** 67% responded "Extremely important."

back to top

Job Zone

Title	Job Zone Four: Considerable Preparation Needed
Education	Most of these occupations require a four-year bachelor's degree, but some do not.
Related Experience	A considerable amount of work-related skill, knowledge, or experience is needed for these occupations. For example, an accountant must complete four years of college and work for several years in accounting to be considered qualified.
Job Training	Employees in these occupations usually need several years of work-related experience, on-the-job training, and/or vocational training.
Job Zone Examples	Many of these occupations involve coordinating, supervising, managing, or training others. Examples include accountants, sales managers, database administrators, teachers, chemists, art directors, and cost estimators.
SVP Range	(7.0 to < 8.0)



1/28/2016 15-1122.00 - Information Security Analysts

back to top

Education

Percentage of Respondents	Education Level Required
65	Bachelor's degree
19	Post-baccalaureate certificate ?
10	Post-secondary certificate ?

This occupation may require a background in the following science, technology, engineering, and mathematics (STEM) educational disciplines:

Computer Science — Computer and Information Sciences, General; Computer and Information Systems Security; Computer Systems Analysis/Analyst; Computer Systems Networking and Telecommunications; Information Science/Studies

back to top

Credentials

Find Training | Find Certifications | Find Licenses | Find Apprenticeships

back to top

Interests

All 3 displayed

Interest code: **CIR**

- **Conventional —** Conventional occupations frequently involve following set procedures and routines. These occupations can include working with data and details more than with ideas. Usually there is a clear line of authority to follow.
- **Investigative —** Investigative occupations frequently involve working with ideas, and require an extensive amount of thinking. These occupations can involve searching for facts and figuring out problems mentally.
- **Realistic —** Realistic occupations frequently involve work activities that include practical, hands-on problems and solutions. They often deal with plants, animals, and real-world materials like wood, tools, and machinery. Many of the occupations require working outside, and do not involve a lot of paperwork or working closely with others.

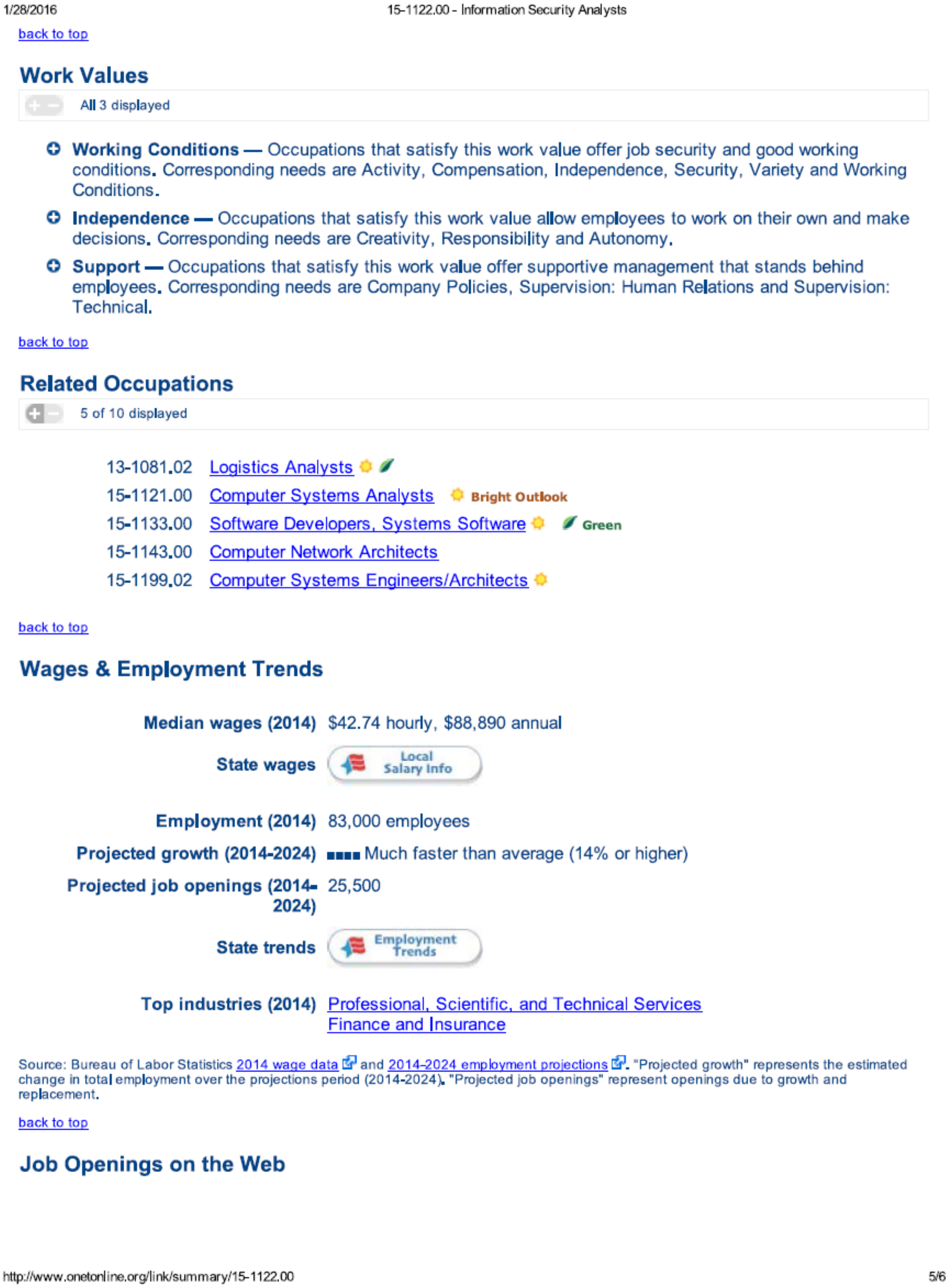
back to top

Work Styles

5 of 16 displayed

- **Integrity —** Job requires being honest and ethical.
- **Analytical Thinking —** Job requires analyzing information and using logic to address work-related issues and problems.
- **Initiative —** Job requires a willingness to take on responsibilities and challenges.
- **Stress Tolerance —** Job requires accepting criticism and dealing calmly and effectively with high stress situations.
- **Dependability —** Job requires being reliable, responsible, and dependable, and fulfilling obligations.

http://www.onetonline.org/link/summary/15-1122.00 4/6



1/28/2016 15-1122.00 - Information Security Analysts

back to top

Work Values

All 3 displayed

- **Working Conditions —** Occupations that satisfy this work value offer job security and good working conditions. Corresponding needs are Activity, Compensation, Independence, Security, Variety and Working Conditions.
- **Independence —** Occupations that satisfy this work value allow employees to work on their own and make decisions. Corresponding needs are Creativity, Responsibility and Autonomy.
- **Support —** Occupations that satisfy this work value offer supportive management that stands behind employees. Corresponding needs are Company Policies, Supervision: Human Relations and Supervision: Technical.

back to top

Related Occupations

5 of 10 displayed

13-1081.02	Logistics Analysts ☀ 🌿
15-1121.00	Computer Systems Analysts ☀ Bright Outlook
15-1133.00	Software Developers, Systems Software ☀ 🌿 Green
15-1143.00	Computer Network Architects
15-1199.02	Computer Systems Engineers/Architects ☀

back to top

Wages & Employment Trends

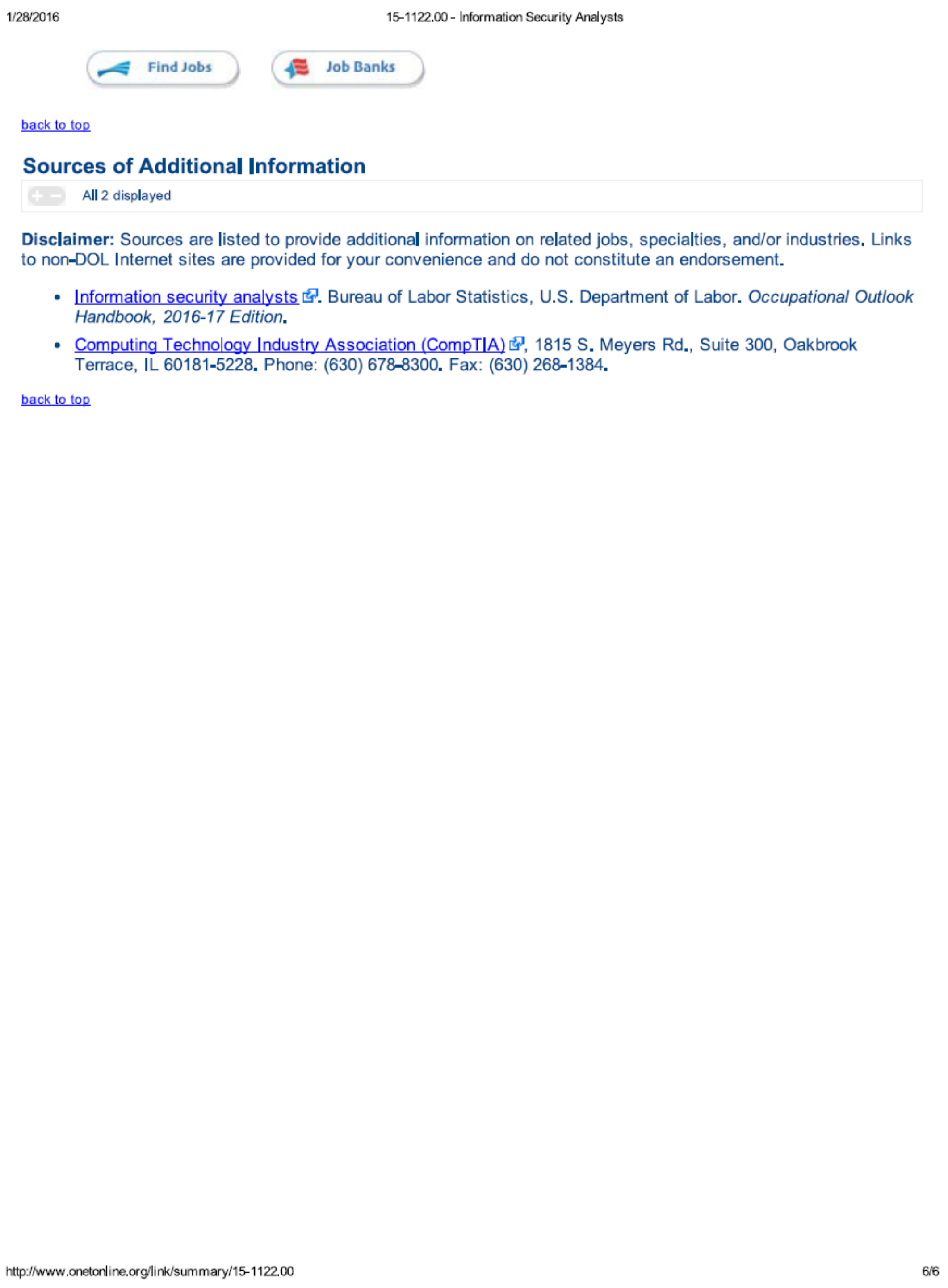
Median wages (2014)	$42.74 hourly, $88,890 annual
State wages	Local Salary Info
Employment (2014)	83,000 employees
Projected growth (2014-2024)	■■■■ Much faster than average (14% or higher)
Projected job openings (2014-2024)	25,500
State trends	Employment Trends
Top industries (2014)	Professional, Scientific, and Technical Services Finance and Insurance

Source: Bureau of Labor Statistics 2014 wage data and 2014-2024 employment projections. "Projected growth" represents the estimated change in total employment over the projections period (2014-2024). "Projected job openings" represent openings due to growth and replacement.

back to top

Job Openings on the Web

http://www.onetonline.org/link/summary/15-1122.00 5/6



1/28/2016 15-1122.00 - Information Security Analysts

back to top

Sources of Additional Information

All 2 displayed

Disclaimer: Sources are listed to provide additional information on related jobs, specialties, and/or industries. Links to non-DOL Internet sites are provided for your convenience and do not constitute an endorsement.

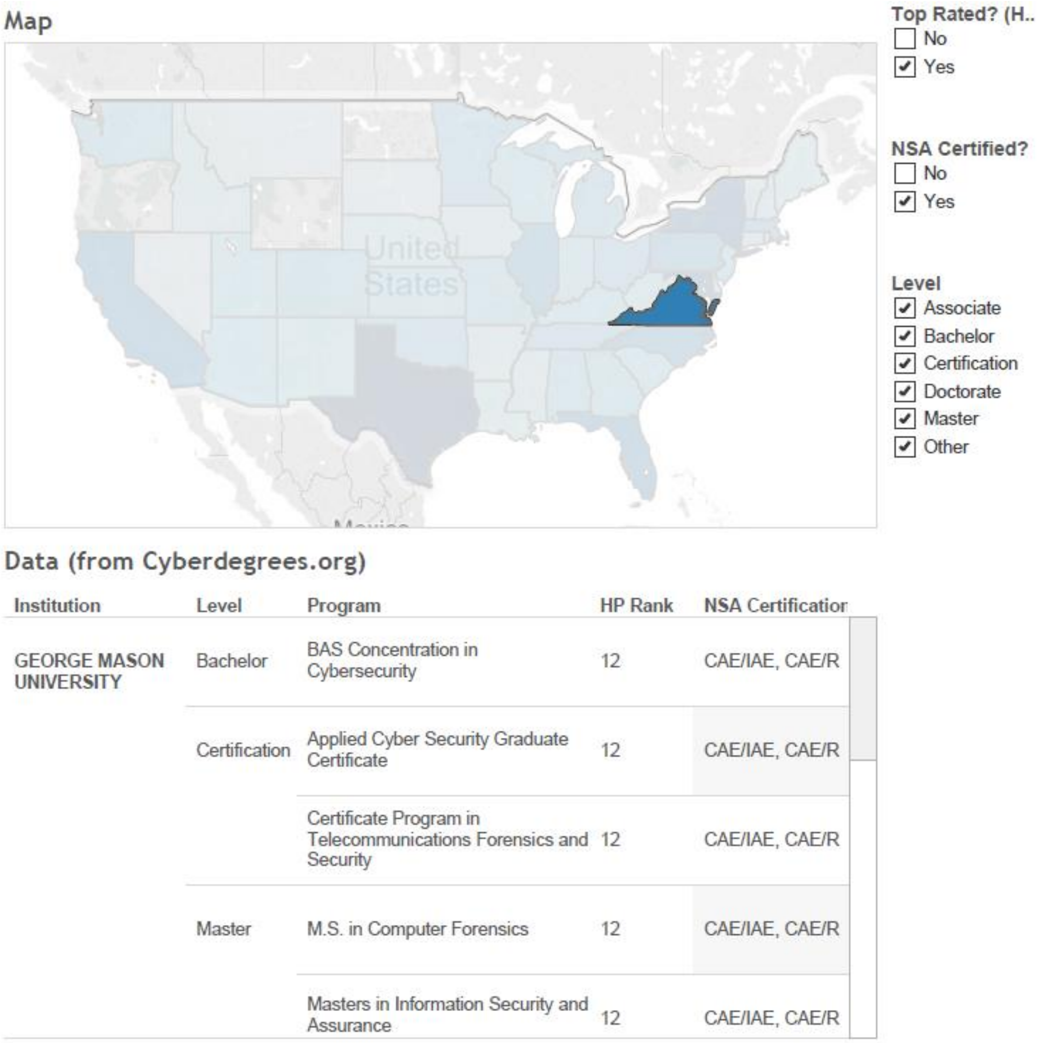
- Information security analysts. Bureau of Labor Statistics, U.S. Department of Labor. *Occupational Outlook Handbook, 2016-17 Edition.*
- Computing Technology Industry Association (CompTIA), 1815 S. Meyers Rd., Suite 300, Oakbrook Terrace, IL 60181-5228. Phone: (630) 678-8300. Fax: (630) 268-1384.

back to top

http://www.onetonline.org/link/summary/15-1122.00 6/6

Appendix B: Cybersecurity Education and Training

Nana, Rikesh (2015). Cybersecurity Program Database. The full database is at: https://public.tableau.com/profile/rikesh#!/vizhome/CybersecurityPrograms/Dashboard1



Map

Top Rated? (H..
□ No
☑ Yes

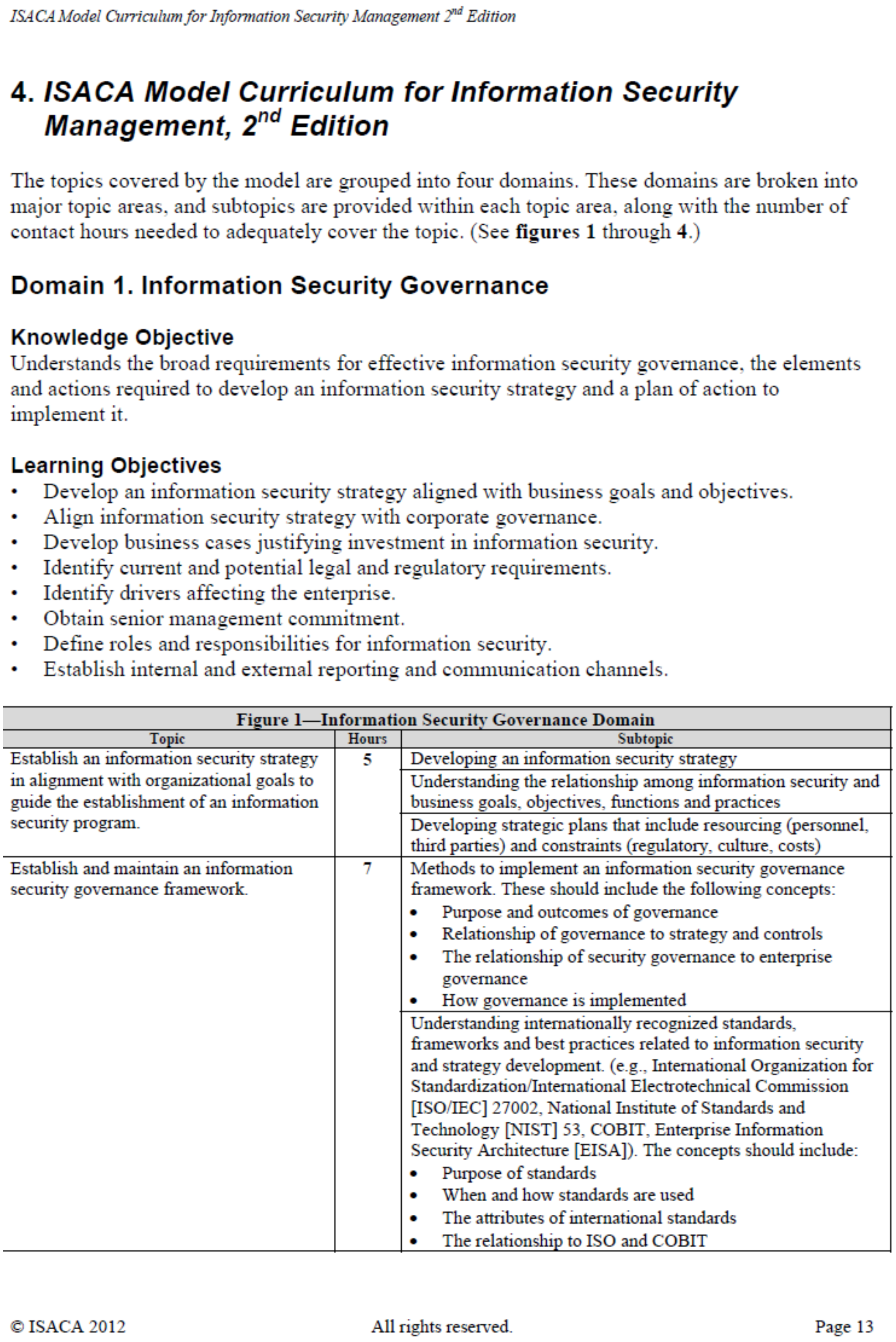
NSA Certified?
□ No
☑ Yes

Level
☑ Associate
☑ Bachelor
☑ Certification
☑ Doctorate
☑ Master
☑ Other

Data (from Cyberdegrees.org)

Institution	Level	Program	HP Rank	NSA Certificatior
GEORGE MASON UNIVERSITY	Bachelor	BAS Concentration in Cybersecurity	12	CAE/IAE, CAE/R
	Certification	Applied Cyber Security Graduate Certificate	12	CAE/IAE, CAE/R
		Certificate Program in Telecommunications Forensics and Security	12	CAE/IAE, CAE/R
	Master	M.S. in Computer Forensics	12	CAE/IAE, CAE/R
		Masters in Information Security and Assurance	12	CAE/IAE, CAE/R

ISACA. (2012). ISACA® Model Curriculum for Information Security Management, 2nd Edition.



ISACA Model Curriculum for Information Security Management 2nd Edition

4. *ISACA Model Curriculum for Information Security Management, 2nd Edition*

The topics covered by the model are grouped into four domains. These domains are broken into major topic areas, and subtopics are provided within each topic area, along with the number of contact hours needed to adequately cover the topic. (See **figures 1** through **4**.)

Domain 1. Information Security Governance

Knowledge Objective

Understands the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy and a plan of action to implement it.

Learning Objectives

- Develop an information security strategy aligned with business goals and objectives.
- Align information security strategy with corporate governance.
- Develop business cases justifying investment in information security.
- Identify current and potential legal and regulatory requirements.
- Identify drivers affecting the enterprise.
- Obtain senior management commitment.
- Define roles and responsibilities for information security.
- Establish internal and external reporting and communication channels.

Figure 1—Information Security Governance Domain

Topic	Hours	Subtopic
Establish an information security strategy in alignment with organizational goals to guide the establishment of an information security program.	5	Developing an information security strategy
		Understanding the relationship among information security and business goals, objectives, functions and practices
		Developing strategic plans that include resourcing (personnel, third parties) and constraints (regulatory, culture, costs)
Establish and maintain an information security governance framework.	7	Methods to implement an information security governance framework. These should include the following concepts: • Purpose and outcomes of governance • Relationship of governance to strategy and controls • The relationship of security governance to enterprise governance • How governance is implemented
		Understanding internationally recognized standards, frameworks and best practices related to information security and strategy development. (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 27002, National Institute of Standards and Technology [NIST] 53, COBIT, Enterprise Information Security Architecture [EISA]). The concepts should include: • Purpose of standards • When and how standards are used • The attributes of international standards • The relationship to ISO and COBIT

© ISACA 2012 All rights reserved. Page 13

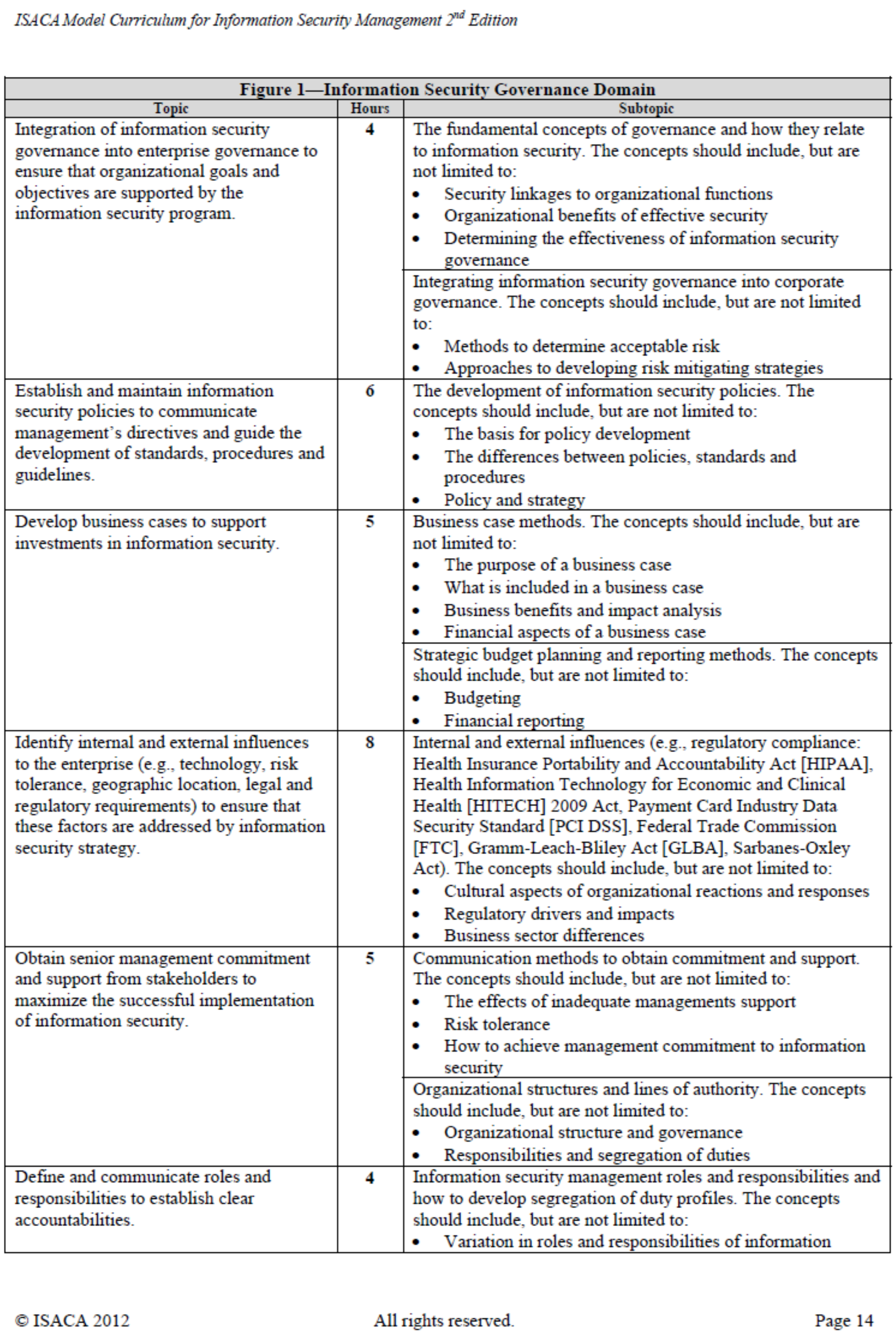


Figure 1—Information Security Governance Domain

Topic	Hours	Subtopic
Integration of information security governance into enterprise governance to ensure that organizational goals and objectives are supported by the information security program.	4	The fundamental concepts of governance and how they relate to information security. The concepts should include, but are not limited to: • Security linkages to organizational functions • Organizational benefits of effective security • Determining the effectiveness of information security governance
		Integrating information security governance into corporate governance. The concepts should include, but are not limited to: • Methods to determine acceptable risk • Approaches to developing risk mitigating strategies
Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.	6	The development of information security policies. The concepts should include, but are not limited to: • The basis for policy development • The differences between policies, standards and procedures • Policy and strategy
Develop business cases to support investments in information security.	5	Business case methods. The concepts should include, but are not limited to: • The purpose of a business case • What is included in a business case • Business benefits and impact analysis • Financial aspects of a business case
		Strategic budget planning and reporting methods. The concepts should include, but are not limited to: • Budgeting • Financial reporting
Identify internal and external influences to the enterprise (e.g., technology, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by information security strategy.	8	Internal and external influences (e.g., regulatory compliance: Health Insurance Portability and Accountability Act [HIPAA], Health Information Technology for Economic and Clinical Health [HITECH] 2009 Act, Payment Card Industry Data Security Standard [PCI DSS], Federal Trade Commission [FTC], Gramm-Leach-Bliley Act [GLBA], Sarbanes-Oxley Act). The concepts should include, but are not limited to: • Cultural aspects of organizational reactions and responses • Regulatory drivers and impacts • Business sector differences
Obtain senior management commitment and support from stakeholders to maximize the successful implementation of information security.	5	Communication methods to obtain commitment and support. The concepts should include, but are not limited to: • The effects of inadequate managements support • Risk tolerance • How to achieve management commitment to information security
		Organizational structures and lines of authority. The concepts should include, but are not limited to: • Organizational structure and governance • Responsibilities and segregation of duties
Define and communicate roles and responsibilities to establish clear accountabilities.	4	Information security management roles and responsibilities and how to develop segregation of duty profiles. The concepts should include, but are not limited to: • Variation in roles and responsibilities of information

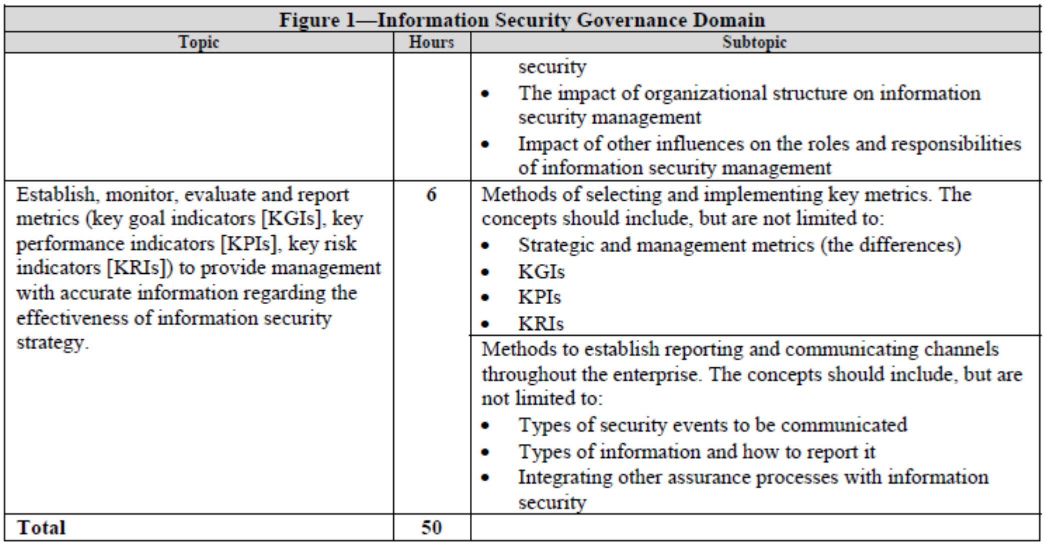
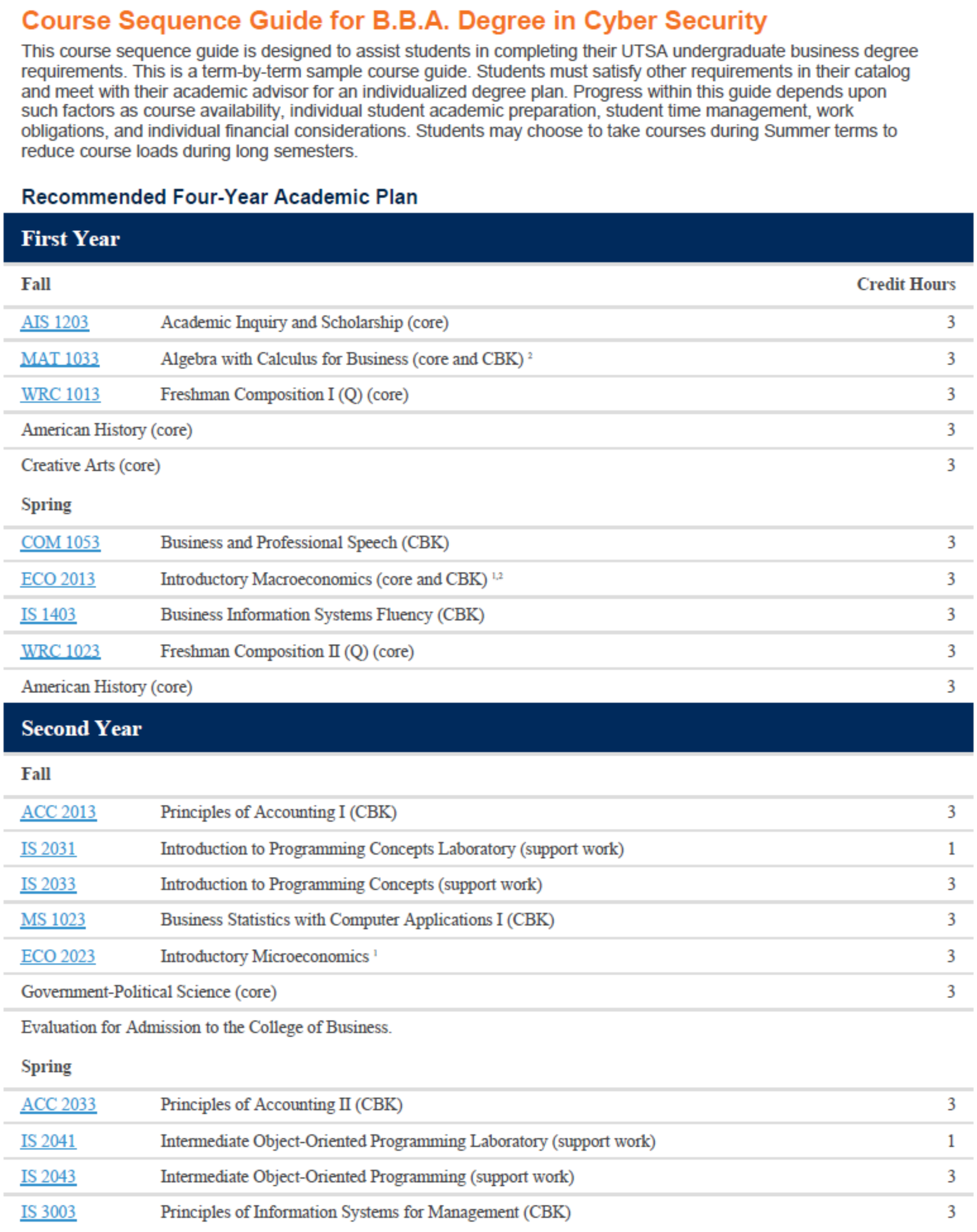


Figure 1—Information Security Governance Domain

Topic	Hours	Subtopic
		security • The impact of organizational structure on information security management • Impact of other influences on the roles and responsibilities of information security management
Establish, monitor, evaluate and report metrics (key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of information security strategy.	**6**	Methods of selecting and implementing key metrics. The concepts should include, but are not limited to: • Strategic and management metrics (the differences) • KGIs • KPIs • KRIs
		Methods to establish reporting and communicating channels throughout the enterprise. The concepts should include, but are not limited to: • Types of security events to be communicated • Types of information and how to report it • Integrating other assurance processes with information security
Total	**50**	

Sample Degree Program: Bachelor of Business Administration Degree program in Cybersecurity at UTSA:

http://catalog.utsa.edu/undergraduate/business/informationsystemscybersecurity/#cybersecurity



Course Sequence Guide for B.B.A. Degree in Cyber Security

This course sequence guide is designed to assist students in completing their UTSA undergraduate business degree requirements. This is a term-by-term sample course guide. Students must satisfy other requirements in their catalog and meet with their academic advisor for an individualized degree plan. Progress within this guide depends upon such factors as course availability, individual student academic preparation, student time management, work obligations, and individual financial considerations. Students may choose to take courses during Summer terms to reduce course loads during long semesters.

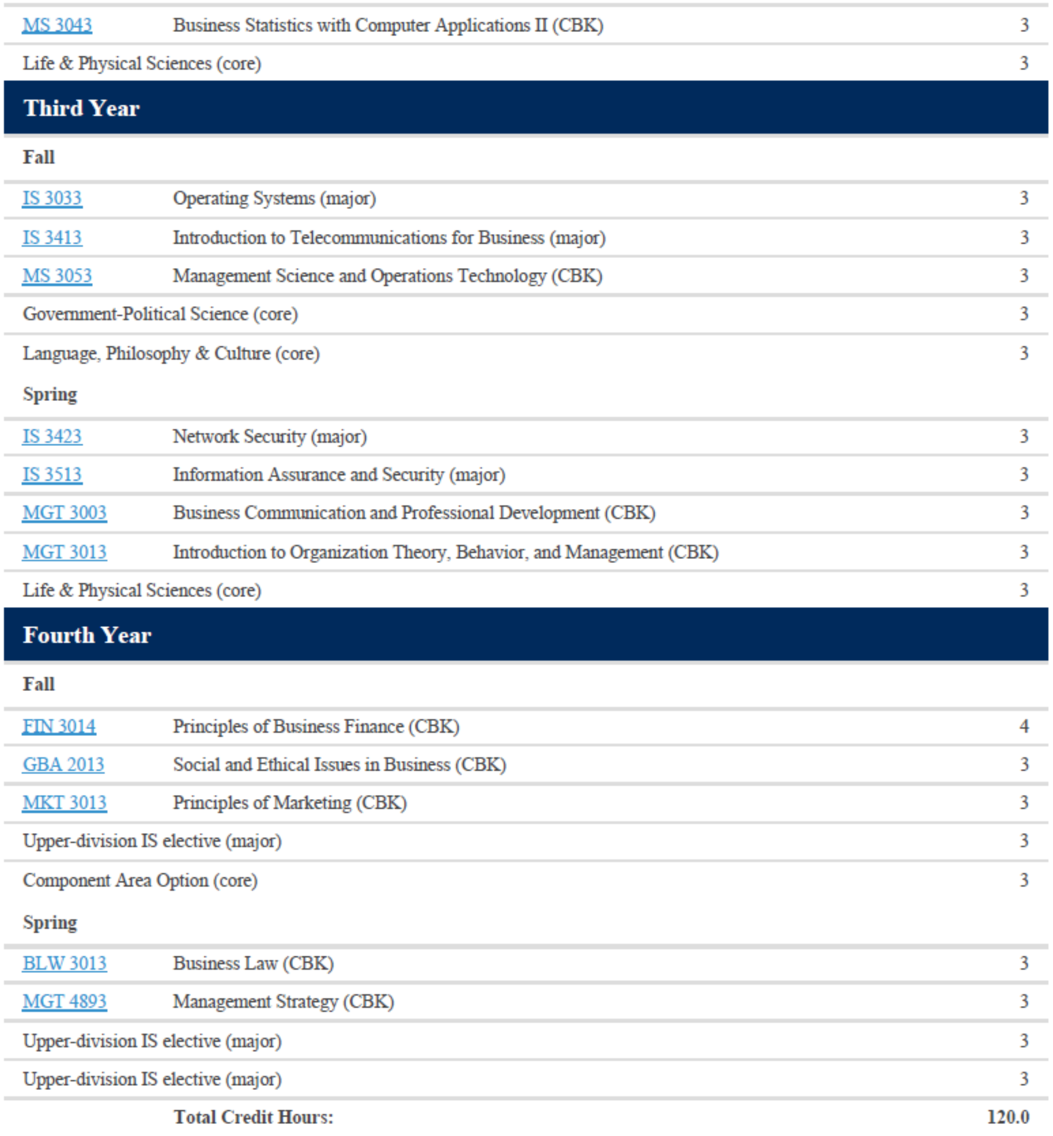
Recommended Four-Year Academic Plan

First Year

Fall		**Credit Hours**
AIS 1203	Academic Inquiry and Scholarship (core)	3
MAT 1033	Algebra with Calculus for Business (core and CBK) [2]	3
WRC 1013	Freshman Composition I (Q) (core)	3
American History (core)		3
Creative Arts (core)		3
Spring		
COM 1053	Business and Professional Speech (CBK)	3
ECO 2013	Introductory Macroeconomics (core and CBK) [1,2]	3
IS 1403	Business Information Systems Fluency (CBK)	3
WRC 1023	Freshman Composition II (Q) (core)	3
American History (core)		3

Second Year

Fall		
ACC 2013	Principles of Accounting I (CBK)	3
IS 2031	Introduction to Programming Concepts Laboratory (support work)	1
IS 2033	Introduction to Programming Concepts (support work)	3
MS 1023	Business Statistics with Computer Applications I (CBK)	3
ECO 2023	Introductory Microeconomics [1]	3
Government-Political Science (core)		3
Evaluation for Admission to the College of Business.		
Spring		
ACC 2033	Principles of Accounting II (CBK)	3
IS 2041	Intermediate Object-Oriented Programming Laboratory (support work)	1
IS 2043	Intermediate Object-Oriented Programming (support work)	3
IS 3003	Principles of Information Systems for Management (CBK)	3



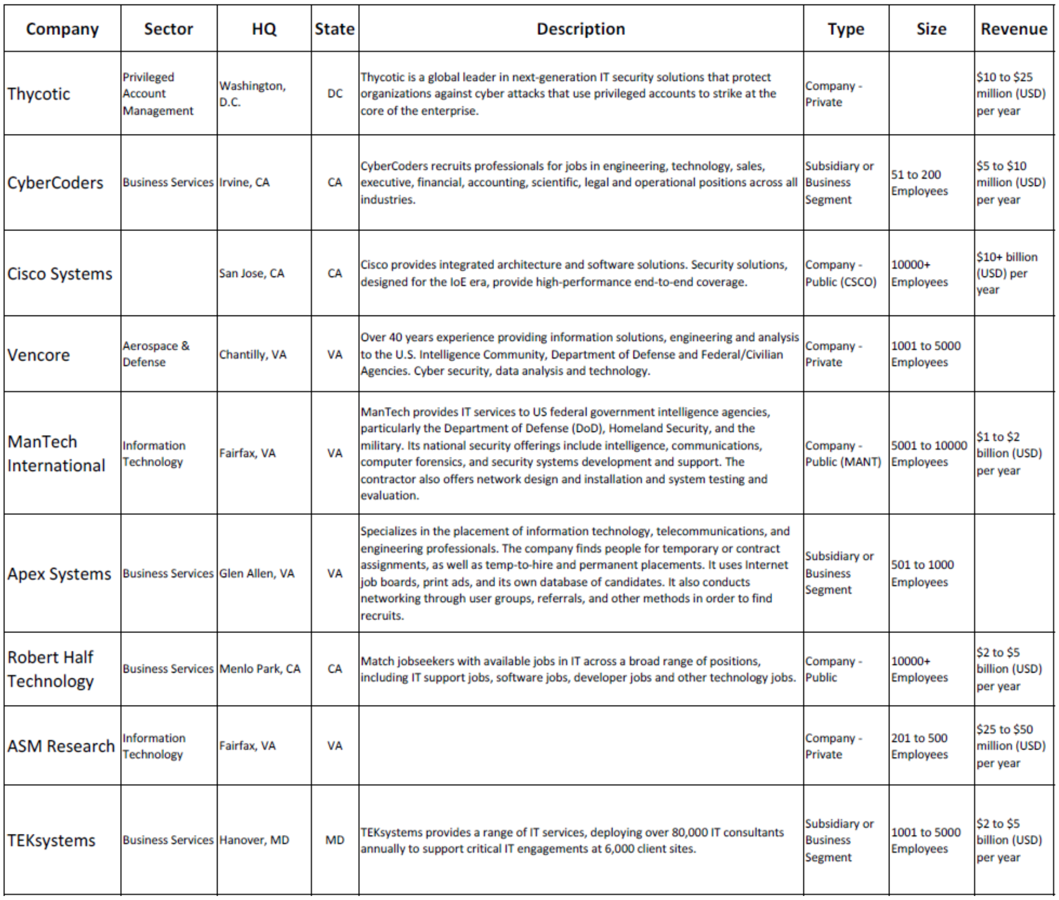
MS 3043	Business Statistics with Computer Applications II (CBK)	3
Life & Physical Sciences (core)		3
Third Year		
Fall		
IS 3033	Operating Systems (major)	3
IS 3413	Introduction to Telecommunications for Business (major)	3
MS 3053	Management Science and Operations Technology (CBK)	3
Government-Political Science (core)		3
Language, Philosophy & Culture (core)		3
Spring		
IS 3423	Network Security (major)	3
IS 3513	Information Assurance and Security (major)	3
MGT 3003	Business Communication and Professional Development (CBK)	3
MGT 3013	Introduction to Organization Theory, Behavior, and Management (CBK)	3
Life & Physical Sciences (core)		3
Fourth Year		
Fall		
FIN 3014	Principles of Business Finance (CBK)	4
GBA 2013	Social and Ethical Issues in Business (CBK)	3
MKT 3013	Principles of Marketing (CBK)	3
Upper-division IS elective (major)		3
Component Area Option (core)		3
Spring		
BLW 3013	Business Law (CBK)	3
MGT 4893	Management Strategy (CBK)	3
Upper-division IS elective (major)		3
Upper-division IS elective (major)		3
	Total Credit Hours:	**120.0**

Appendix C: Cybersecurity Companies and Civilian Career Opportunities

This list of firms that employ cybersecurity professionals was drawn from Cybersecurity Ventures list of Top 25 Cybersecurity Companies To Watch in 2016, along with information from the CareerBuilder and Glassdoor websites.

Company	Sector	HQ	State	Description	Type	Size	Revenue
root9B	Cybersecurity Consulting and Operational Support	Colorado Springs, Colo.	CO	root9B is a provider of cybersecurity and advance technology training capabilities, operational support and consulting services. The company is dedicated to the delivery of solutions and services based on technical innovation and professional excellence. root9B's workforce consists of U.S. military and law enforcement veterans with extensive experience in providing advanced technology solutions.	Company - Private	11 to 50 employees	
Lancope	Network Visibility and Security Intelligence	Alpharetta, Ga	GA	Lancope, Inc. is a leading provider of network visibility and security intelligence to defend enterprises against today's top threats. By collecting and analyzing NetFlow, IPFIX and other types of flow data, Lancope's StealthWatch® System helps organizations quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats.	Company - Private	51 to 200 Employees	$5 to $10 million (USD) per year
AlienVault	Threat Detection and Response	San Mateo, Calif.	CA	To give its customers the very best threat detection and response, AlienVault's unified platform - AlienVault Unified Security Management (USM) - combines five key security capabilities with expert threat intelligence that is updated every 30 minutes with data from the Open Threat Exchange (OTX) that has been analyzed and classified by the AlienVault Labs team. Every day, AlienVault Labs analyzes an immense amount of data submitted to the OTX by more than 8,000 contributing members from 140+ countries.	Company - Private	201 to 500 employees	
Norse	Live Attack Intelligence	San Mateo, Calif.	CA	Norse delivers continuously updated and unique Internet and darknet intel that helps organizations detect and block attacks that other systems miss. The Norse DarkMatter™ platform detects new threats and tags nascent hazards long before they are spotted by traditional threat intelligence tools.	Company - Private	51 to 200 Employees	
IBM Security	Enterprise IT Security Solutions	Waltham, Mass.	MA	As a global leader in IT security, IBM offers the strategies, capabilities, and technologies necessary to help agencies preemptively protect Web applications from threats and address the complexities and growing costs of security risk management and compliance.	Subsidiary or Business Segment		
AVG Technologies	Antivirus and Internet Security Software	Prague, Czech Republic		AVG is the online security company providing leading software and services to secure devices, data and people. AVG has over 188 million active users, as of September 30, 2014, using AVG´s products and services including Internet security, performance optimization, and personal privacy and identity protection.			
FireEye	Advanced Threat Protection	Milpitas, Calif	CA	FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks.	Company - Public (FEYE)	1,001 to 5,000 employees	581.2 million
Forcepoint	Cloud, Mobility and IoT Security	Austin, Texas	TX	Forcepoint was created to empower organizations to drive their business forward by safely embracing transformative technologies - cloud, mobility, Internet of Things (IoT), and others - through a unified, cloud-centric platform that safeguards users, networks and data while eliminating the inefficiencies involved in managing a collection of point security products.	Subsidiary or Business Segment	1,001 to 5,000 employees	361.5 million
Veracode	Application Security Testing	Burlington, Mass	MA	Every enterprise is now a technology company. Mobile, cloud, social media and Big Data are dramatically changing the way we deliver business innovation. Veracode offers a fundamentally different approach to application-layer security. Their subscription-based service combines a powerful, cloud-based platform with deep security expertise and proven best practices for managing enterprise-wide governance programs.	Company - Private	201 to 500 employees	$100 to $500 million (USD) per year
BT	Security and Risk Management Solutions	London, UK		BT provides a full range of cybersecurity consultancy and services. They conduct ethical hacking exercises to identify weaknesses, and then undertake continuous vulnerability scanning and threat monitoring.			
Clearwater Compliance	Risk Management and Compliance	Nashville, Tenn.	TN	Clearwater Compliance helps health care organizations ensure patient safety and improve the quality of care by safeguarding the confidentiality, integrity and availability of protected health information (PHI). The company has assisted more than 400 customers to operationalize and mature their information privacy, security, compliance and information risk management programs.	Company- Private	11 to 50 employees	

Company	Sector	HQ	State	Description	Type	Size	Revenue
Palo Alto Networks	Threat Detection and Prevention	Santa Clara, Calif.	CA	Palo Alto Networks' security platform natively brings together all key network security functions, including advanced threat protection, firewall, IDS/IPS, and URL filtering. Because these functions are natively-built into the platform and share important information across the respective disciplines, it ensures better security than legacy firewalls, UTMs, or point threat detection products.	Company - Public (PANW)		$500 million to $1 billion (USD) per year
Trend Micro	Server, Cloud and Content Security	Tokyo, Japan		As a global leader in IT security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With over 25 years of security expertise, the company is recognized as the market leader in server security, cloud security, and small business content security.			
Code Dx	Software Assurance Analytics	Northport, N.Y.	NY	Code Dx is a software assurance analytics tool that consolidates and normalizes vulnerabilities detected by disparate code analysis tools. Its visual analytics help you triage and prioritize your software's vulnerabilities for efficient remediation.			
Sera-Brynn	Cyber Risk Management	Suffolk, Va.	VA	Sera-Brynn is a cybersecurity firm and PCI QSA dedicated to helping clients secure their computing environments and meet applicable mandatory industry and government compliance requirements.			
Sophos	Antivirus and Malware Protection	Abingdon, UK		Sophos began producing antivirus and encryption products nearly 30 years ago. Today, the company's products help secure the networks used by 100 million people in 150 countries and 100,000 businesses. As IT networks grow in complexity, Sophos focuses on keeping IT security simple and reliable.			
Intel Security Group	Antivirus, Malware and Threat Protection	Santa Clara, Calif.	CA	Intel Security Group combines the security expertise of McAfee with the innovation, performance and trust of Intel, allowing users to simplify security with a single platform and unified framework backed by real-time threat intelligence.	Subsidiary or Business Segment		$10+ billion (USD) per year
IKANOW	Information Security Analytics	Reston, Va.	VA	Cyber-threat intelligence, risk management, and SIEM tools			
Cavirin	Automated IT and Cloud Security	Santa Clara, Calif	CA	Instead of thinking of the cloud like a data center in the sky, or "tacking on" cloud functionality as an afterthought to a data center product, Cavirin was designed with cloud architecture in mind. They created a system to allow the user to create a single security "bubble" and extend it to the entire IT ecosystem, both in the data center and across multiple cloud environments.	Company - Private		
Digital Defense	Managed Security Risk Assessment	San Antonio, Texas	TX	Founded in 1999, Digital Defense, Inc. is a provider of managed security risk assessment solutions, protecting billions of dollars in assets for small businesses to Fortune companies in over 65 countries.	Company - Private		
Dell SecureWorks	Managed Security Services	Atlanta, Ga.	GA	Dell SecureWorks focuses exclusively on information security services to protect thousands of customers around the world. As a security service provider, Dell SecureWorks strives to be a world leader in everything related to IT security; from firewall management services, combating advanced persistent threats to ensuring your PCI readiness for compliance.	Subsidiary or Business Segment	501 to 1000 Employees	$50 to $100 million (USD) per year
Herjavec Group	Information Security Service	Toronto, Canada		Dynamic IT entrepreneur Robert Herjavec, founded Herjavec Group in 2003, which quickly became one of North America's fastest-growing technology companies, accelerating from $400K to $140 million in sales annually over 12 years. The company delivers managed security services globally supported by a state-of-the-art, PCI compliant Security Operations Centre (SOC), operated 24/7/365 by certified security professionals. This expertise is coupled with a leadership position across a wide range of functions including compliance, risk management, networking and incident response.			
Nexusguard	Cloud Enabled DDoS Mitigation	San Francisco, Calif.	CA	As a longtime leader in DDoS defense, Nexusguard is at the forefront of the fight against malicious Internet attacks, protecting organizations worldwide from threats to their websites, services, and reputations. Continually evolving to face new threats as they emerge, the company has the tools, insight, and know-how to protect clients' vital business systems no matter what comes their way.	Company - Private		

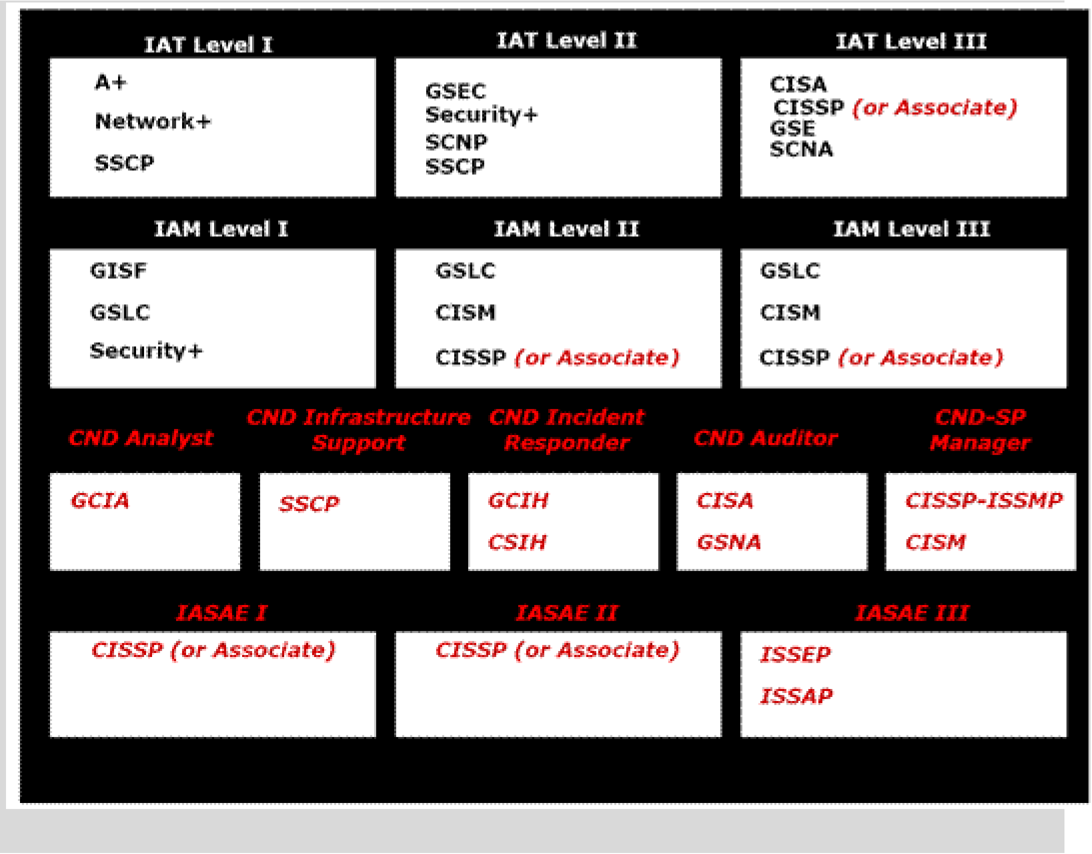


Company	Sector	HQ	State	Description	Type	Size	Revenue
Thycotic	Privileged Account Management	Washington, D.C.	DC	Thycotic is a global leader in next-generation IT security solutions that protect organizations against cyber attacks that use privileged accounts to strike at the core of the enterprise.	Company - Private		$10 to $25 million (USD) per year
CyberCoders	Business Services	Irvine, CA	CA	CyberCoders recruits professionals for jobs in engineering, technology, sales, executive, financial, accounting, scientific, legal and operational positions across all industries.	Subsidiary or Business Segment	51 to 200 Employees	$5 to $10 million (USD) per year
Cisco Systems		San Jose, CA	CA	Cisco provides integrated architecture and software solutions. Security solutions, designed for the IoE era, provide high-performance end-to-end coverage.	Company - Public (CSCO)	10000+ Employees	$10+ billion (USD) per year
Vencore	Aerospace & Defense	Chantilly, VA	VA	Over 40 years experience providing information solutions, engineering and analysis to the U.S. Intelligence Community, Department of Defense and Federal/Civilian Agencies. Cyber security, data analysis and technology.	Company - Private	1001 to 5000 Employees	
ManTech International	Information Technology	Fairfax, VA	VA	ManTech provides IT services to US federal government intelligence agencies, particularly the Department of Defense (DoD), Homeland Security, and the military. Its national security offerings include intelligence, communications, computer forensics, and security systems development and support. The contractor also offers network design and installation and system testing and evaluation.	Company - Public (MANT)	5001 to 10000 Employees	$1 to $2 billion (USD) per year
Apex Systems	Business Services	Glen Allen, VA	VA	Specializes in the placement of information technology, telecommunications, and engineering professionals. The company finds people for temporary or contract assignments, as well as temp-to-hire and permanent placements. It uses Internet job boards, print ads, and its own database of candidates. It also conducts networking through user groups, referrals, and other methods in order to find recruits.	Subsidiary or Business Segment	501 to 1000 Employees	
Robert Half Technology	Business Services	Menlo Park, CA	CA	Match jobseekers with available jobs in IT across a broad range of positions, including IT support jobs, software jobs, developer jobs and other technology jobs.	Company - Public	10000+ Employees	$2 to $5 billion (USD) per year
ASM Research	Information Technology	Fairfax, VA	VA		Company - Private	201 to 500 Employees	$25 to $50 million (USD) per year
TEKsystems	Business Services	Hanover, MD	MD	TEKsystems provides a range of IT services, deploying over 80,000 IT consultants annually to support critical IT engagements at 6,000 client sites.	Subsidiary or Business Segment	1001 to 5000 Employees	$2 to $5 billion (USD) per year

Appendix D: Cybersecurity Certifications

This list of DOD Approved Baseline Information Assurance Certifications was produced by Transcender, a vendor of training and exam preparation courses for cybersecurity professionals [5]. The table can be found at the following link:

https://www.transcender.com/gen.aspx?pf=page&sn=tra_dod8570.1_sec



IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA CISSP *(or Associate)* GSE SCNA

IAM Level I	IAM Level II	IAM Level III
GISF GSLC Security+	GSLC CISM CISSP *(or Associate)*	GSLC CISM CISSP *(or Associate)*

CND Analyst	*CND Infrastructure Support*	*CND Incident Responder*	*CND Auditor*	*CND-SP Manager*
GCIA	*SSCP*	*GCIH* *CSIH*	*CISA* *GSNA*	*CISSP-ISSMP* *CISM*

IASAE I	*IASAE II*	*IASAE III*
CISSP (or Associate)	*CISSP (or Associate)*	*ISSEP* *ISSAP*

Table 8 provides definitions for the acronyms in the above list.

Table 8. Cybersecurity certification acronyms and definitions

Acronym	Definition
IAT	Information Assurance Technical
SSCP	Systems Security Certified Practitioner
GSEC	G Security Essentials Certification
SCNP	Security Certified Network Professional
CISA	Certified Information System Auditor
CISSP	Certified Information Systems Security Professional
GSE	G Security Expert
SCNA	Sun Certified Network Administrator
IAM	Information Assurance Management
GISF	G Information Security Fundamentals Certification
GSLC	G Security Leadership Certification
CISM	Certified Information Security Manager
CND	Computer Network Defense
GCIA	G Certified Intrusion Analyst
GCIH	G Certified Incident Handler
CSIH	Certified Computer Security Incident Handler
GSNA	G Systems and Network Auditor Certification
IASAE	Information Assurance Systems Architecture and Engineering
ISSMP	Information System Security Management Professional
ISSEP	Information Systems Security Engineering Professional
ISSAP	Information Systems Security Architecture Professional

Note: These acronyms are listed separately here for the convenience of the reader. Many of these acronyms also are listed in the glossary.

References

[1] Peterson, Jeffery, Gary Lee, Annemarie Randazzo-Matsel, and Kim Deal (2015). *Support to the Cyber Task Force: Cyberspace Operations Workforce Development.* CNA. DIM-2015-U-010999-Final.

[2] Libicki, Martin, David Senty, and Julia Pollak (2014). *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market.* RAND Corporation. RR-430.

[3] Ladner, Justin, Jeffery Peterson, and Ron Nickel (2015). *Scraping the Surface: An Exploration of Big Data in the Context of Sexual Assault.* CNA. DRM-2015-U-011692-Final.

[4] SANS Institute (2014). Cybersecurity Professional Trends: A SANS Survey. Accessed Mar. 30, 2016 https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615.

[5] Peterson, Jeffery, Michelle Dolfini-Reed, Lewis G. Lee, and John Pearson (2015). *Managing the Marine Corps Enlisted Cyberspace Operations Workforce.* CNA. DRM-2014-U-009016-Final.

Bibliography

Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Chief Information Officer (2015). Information Assurance Workforce Improvement Program. DoD 8570.01-M (http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf).

Burning Glass Technologies. (2015). Job Market Intelligence: Cybersecurity Jobs, 2015 (http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf).

Bureau of Labor Statistics, Employment Projections. (2014). Information Security (http://data.bls.gov/projections/occupationProj).

Bureau of Labor Statistics, National Employment Matrix (2015). Industries Where Information Security Analysts Are Employed (http://data.bls.gov/projections/nationalMatrix?queryParams=15-1122-405&ioType=o).

Bureau of Labor Statistics, Occupational Outlook Handbook (2015). Information Security Analysts (http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm).

Bureau of Labor Statistics, Occupational Employment Statistics (2014). Occupational Employment and Wages, May 2014. 15-1122 Information Security Analysts (http://www.bls.gov/oes/current/oes151122.htm).

Cybersecurity Ventures (2015). Top 25 Cybersecurity Companies to Watch in 2016 (http://www.itbusinessedge.com/slideshows/top-25-cybersecurity-companies-to-watch-in-2015-01.html).

ISACA. (2012). ISACA® Model Curriculum for Information Security Management, 2nd Edition (http://www.isaca.org/Knowledge-Center/Academia/Pages/Model-Curriculum-for-Information-Security-Management.aspx).

ISACA. (2012). ISACA® Model Curriculum for IS Audit and Control, 3rd Edition (http://www.isaca.org/Knowledge-Center/Academia/Pages/Model-Curriculum-for-IS-Audit-and-Control-3rd-Edition.aspx).

Nana, Rikesh (2015). Cybersecurity Program Database (https://public.tableau.com/profile/rikesh#!/vizhome/CybersecurityPrograms/Dashboard1).

National Security Agency, Central Security Service. (2015). Centers of Academic Excellence Institutions (https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml).

O*Net Online (2015). Summary Report for: 15-1122.00 - Information Security Analysts (http://www.onetonline.org/link/summary/15-1122.00).

PayScale, Inc. (2016). Information Security Analyst Salary (United States). (http://www.payscale.com/research/US/Job=Information_Security_Analyst/Salary).

Ponemon Institute LLC. (2014). 2014 Best Schools for Cybersecurity. Ponemon Institute Research Report sponsored by HP Enterprise Security (http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf).

Sargent, John F., Jr. (2014). The U.S. Science and Engineering Workforce: Recent, Current, and Projected Employment, Wages, and Unemployment. Congressional Research Service. (https://www.fas.org/sgp/crs/misc/R43061.pdf).

U.S. News and World Report (2015). Online Cybersecurity Bachelor's Degree (http://www.usnews.com/education/online-education/cyber-security-bachelors-degree).

This page intentionally left blank.

CNA

This report was written by CNA's Resource Analysis Division (RAD).

RAD provides analytical services—through empirical research, modeling, and simulation—to help develop, evaluate, and implement policies, practices, and programs that make people, budgets, and assets more effective and efficient. Major areas of research include health research and policy; energy and environment; manpower management; acquisition and cost; infrastructure; and military readiness.

DRM-2016-U-013905-Final

CNA is a not-for-profit research organization
that serves the public interest by providing
in-depth analysis and result-oriented solutions
to help government leaders choose
the best course of action
in setting policy and managing operations.

Nobody gets closer—
to the people, to the data, to the problem.

www.cna.org ● 703-824-2000

3003 Washington Boulevard, Arlington, VA 22201