2025

NCyTE CENTER
National Cybersecurity Training & Education Center

Whatcom COMMUNITY COLLEGE

SJI SEATTLE JOBS INITIATIVE

CYBERSECURITY PROGRAM CODING

Critical Step to Assessing Education to Workforce Outcomes

This material is based upon work supported by the National Science Foundation under Grant #2054724.. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Prepared By :
Seattle Jobs Initiative

Delivered To :
National Cybersecurity Training and Education Center (NCyTE)

research@seattlejobsinit.com

Executive Summary

Background

This report examines how cybersecurity programs nationwide are coded using the CIP code classification system. Because these codes are often used to generate aggregate statistics on post-secondary education programs, which informs policymaking and investment decisions, selecting a code that best reflects the program's curriculum is essential to accurately estimating the supply of cybersecurity workers nationwide.

This analysis first focused on information about the Center of Academic Excellence (CAE) in Cybersecurity-designated programs nationwide, surveying program representatives to collect data on cybersecurity program titles and CIP codes. The research team then gathered information on a sample of non-CAE-designated programs sharing the same CIP codes as the CAE-designated programs.

Finally, the team examined the alignment between two existing cybersecurity workforce frameworks, the NICE framework and the DCWF, and the BLS's Standard Occupation Classification (SOC). The SOC provides aggregate information about the number of people employed, their demographics, their wages, and typical educational backgrounds across the economy. However, as an economy-wide classification system, it may not reflect the nuances of an emerging field like cybersecurity.

Findings

Post-secondary programs solely focusing on cybersecurity (Bachelor in Cybersecurity, for example) are consistently coded with a small set of CIP codes, the most common of which among the CAE-designated programs surveyed was 11.1003: "Computer and Information Systems Security / Auditing/ Information Assurance." This is the best-fitting umbrella CIP code for cybersecurity programs.

CIP codes whose title or description explicitly refer to cybersecurity—Cyber/Computer Forensics and Counterterrorism, for example—were much less common, but this can be explained by the fact that fewer programs target military cybersecurity applications.

Programs offering cybersecurity as a specialty track or concentration are more likely to be coded using the CIP code of the broader program. For example, computer science programs with a concentration in cybersecurity are coded using the "Computer Science" CIP code. This limits the ability to estimate the number of computer science graduates trained in cybersecurity and related fields. The situation is similar for other educational sectors offering cybersecurity or forensics tracks, particularly business administration and accounting.

Recommendations

For the much larger set of programs like Computer Science, Business, and Accounting, creating new subcodes for programs with cybersecurity tracks that reflect these tracks' distinct tools and content would be helpful.

Given the growth of the cybersecurity sector, there is a growing need for specialized management. Developing codes for cybersecurity management programs would reflect training that combines cybersecurity technical skills with management skills. This also aligns with the number of management roles in the NICE Framework and DCWF.

As was initially hypothesized, several cybersecurity programs have either inherited the CIP code of the program they grew out of or have not updated their code from the 2010 classification. While this is a clear minority of programs, a significant portion still maintains a more general “Computer Science” or “Computer Systems Networking and Telecommunications” that would more cleanly fit into a more specific cybersecurity CIP code.

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

AAS	Associate of Applied Science
BLS	Bureau of Labor Statistics
BS	Bachelor of Science
CAE-CD	Centers of Academic Excellence in Cybersecurity Program for Cyber Defense
CAE-CO	Centers of Academic Excellence in Cybersecurity Program for Cyber Operations
CAE-R	Centers of Academic Excellence in Cybersecurity Program for Cyber Research
CIP	Classification of Instructional Programs
DCWF	Defense Cyber Workforce Framework
DOD	Department of Defense
DOL	Department of Labor
IPEDS	Integrated Postsecondary Education Data System
KSA	Knowledge, Skills, and Abilities
KU	Knowledge Unit
MOS	Military Occupational Specialty
NCAE-C	National Centers of Academic Excellence in Cybersecurity
NCES	National Center for Education Statistics
NCyTE	National Cybersecurity Training and Education Center
NICE	National Initiative on Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
O*NET	Occupational Information Network
SJI	Seattle Jobs Initiative
SOC	Standard Occupational Classification
SVC	Support Vector Classifiers

Introduction

Background and Context

Sound policy decision-making requires precise research and data collection to provide valuable and accurate information. In higher education and workforce development, planning for and developing new programs and assessing how well existing programs meet the needs of employers better requires identifying existing programs, understanding their content, and evaluating the alignment between their content and the skills needed in the workplace.

Identifying cybersecurity programs at a national scale helps provide an exhaustive assessment of the sector's current state. It would help plan how best to size program capacity to ensure that graduation rates meet the number of workers cybersecurity employers need and how to update curricula to ensure graduates have the skills in demand. It is standard for postsecondary programs to be categorized using the National Center for Education Statistics (NCES) Classification of Instructional Programs (CIP) codes. These codes, developed by the National Center for Education Statistics (NCES), are used throughout the higher education system to report program characteristics and outcomes, including the number of enrollees and graduates. Each CIP code has a related definition, which includes broad learning outcomes and example program titles (see Appendix A for additional information about CIP code structure).

However, despite their importance for reporting programs and institutional outcomes, these CIP codes are often not updated as the CIP code classification is updated or programs change. New programs frequently inherit the CIP code for the program or programs out of which they evolved. This is not easy to detect because the CIP codes and program names are not consistently reported together outside the institution's internal reporting.

This challenge of capturing programs is particularly acute in a field like cybersecurity, which has rapidly emerged and is in high demand. It is suspected that many cybersecurity programs are miscoded. They emerged before the 2020 update when cybersecurity was first added to the CIP classification schema and used the previous taxonomy (e.g., Telecommunications Management in 2010 CIP). They may have emerged from connected but taxonomically distinct programs like Business Administration and carried that CIP code rather than updated CIP codes aligned with the 2020 taxonomy (Cybersecurity Defense, Computer Engineering, and Telecom Management).

If accurate, estimating cybersecurity graduates using CIP-based databases such as the Integrated Postsecondary Education Data System (IPEDS) would produce conservative results that do not capture all cybersecurity graduates. This makes it challenging to assess whether enough cybersecurity workers graduate every year to meet the labor market demand and if cybersecurity graduates are employed in cybersecurity occupations.

The cybersecurity workforce is only large enough to cover 72% of cybersecurity jobs.[1] This drives home the need for more postsecondary education planning to meet the growing demand and ensure that the cybersecurity workforce is well-prepared and qualified to tackle the sector's challenges.

Purpose and Scope

The National Cybersecurity Training and Education Center (NCyTE) sought to address this and contracted with Seattle Jobs Initiative (SJI) to conduct a study. This study's primary objective is to evaluate how existing cybersecurity programs nationwide are classified and whether they are

categorized consistently based on program content. The final report will first describe the different data sources used in this exercise to collect programs' CIP codes and collect program curriculum and learning objectives (Figure 1).

Given the extensiveness of the CIP taxonomy, this project has two phases. The first focuses on collecting and analyzing information on the Center of Academic Excellence (CAE) in Cybersecurity-designated programs nationwide to help center the analysis and identify the most common CIP codes used in cybersecurity. Information about these programs is already easily accessible from the National Centers of Academic Excellence database. However, CAE does not collect programs' CIP codes. Thus, SJI surveyed CAE-designated programs.

In the second phase, this research project leverages the CIP codes used by the CAE-designated programs to analyze a sample of other programs nationwide that are also classified with these codes.

In conjunction with analyzing of cybersecurity programs' CIP codes, SJI developed crosswalks between CIP codes for post-secondary education programs, the Bureau of Labor Statistics Standard Occupation Classification (SOC)[2] codes for occupations, and cybersecurity work role frameworks. These included the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework,[3] and the Department of Defense's (DOD) Cyber Workforce Framework (DCWF).[4] These crosswalks helped identify how post-secondary programs align with these different skill and role frameworks and how SOC job titles align with cyber-specific work roles.

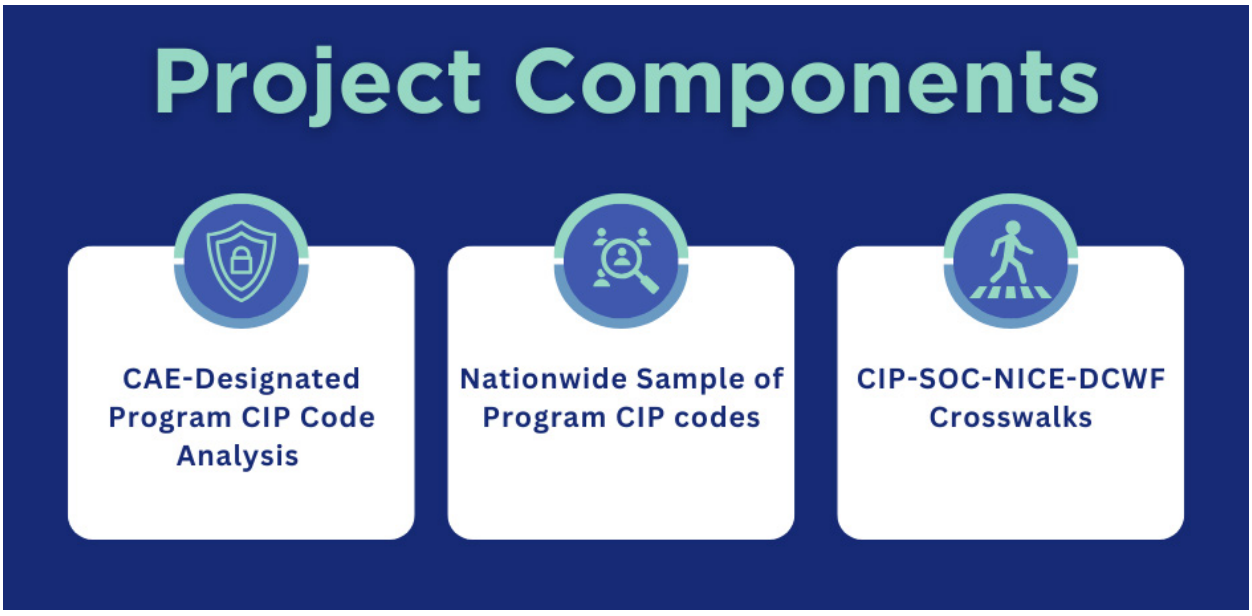

Figure 1. Project Components

Literature Review

In a rapidly changing political and technological landscape, post-secondary institutions and other job training programs must keep pace with the labor market needs by regularly updating course content, planning for new programs, and expanding capacity as needed. Labor market and

education data play an essential role in this planning process. Institutions and affiliated organizations rely on statistical evidence to apply for funding and analyze and compare intended and realized student outcomes. The need for accurate program-level data is thus broad and wide-ranging, from program classification to carry nationwide research to post-graduation employment information to establish relationships with employer partners. However, education data is regularly scrutinized due to incomplete, inaccurate, or non-representative information.

For example, the National Postsecondary Education Cooperative Working Group on Student Outcomes used two case studies of student outcomes data collection combined with working group meetings to study the strengths and weaknesses of student outcomes data. Regarding state centralized databases, working group participants raised concerns about data quality on several aspects ranging from outdated occupational information, linked wage records, and varying data field definitions and interpretations to the lack of data standardization across (or within, as noted by the authors) institutions.[5]

Similarly, regarding the need for improved data on online program outcomes, Kelchen also noted the potential lack of harmonization of CIP code use among colleges and universities.[6] South Dakota Board of Regents Academic Affairs Council also raised this issue when working to identify program duplication in the university system. Some programs with the same CIP codes focused on different educational areas, while similar programs had different CIP codes.[7]

The National Student Clearinghouse is a nonprofit organization providing educational reporting and data exchange services for 3,600 participating institutions nationwide.[8] Using their publicly available CIP Code Lookup Table, it is possible to complete a cursory analysis of CIP codes assigned to programs with the word “cyber” in the title. While this analysis is conservative in nature and does not include all cybersecurity degrees, it still offers some insight into CIP code use practices among institutions.

For example, 973 program titles nationwide have the term “cyber” in their title and appear to focus on cybersecurity (Figure 2). These programs use 78 CIP codes, including one inherited from the 2010 CIP taxonomy (“Security and Protective Services”). Forty-one percent of these programs use the CIP code titled “Computer and Information Systems Security/Auditing/Information Assurance,” the remaining 59% use a wide variety of codes ranging from categories directly related to computer science such as “Computer and Information Sciences, General” and “Computer Systems Networking and Telecommunications” to categories representative of national security such as “Cyber/Computer Forensics and Counterterrorism” and “Cyber/Electronic Operations and Warfare” or more ad hoc degrees like “Accounting Technology/Technician and Bookkeeping” and “Speech Communication and Rhetoric.” While the latter refers to a double major in communications and cybersecurity, this further indicates the challenge of providing an accurate count of cybersecurity graduates nationwide.

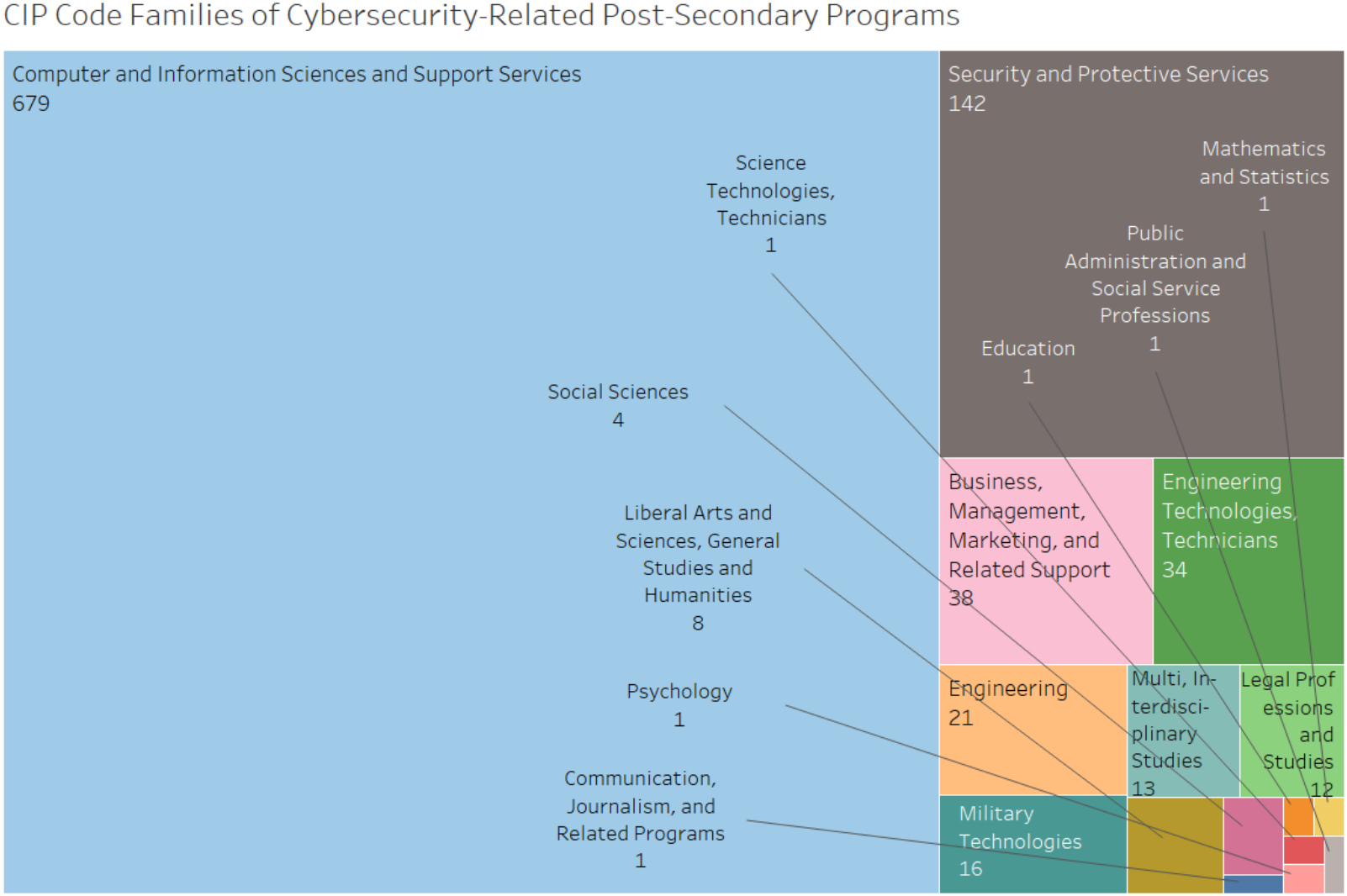

Figure 2. CIP Code Use by Cybersecurity and Cyber Defense Post-Secondary Programs
Source: National Student Clearinghouse, CIP Code Lookup Table, 2023

Methodology

The primary goals of this research project are to understand which CIP codes cybersecurity programs are using nationwide and whether programs with similar learning objectives are coded consistently. The team also analyzed and identified the CIP codes best aligned to the following codes and frameworks:

- National Initiative on Cybersecurity Education (NICE) Workforce Framework for Cybersecurity[3]
- The Department of Defense (DOD) Cyber Workforce Framework (DCWF) work roles[4]
- Standard Occupation Code (SOC) codes that NICE and DCWF work roles can lead to[2]

Research Questions

There are four primary research questions in this project:

1. What CIP codes do CAE-designated cybersecurity programs use?
2. What CIP codes do non-CAE-designated cybersecurity programs use?
3. Are these codes aligned with the programs' titles and learning objectives?
4. How do program CIP codes align with SOC classification and the NICE and DCWF frameworks?

CIP Code Use

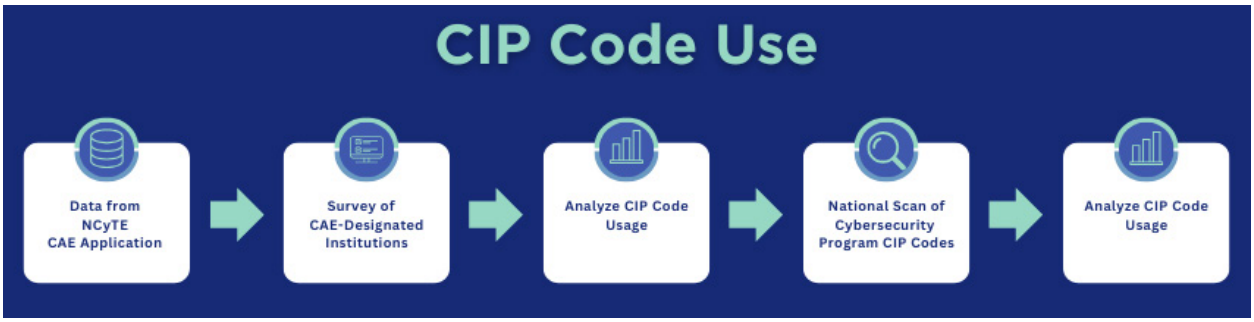

Figure 3. CIP Code Use Analysis

To analyze how cybersecurity programs are categorized nationwide (Figure 3), the research team first obtained from NCyTE information on CAE-designated programs collected via the CAE designation application. In the application, program representatives must provide detailed information about the program or programs that will earn the institution the CAE designation. Information provided includes:

- Course titles
- Associated knowledge units (KUs)
- Alignment with the NICE Framework work role categories

However, the CAE application does not request program CIP codes. In addition, to satisfy their various reporting requirements, post-secondary institutions often only submit either program titles or CIP codes, but not both. Thus, there is no nationwide non-proprietary repository of program titles connected to CIP codes, nor do states consistently collect this data.

To bridge this gap, the research team developed a survey of CAE-designated institutions to collect information on their cybersecurity program titles and related CIP codes (Appendix A). SJI sent the survey program coordinators listed on the CAE-designation application and university keyholders obtained from desk research to collect CAE-designated programs' CIP codes.

This survey was distributed in multiple waves between February and October 2024 to 401 program representatives. It was pre-populated with the courses in each institution's CAE application, and respondents were asked to add other cybersecurity-related programs at their institution regardless of their inclusion in the CAE application and provide their related six-digit CIP code.

Respondents were also asked to specify the type of degree obtained by program graduates and whether military veterans may obtain credit for prior learning based on their military occupational specialty (MOS) in the program. Survey respondents were also asked whether their institution had cybersecurity program transfer credits and advanced placement articulation agreements with local high schools.

Survey responses on program title and CIP codes were matched with the data received from NCyTE to link program CIP codes to program content (NICE Framework categories, individual course titles, and knowledge units related to each course).

Using survey responses, the team identified the CIP codes most used by cybersecurity programs by addressing the following questions:

1. What are the CAE-Cyber Defense (CD), CAE-Cyber Operations (CO), and CAE-Research (R) designated postsecondary programs nationwide?
2. What are the names of these degrees and their associated Knowledge Unit Alignment Summary (KU)?
3. What are these degrees' CIP codes as reported to IPEDS?
4. Are similar programs based on program titles and learning objectives using similar CIP codes?
5. Is the content of the CAE-designated program aligned with the titles and definitions of the CIP codes supplied by the survey respondents?

Table 1. CAE-Designated Institution Survey Summary

Survey Summary	*N*
CAE-Designated Institutions Surveyed	357
Responses	188

Using the CIP codes most used by CAE-designated institutions to identify cybersecurity programs nationwide, the research scope was then expanded to non-CAE-designated programs to research the following questions:

1. Which other postsecondary institutions nationwide use CIP codes similar to the ones used by CAE-designated programs?
2. Depending on data availability and using degree titles and/or graduation data, which programs are the most likely to be related to cybersecurity?

The team first selected the CIP codes most used by CAE-designated programs to identify other potential cybersecurity programs nationwide using the IPEDS database. However, this database only contains the institution name and program CIP code. It does not include the program title.

The team thus located program titles for programs associated with CIP codes retrieved from the IPEDS database via websites for individual states' higher education statistics reporting and individual institutions' program listing for the program title associated with the CIP code. This resulted in a sample of convenience; only select states routinely compile this data and make it accessible.

Table 2. Non-CAE Institution Program Scan

Program Scan of Non-CAE Institutions	*N*
Institutions with Identified CIP Codes	2,598
Unique Credentialed Programs with Identified CIP Codes	15,448
Institutions with CIP Codes Connected to Program Names	534
Program Name–CIP Code Pairs	4,208
Cyber Programs Name–CIP Code Pairs	181

More details about this methodology can be found in Appendix C.

Work Roles Alignment

The second part of the project was dedicated to evaluating the alignment between CIP and SOC code classifications, the NICE Framework (Appendix A and Appendix),[3] and the Department of Defense Cyber Workforce Framework (Appendix A and Appendix).[4] The team has created crosswalks between the following frameworks and classifications (Figure 4):

- ### *Standard Occupational Classification*

  The Standard Occupational Classification (SOC) system is developed and maintained by the Bureau of Labor Statistics (BLS) classification to categorize occupations in the labor market. This system is used to characterize the workforce by occupation across the US. Occupations span industries. For example, SOC captures a database administrator (SOC 15-1242) employed by a manufacturer and one working for a university.

- ### *NICE Framework*

  NICE is a partnership between government, academia, and the private sector whose goal is to help employers develop their cybersecurity workforce. They have developed the NICE Framework or the Workforce Framework for Cybersecurity. The NICE Framework and DCWF provide standard descriptions and categories of cybersecurity work roles and associated knowledge, skills, and abilities (KSAs). The NICE Framework comprises seven (7) categories of common cybersecurity functions, 33 specialty areas of cybersecurity work, and 52 common work roles

- ### *Department of Defense Cyber Workforce Framework*

  Similarly, the Department of Defense Cyber Workforce Framework (DCWF) provides a consolidated classification of cybersecurity work roles in the DOD defined by DOD directive 8140.01. This work leveraged the NICE Framework to define work roles for the Defense context.[4] Like the NICE Framework, DCWF describes key functions, tasks, and

necessary knowledge, skills, and abilities. DCWF has 72 work roles across seven (7) workforce elements.

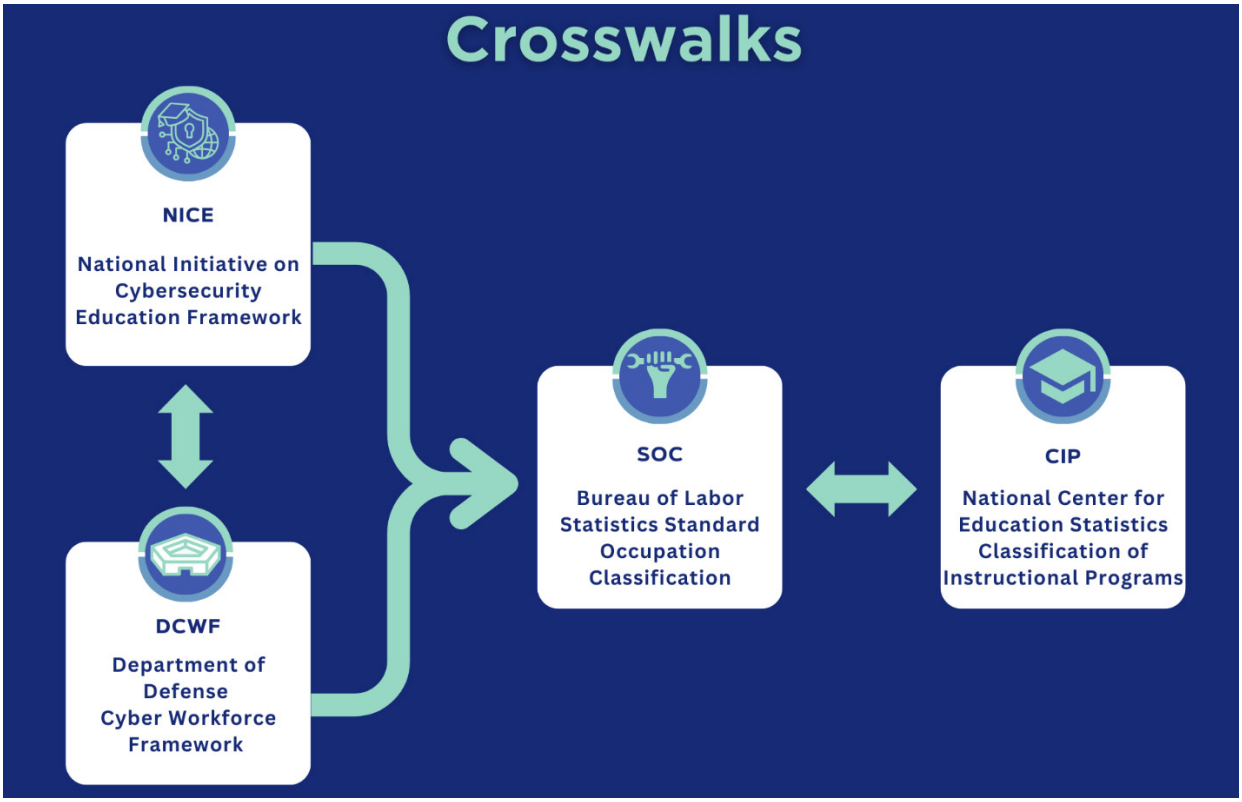

Figure 4. Crosswalks

The research team used the descriptions of work roles in the NICE Framework and the DCWF to evaluate alignment and create a crosswalk with CIP codes for post-secondary programs. This crosswalk helps identify the post-secondary programs most likely to prepare students for each work role in these two frameworks. A similar approach was taken to create a crosswalk between the SOC occupation codes and the NICE Framework and DCWF. This crosswalk presents the SOC occupations most closely aligned with the NICE Framework and DCWF work roles.

Database Creation

Program-Related Tables

The program-specific information is organized in multiple tables in the database:

1. **Institution Table.** The first table presents information at the institution level, including the institution name, location, website, president's name and contact information, institution type, CAE designations obtained, program(s) point of contact information (name, email, phone number, and department), number of transfer pathway agreements, if any, and advance placement agreements, if any.
2. **Program Table.** The second table contains information at the cybersecurity program level, including program name, alignment with NICE work role categories, whether the institution was included in and completed the survey, the CAE designations for which the program has been validated, the program CIP code, the type of degrees the program can lead to

(certificate, associate, etc.), and the type of MOS credits for prior learning veterans have access to (if any).

3. **Course Table.** The third table is the program table, listing the names of each CAE-designated program course, the knowledge units (KUs) taught in each course, the code of these KUs, and the KU type (Foundational, Technical, Non-Technical, or Optional), if known.

Learning Objectives

The research team also collected additional information from the Department of Defense Public Cyber Exchange's CAE Document Library,[9] including the list of learning outcomes and topics for each knowledge unit. Specifically, each type of CAE designation, except the CAE-R, must prepare students for a set of knowledge units categorized as Foundational, Technical Core, Non-Technical Core, and Optional. The programs must prepare students for an established number of knowledge units based on the CAE designation and degree type.

Thus, the database also includes a **knowledge units table** listing the knowledge units recognized in the CAE-designation requirements, including KU code, title, category, and various learning objectives associated with the KU.

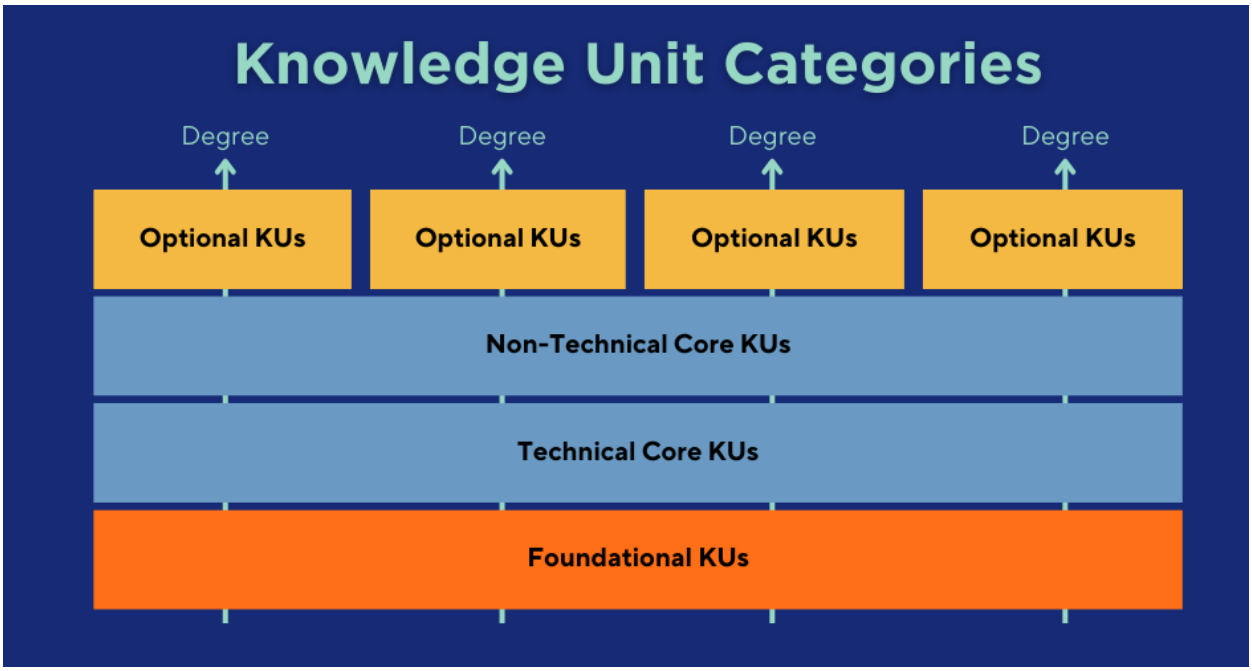

Figure 5. Knowledge Unit Categories

Work-Role Tables

This project also assesses the alignment between CIP and SOC codes with the Workforce Framework for Cybersecurity (NICE Framework) and the Department of Defense Cyber Workforce Framework (DCWF Framework). The team thus also collected data on the NICE Framework Components developed by the National Institute of Standards and Technology (NIST), which contained information on the NICE Framework work roles and their related task, knowledge, and skill (TKS) statements. Similarly, the DCWF Framework also provides information

on cyber work roles (several overlap with NICE work roles), related job descriptions, and typical education requirements by type of position (entry-level, intermediate, and advanced).

The work roles-related tables include:

1. The **NICE Category Table** lists each NICE category's title code and description.
2. The **Task, Knowledge, Skill Table** lists all the tasks, knowledge, and skills (TKS) contained in the NICE Framework with their code, type (task, knowledge, or skill), and description.
3. The **Work Role Table** shows each NICE work role's identification code, title, description, and NICE category.
4. The **Work Role-TKS Table** links the NICE work roles to their required TKSs.
5. The **DCWF Work Role Table** shows each DCWF work role's identification code, title, description, and education requirements.

The research team also added information on CIP and SOC code classifications and the CIP-to-SOC Crosswalk, a collaboration between the Bureau of Labor Statistics (BLS) and the NCES. This crosswalk matches each six-digit CIP code with the six-digit SOC occupations that require similar skills and knowledge as taught in instructional programs. The database includes the following two additional tables:

- **2020 CIP Code Classification Table** (latest available as of November 2024) includes the CIP code, its broader CIP category, its title, a definition, and example programs from the U.S. Department of Education's National Center for Education Statistics (NCES) if available.*
- **The CIP-SOC Table lists the occupation SOC codes that most closely align with** each CIP code.

Tables & Schema

The database has the following tables (Table 3) and schema (Figure 6 and Figure 7):

Table 3. Database Tables

Program-Related Tables	Work-Role Tables
College	NICE Framework Category
Program	NICE Work Role
Course	DWCF Work Role
Knowledge Unit	Task, Knowledge, Skills
	NICE Work Role-TKS
	CIP-to-SOC

* The Classification of Instructional Programs is revised every ten years. New CIP codes are added if they meet one of the following criteria: identified by NCES Research, identified by a member of the Technical Review plan, requested by a federal agency, requested by a state agency, or requested by an IPEDS keyholder plus at least 10 institutions offering a program or nearly 10 in rapidly growing instructional areas.[10]

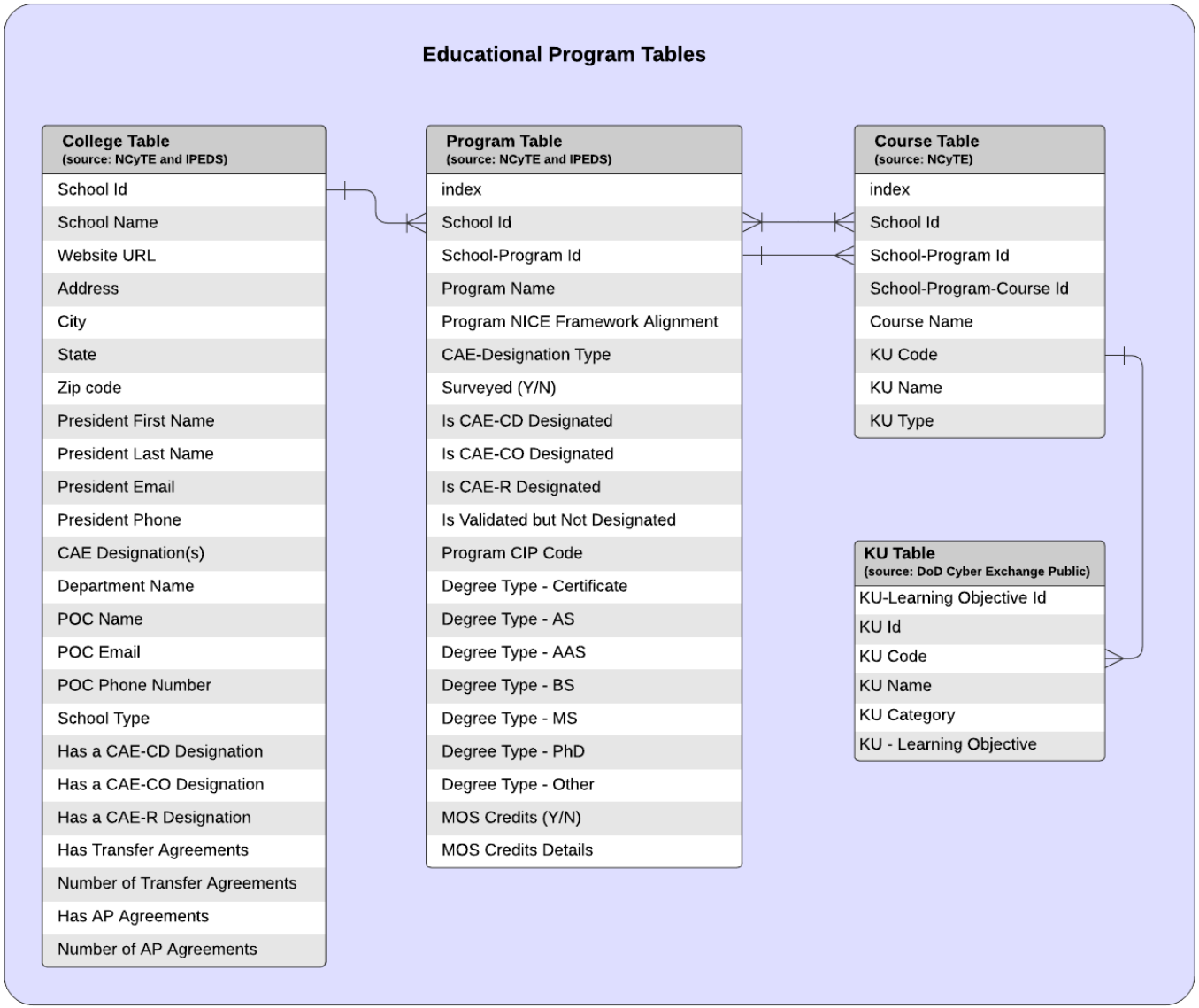

Figure 6. Database Schema: Education Tables

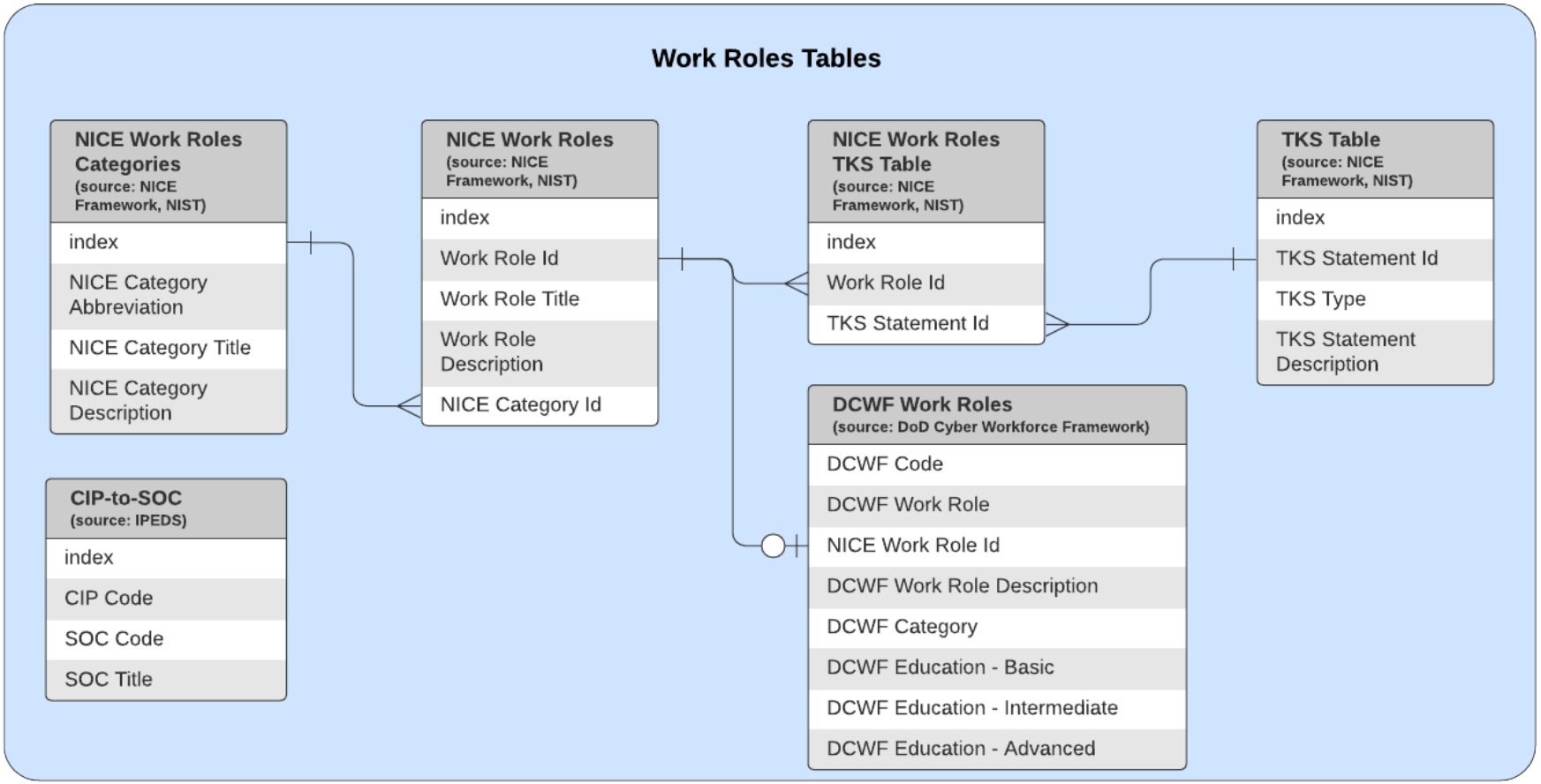

Figure 7. Database Schema: Work Roles Tables

Analysis

Program Coding Consistency

This database linking program components to NICE Framework and DCWF work roles and SOC occupations allowed the team to evaluate whether programs used the CIP code that best reflects their content. To do this, the research team combined a supervised Support Vector Machine (SVM) classification and topic modeling analysis to complete this work in addition to manual review.

Support vector classifiers (SVCs) are routinely used to perform supervised classification tasks in which part of the data has already been labeled. Using this set of pre-labeled observations, SVCs aim to find a decision boundary, a function of the various features present in the data, and weights that the model will learn to maximize the distance between the boundaries of the various labels. The model then estimates label probability using a five-fold cross-validation. First, a small set of programs were manually classified depending on their program title and course content. Groups consisted of:

- Cybersecurity
- Information Assurance/Science/Systems/Security
- Computer Science
- Cyber Defense
- Forensics & Crimes
- Other

An SVC model was then used to select the most appropriate group for each of the remaining CAE-designated programs in the dataset, again based on their program title and course content.

A topic modeling algorithm was then used to explore further the content of the CAE-designated programs in each broad group. This algorithm first breaks down a combination of the program title, course title, and learning objectives into a collection of root words (tokens) and reports how often they appear in this program content combination. This algorithm then uses a non-negative matrix factorization dimension reduction method to retrieve the most important keywords (topics) from the program content in each group. This helps explore the primary program content most relevant to each group and understand how content differs by group.

The team conducted the same analysis of program titles at other institutions as the analysis of CAE-designated institutions' program information. This extension aims to provide additional insight into how CIP codes are used and opportunities to harmonize and improve alignment with the NICE Framework.

CIP and SOC Code Alignment

The team then leveraged the CIP code classification, the NCES's CIP to SOC crosswalk,[11] the NICE Framework, and the DCWF to evaluate the alignment between NICE and DCWF work roles, CIP codes, and SOC codes. For each CIP code, the team first aggregated the learning objectives of CAE-designated programs using this CIP code. This list was then used to compare keywords of learning objectives for each CIP code with keywords in the TKSs for each NICE work role. This step led to creating an initial draft of the NICE work role to CIP crosswalk that was then manually reviewed to compare the CIP code and NICE work role descriptions to identify best fits.

Then, using the CIP to SOC crosswalk, each NICE work role was matched to a first set of SOC codes based on their best CIP code fits. This NICE work role to SOC crosswalk was also manually reviewed, and the NICE and SOC code descriptions were compared to identify the best fit. A similar approach was adopted to create a crosswalk between the DCWF and the SOC classification.

Findings

CIP Code Use

Before assessing whether cybersecurity and other related programs use appropriate CIP codes, it would be helpful first to evaluate the alignment of the CIP code classification (see Appendix A) with the cybersecurity sector in general. The latter is relatively broad, ranging from securing networks, applications, and software to analyzing and managing vulnerabilities to handling and investigating incidents, among others.

A cursory analysis of the CIP code classification shows that the broad categories at the two-digit level of CIP codes most likely to be related to cybersecurity and related sectors are the following:

- 11. Computer and Information Sciences and Support Services
- 14. Engineering
- 15. Engineering/Engineering-Related Technologies/Technicians
- 29. Military Technologies and Applied Sciences
- 43. Homeland Security, Law Enforcement, Firefighting, and Related Protective Services

In these five broad categories, only three CIP codes directly refer to cyber or cybersecurity in their title, thus having an explicit link to this sector (Figure 8).

- 29.0207 Cyber/Electronic Operations and Warfare
- 43.0402 Cyber/Computer Forensics and Counterterrorism
- 43.0404 Cybersecurity Defense Strategy/Policy

Others in the Homeland Security, Law Enforcement, Firefighting, and Related Protective Services (43) category refer to Security Science, Critical Infrastructure Protection, and Law Enforcement Intelligence Analysis, which are other key cybersecurity applications. Information Assurance and Systems Security are other essential occupational categories in cybersecurity and are best represented by the CIP codes in the Computer & Information Sciences (11) and Engineering groups (14):

- 11.1003 Information System Security
- 11.1001 Network and System Administration
- 14.4701 Electrical and Computer Engineering

Information System Security is the best umbrella CIP code for cybersecurity programs that do not fit into other explicitly cyber CIP codes despite not having cyber in the title. However, the other codes, especially Computer Engineering, allude to more sector- and application-neutral skills. Even if 14.1701 is correctly assigned to cybersecurity-related programs, it would be difficult to identify which Computer Engineering programs prepare students specifically for a cybersecurity career without more information on program content.

CIP Codes with Cyber-Related Knowledge in Title or Description

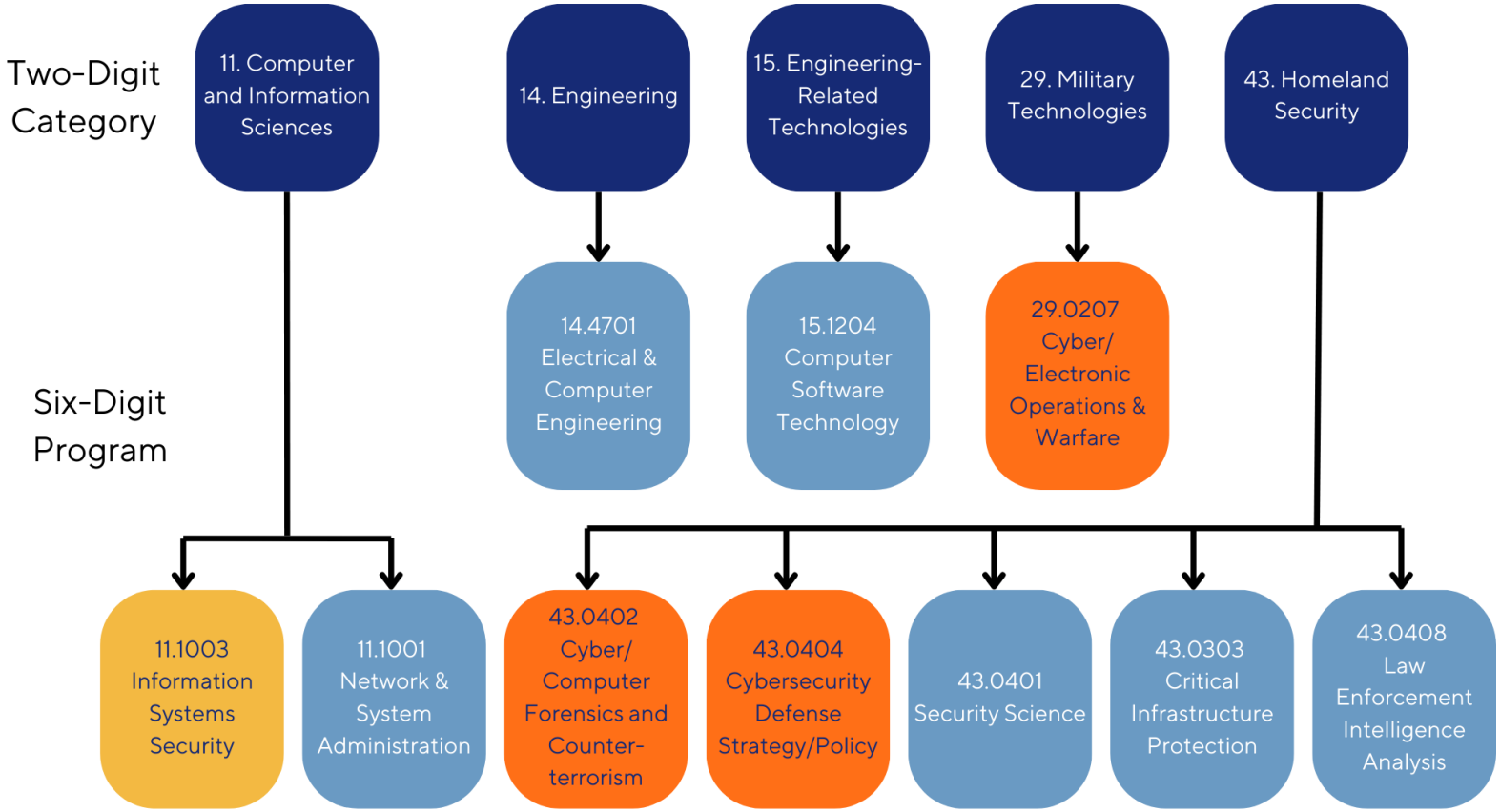

Figure 8. CIP Codes with Cyber-Related Knowledge in Title or Description

CIP Code Use in CAE-Designated Institutions

Common Codes

The research team surveyed representatives of CAE-designated institutions to obtain the CIP codes assigned to each cybersecurity program at their school. Figure 9 presents the CIP codes commonly (more than 1% of programs) assigned to cybersecurity programs at CAE-designated institutions and their relative frequency in the data (see Appendix D for CIP code descriptions)

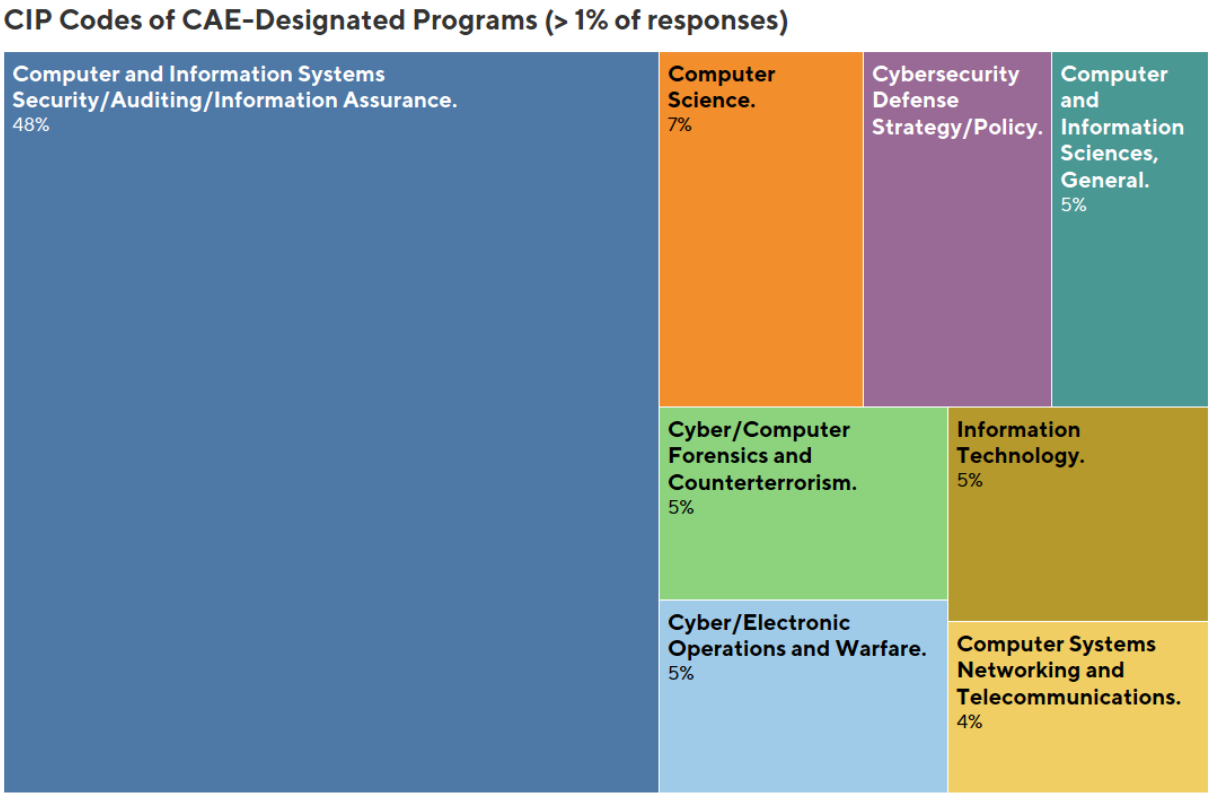

Figure 9. CIP Codes of CAE-Designated Programs

The “Computer and Information Systems Security / Auditing/ Information Assurance” CIP code (11.1003) is by far used the most often among cybersecurity programs at CAE-designated institutions (45% of recorded responses). According to the official CIP classification, programs with this CIP code “prepare individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures.”

Programs with these CIP codes are most commonly explicitly titled cybersecurity programs (e.g., Bachelor or Master of Science in Cybersecurity). This CIP code is also very common among information assurance or information security programs (e.g., Bachelor of Science in Information Systems and Technology or Associate of Applied Science (AAS) in Computer Information Systems, Cybersecurity/IT). Some programs that prepare students for a career in digital forensics, cyber defense, and cyber operations also use this code.

Cyber-explicit CIP codes (i.e., codes with cyber or cybersecurity in the title) are much less common. These codes seem most appropriate for military and law enforcement occupations, as outlined above. However, post-secondary programs exclusively targeting the military sector are

much less common than other general information assurance or cybersecurity programs, explaining why these codes occur much less frequently in the data.

While the code “Cyber/Computer Forensics and Counterterrorism” is used by a few cybersecurity degrees (e.g., Bachelor of Science in Cybersecurity), it is only assigned to a handful of forensics-related programs (e.g., Digital Forensics & Cyber Investigation or Cybercriminology and Security Studies).

Computer Science is also often used by CAE-designated institutions. However, this code, defined as “[a] program that focuses on computer theory, computing problems, and solutions, and the design of computer systems and user interfaces from a scientific perspective,” remains too general to infer specific cybersecurity content. This may hinder efforts to catalog and separate cybersecurity programs related to computer science from other general computer science programs also assigned this code.

While some programs assigned a “Computer Science” CIP code are cybersecurity programs (e.g., Bachelor or Master of Science in Cybersecurity), most are computer science programs with a concentration or track in cybersecurity. These programs are thus correctly coded; however, it becomes nearly impossible to estimate the number of cybersecurity students who graduate from those pathways using standard education databases like IPEDS.

Uncommon "Codes"

In addition to the most common CIP codes outlined in the previous section, CAE-designated institutions use a variety of additional codes to categorize their programs. The least common CIP codes (fewer than 1% of recorded responses) are outlined in Table 4.

Table 4. Uncommon CIP Codes of CAE-Designated Programs

CIP Family Title with Code	CIP Code	CIP Title
11. Computer and Information Sciences and Support services	11.0199	Computer and Information Sciences, Other
	11.0201	Computer Programing/Programing General
	11.1006	Computer Support Specialist
	11.1099	Computer/Information Technology Services Administration and Management, Other
	11.9999	Computer and Information Sciences and Support Services, Other
14. Engineering	14.1003	Laser and Optical Engineering
	14.2701	Systems Engineering
	14.4701	Electrical and Computer Engineering
15. Engineering and Engineering-Related Technologies and Technicians	15.1201	Computer Engineering Technology/Technician
43. Homeland Security, Law Enforcement, Firefighting, and Related Protected Services	43.0401	Security Science and Technology, General
	43.0405	Financial Forensics and Fraud Investigation
44. Public Administration and Social Service Professions	44.0401	Public Administration

CIP Family Title with Code	CIP Code	CIP Title
52. Business, Management, Marketing, and Related Support Services	52.0201	Business Administration and Management, General
	52.0251	Risk Management
	52.0299	Business Administration, Management, Operations, Other
	52.0399	Accounting and Related Services, Other
	52.1201	Management Information Systems, General
	52.2101	Telecommunications Management

Many other codes in the "Computer & Information Sciences and Support Services" CIP code family are most frequent in the uncommon code group. Many programs using codes starting with "Computer & Information Sciences" again refer to Computer Science programs with a concentration in cybersecurity or information security, pointing to the need for guidance targeted at program administrators to harmonize CIP code selection in case of minors, special tracks, or concentrations. Some administrators use codes ending with "Other," which could indicate human error in CIP code selection or that the available CIP codes do not represent these programs accurately.

Additionally, there are six programs with codes from the "Business, Management, Marketing, and Related Support Services" CIP code family. Three of six programs appear to have a CIP code that does not clearly align with the apparent program content based on the program title and required coursework. Miscoded programs include a Bachelor's in Cybersecurity coded as Business Administration, a degree in Information Technology coded as Management Information Systems, and a degree in Management Information Systems with a concentration in Cybersecurity coded as Management Information Systems.

There are also three programs that are coded as business management-related but do include cybersecurity components. For example, a degree in Cyber Accounting is coded as Accounting, and a Bachelor of Business Administration with a concentration in Cyber Defense is coded as Business Administration. Similarly, a Cyber Risk Management Graduate Certificate is coded as Risk Management (52.0215) in the Business, Management, Marketing, and Related Support Services CIP code family.

This points to the same problem highlighted for Computer Science programs: programs offering concentrations or special tracks in cybersecurity tend to use the CIP code of the core program (Computer Science or Business Administration, for instance) rather than a code more directly related to cybersecurity programs. Given the large number of Computer Science, Computer Engineering, and Business Administration post-secondary programs nationwide, it would be impossible to parse out students who completed a cybersecurity concentration from all other students who graduated from the general program if the same CIP code is used for both groups. Given the relatively large number of programs at CAE-designated institutions that are concentrations, tracks, or specializations (approximately 16% of the data), it would be helpful to provide guidance on how to code these special programs to ensure that all cybersecurity students are accounted for in analysis relying on CIP code data.

Additionally, if many students graduate from cybersecurity concentrations, program administrators could eventually consider splitting these programs to create stand-alone cybersecurity pathways.

Other uncommon CIP codes include “Engineering” and the “Engineering/Engineering-Related Technologies/Technicians” families. Only three programs among survey responses have these codes, and two appear to have no direct link to cybersecurity. Another program appears to be miscoded as its title is “Master of Engineering in Cybersecurity,” which does not have any direct link to its CIP code (“Laser and Optical Engineering”).

Finally, it is important to note that no programs at CAE-designated institutions among the survey responses have a military intelligence-related CIP code. However, these codes, specifically those under the “Military Technologies and Applied Sciences,” seem appropriate for cybersecurity or digital investigations study programs preparing students for a career in the military. These codes surfaced during the work alignment analysis and included, for example, the “Command & Control (C3, C4I) Systems and Operations” code, whose definition is:

> *A program that focuses on the theory, technology, and operational use of information and decision systems in support of battlefield, theatre, and global strategic operations. Includes instruction in applied mathematics and statistics, computer systems, real-time analysis and decision systems, surveillance and navigation systems, information and communications technology, information security, situational awareness, system integration, joint operations, and applications to specific command problems and services.*

CIP Code Use by Program Type

Evaluating whether programs in similar sectors use CIP codes consistently is also interesting. This could help identify the type of programs that need greater guidance to harmonize CIP code use between pathways with similar coursework, minimize miscoding, and ensure that all cybersecurity-related students can be accounted for in future analysis (Figure 10, Figure 12, and Figure 13). In this analysis, detailed in the Program Coding Consistency section above, a small set of programs was manually classified based on their program title and course content into eight groups (Figure 10):

- Cybersecurity
- Cyber Defense
- Cyber Crime and Forensics
- Business and Accounting
- Engineering
- Computer Science
- Information Assurance Science
- Other

An SVC model was then used to select the most appropriate group for each of the remaining CAE-designated programs in the dataset, again based on their program title and course content.

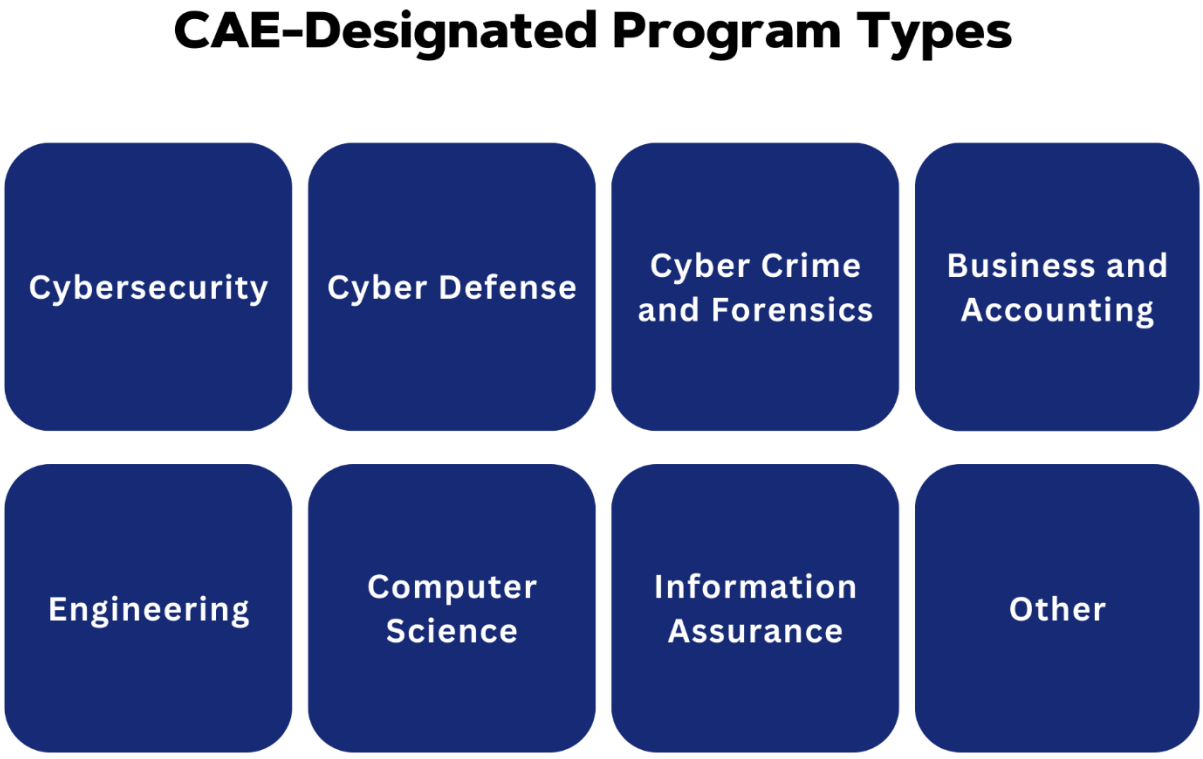

Figure 10. CAE-Designated Program Types

Cybersecurity is the most numerous category, accounting for 39% of the programs. Information assurance is the second largest category, with 28% of programs falling into this category. Cyber Defense, Cyber Crime and Forensics, and Engineering are the smallest categories, each accounting for only 4% of programs (Figure 11).

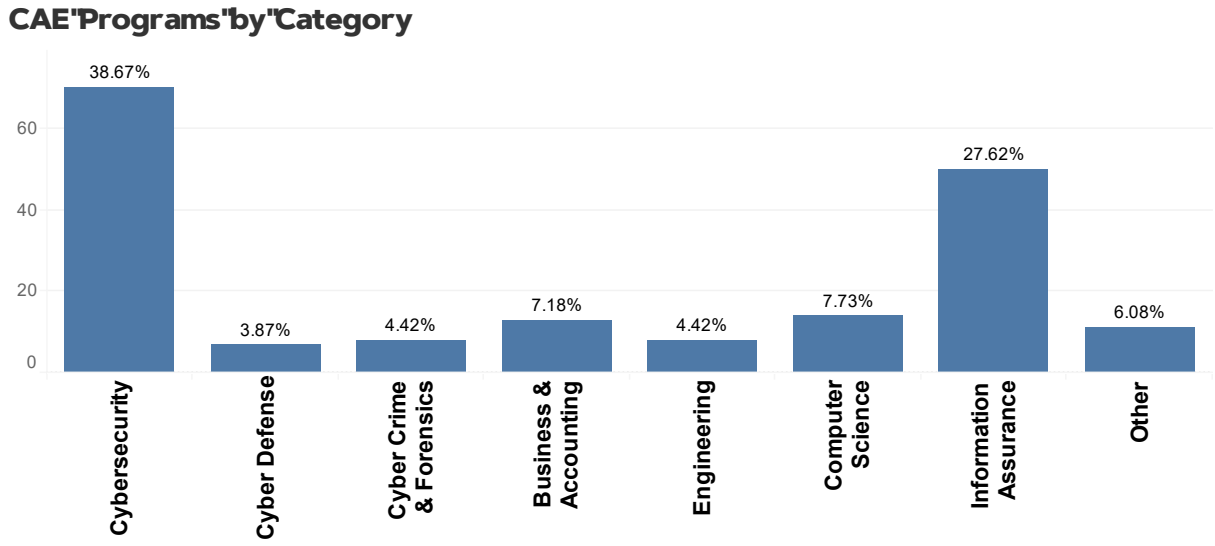

Figure 11. Number of CAE-Designate Programs by Category

Using these categories, we can assess the use of CIP codes to identify patterns and areas of improved harmonization (Figure 12 and Figure 13).

Cybersecurity

Seventy-one percent of exclusive cybersecurity programs (e.g., BS or AAS in Cybersecurity) use a CIP code from the Computer and Information Sciences and Support Services family. Specifically, 59% of these programs have been assigned the “Computer and Information Systems Security/Auditing/Information Assurance” code. Some programs use a “Computer Science” or “Computer Systems Networking and Telecommunications” code, which could potentially indicate that they have spun out of another program but are still using the CIP code of this previous program.

Cyber Defense

CIP code use among cyber defense programs is relatively consistent. Most programs use the primary “Computer and Information Systems Security/Auditing/Information Assurance” code, followed by “Cyber/Electronic Operations and Warfare”. One program has been assigned, “Computer Systems Networking and Telecommunications”.

Cyber Crime and Forensics

First, programs focusing on cybercrime or digital forensics are evenly split between the “Computer and Information Sciences and Support Services” and the “Homeland Security, Law Enforcement, Firefighting, and Related Protective Services” CIP code families. The most common CIP codes assigned in this group include the widely used “Computer and Information Systems Security/Auditing/Information Assurance” and “Cyber/Computer Forensics and Counterterrorism”.

Business & Accounting

More than half of the programs focusing on Business & Management or Compliance & Accounting also use the common “Computer and Information Systems Security/Auditing/Information Assurance.” Beyond two degrees in Cybersecurity Compliance and Business Administration with a concentration in cybersecurity, most of these programs are Cybersecurity Management programs. Currently, no CIP code specifically refers to these types of pathways.

Cyber and Cybersecurity Engineering

Several programs categorized as belonging to the “Engineering” sector offer degrees in Information Security Engineering and again use codes related to Computer and Information Sciences. However, CIP code use is very disparate for programs focusing on Cybersecurity Engineering as codes range from “Computer Science” to “Network and System Administration” and “Cyber/Electronic Operations and Warfare,” or even “Laser and Optical Engineering.”

Computer Science

As highlighted in the previous section, most Computer Science programs in the dataset are Computer Science degrees with a track, concentration, or specialization in cybersecurity. Despite this emphasis on cybersecurity, most programs still use a Computer Science-related CIP code or the generic “Computer and Information Sciences, General”. Only a handful use the “Computer and Information Systems Security/Auditing/Information Assurance” or the “Cyber/Electronic Operations and Warfare” codes that are more specifically targeting cybersecurity or information security.

Information "Assurance"

The Information Assurance Science/Systems/Security group is the second largest and contains programs focusing on various pathways. The most common is Information (Systems) Security, followed by Information Assurance. Some of these programs also offer a concentration in cybersecurity. Some are computer science programs with a specialization in Information Security or Assurance.

As a result, 92% of these programs use CIP codes from the “Computer and Information Sciences and Support Services” family. Again, “Computer and Information Systems Security/Auditing/Information Assurance” is the most used CIP code, followed by “Information Technology.”

Four programs appear miscoded. For example, a Cybersecurity Certificate is coded as “Computer Support Specialist”, while a Bachelor’s in Information Technology with a Concentration in Cybersecurity is coded as “Financial Forensics and Fraud Investigation.”

Other

Finally, programs coded as “Other” include degrees that do not clearly belong to the other groups listed above, which, for example, include Cyber Operations or Cyber Threat Intelligence. While most of these degrees also use “Computer and Information Systems Security/Auditing/Information Assurance” as their CIP code, some are assigned codes from the “Homeland Security, Law Enforcement, Firefighting, and Related Protective Services” family.

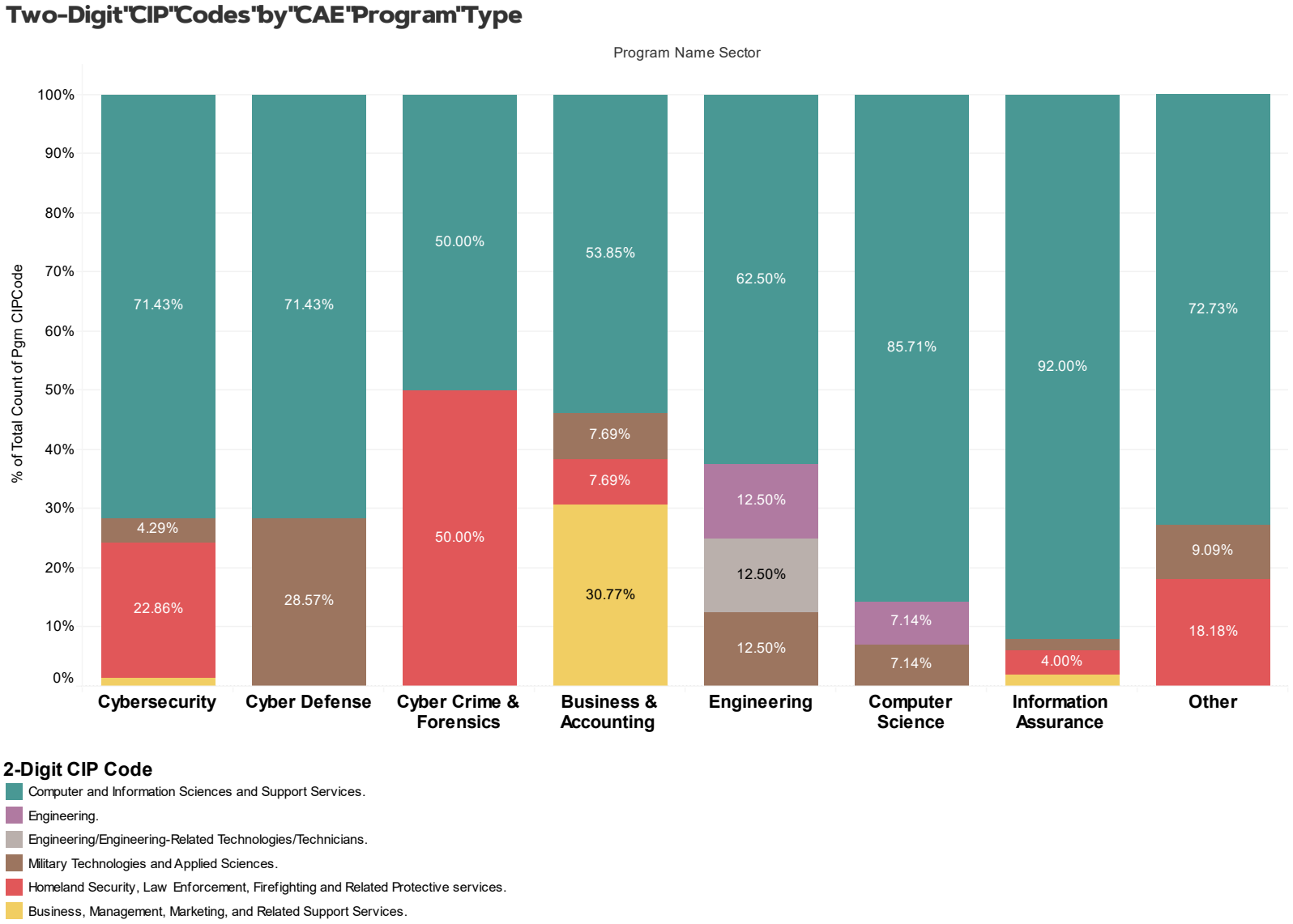

Figure 12. Two-Digit CIP Codes by Program Type

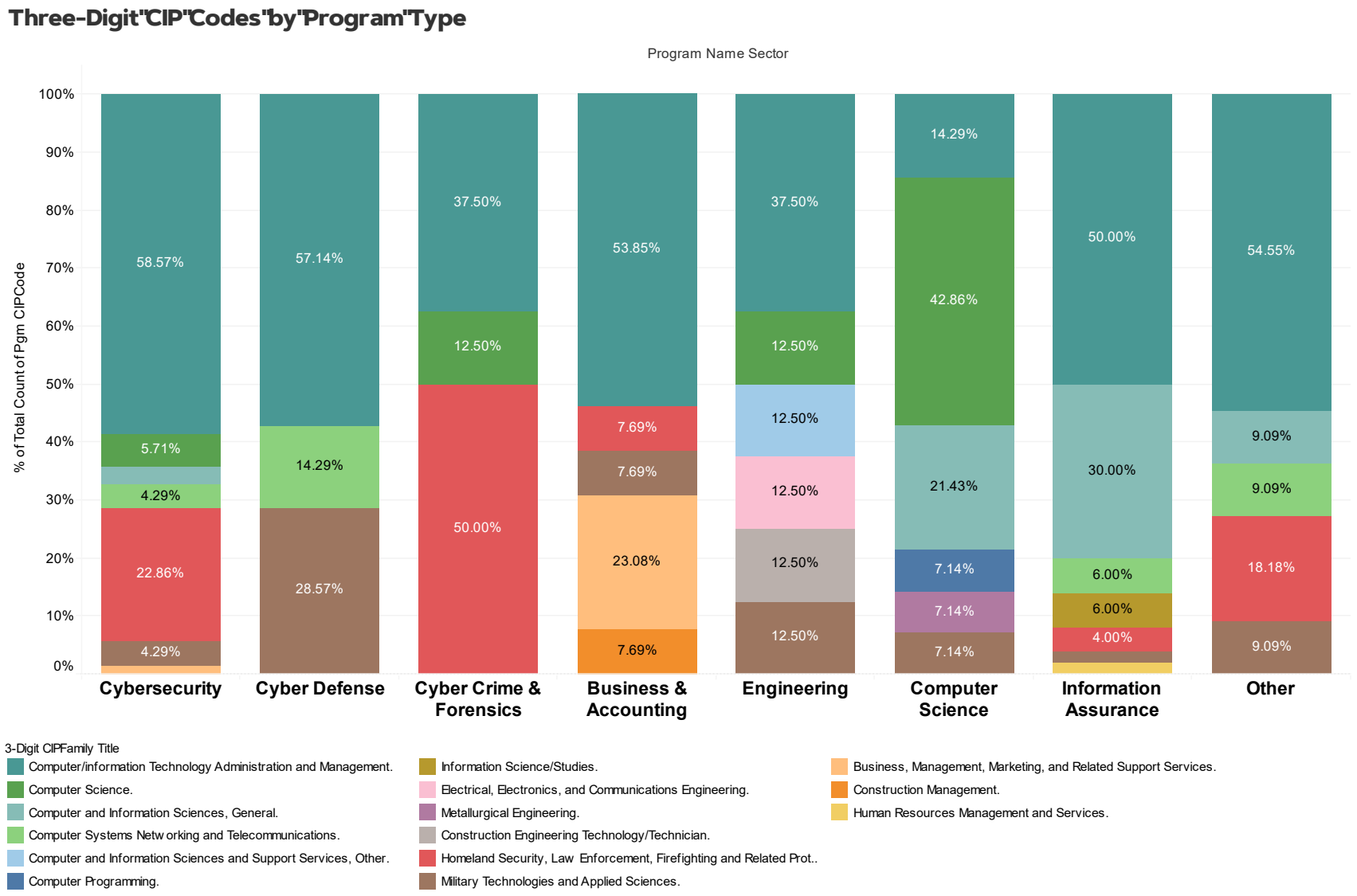

Figure 13. Three-Digit CIP Codes by Program Type

CIP Code Use in non-CAE-Designated Institutions

The analysis was then extended to institutions that do not currently have a CAE designation. As explained in the previous section, a significant share of cybersecurity-related programs are concentrations or special tracks in more general Computer Science and Business Administration. Due to data limitations, it is impossible to determine which Computer Science and Business Administration programs at non-CAE-designated institutions fall into this category. They are thus excluded from the two following analyses of how various cybersecurity programs use CIP codes (Figure 14, Figure 15, and Figure 16).

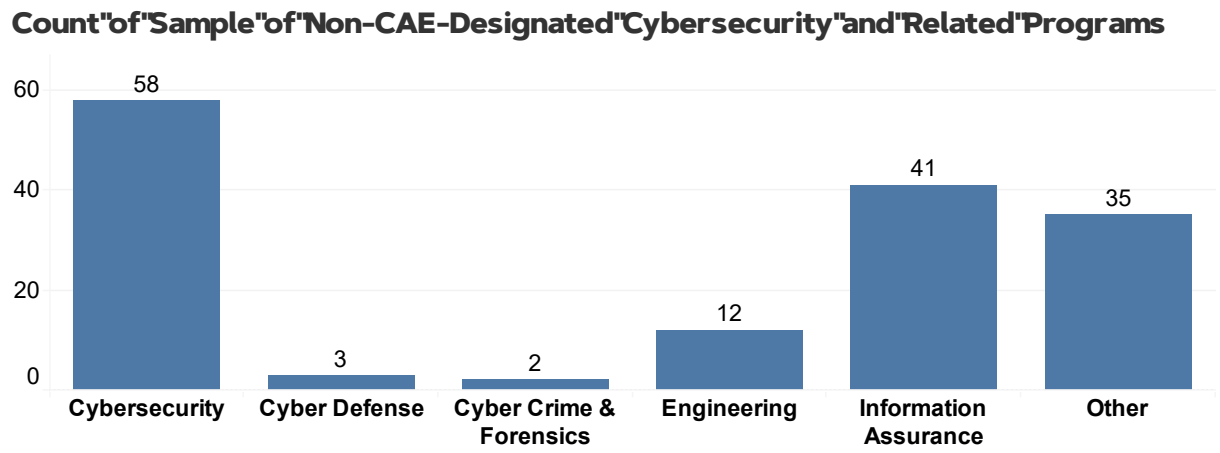

Figure 14. Count of Sample of Non-CAE-Designated Cybersecurity and Related Programs by Category

Cybersecurity

As outlined in earlier sections, most (83%) programs focusing on cybersecurity (including degrees in cybersecurity analytics or -management) use CIP Code 11.1003 corresponding to "Computer and Information Systems Security/Auditing/Information Assurance." It is followed by "Computer and Information Sciences, General" (7%) and "Cybersecurity Defense Strategy/Policy" (3% of cybersecurity programs). Regarding sub-sectors, programs focusing on cybersecurity management or governance also use 11.1003, except one using the "Management Information Systems" code. Finally, a single non-management-related cybersecurity program used a Human Resources Management and Services (52) code, potentially indicating that this program had spun off another program.

Cyber Defense

The sample size for cyber defense programs is relatively small, but most programs also use CIP Code 11.1003, which corresponds to "Computer and Information Systems Security/Auditing/Information Assurance." Another one, focusing on networking and cybersecurity, elected a code more representative of telecommunication networks (code 11.0901 Computer Systems Networking and Telecommunications).

Cyber Crime and Forensics

Only two forensics programs are explicitly related to cybersecurity in the sample. These digital forensics programs prepare students to conduct cybersecurity investigations to solve computer,

mobile, or network crimes, among others and typically expose them to a mix of criminal justice and computer science coursework. These programs use a CIP code from the “Homeland Security, Law Enforcement, Firefighting, and Related Protective Services” family.

Cyber and Cybersecurity Engineering

The sample also includes cybersecurity engineering programs. All but one use CIP Code 11.1003 corresponding to “Computer and Information Systems Security/Auditing/Information Assurance.”, consistent with the regular cybersecurity programs. A single program uses a code from the engineering family (14.0999: “Computer Engineering, Other”).

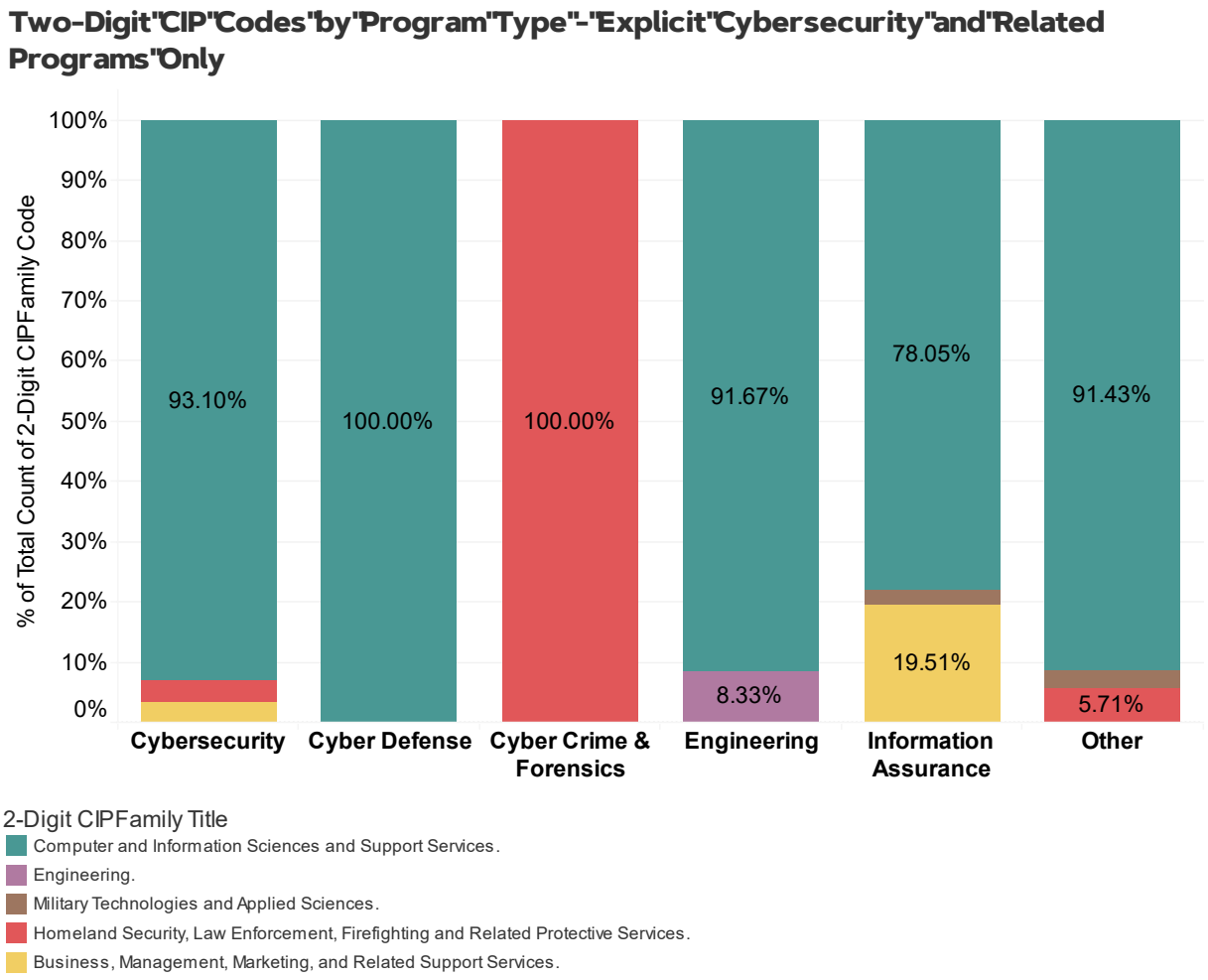

Figure 15. Non-CAE Cybersecurity and Related Programs Two-Digit CIP Codes

Information Assurance

The Information Assurance program category includes a variety of programs, the majority of which are Computer Information Systems or Computer Information Technology. While most use the Computer and Information Sciences General CIP code, a minority uses another from business administration: Human Resources Management and Services. Programs were likely spun off from Management Information Systems programs and have not updated their CIP code since.

Other programs in this category are related to information, data, and software security and use a Computer/Information Technology Administration and Management CIP code. A single degree related to cyber and information operations uses a code from the Military Technologies family.

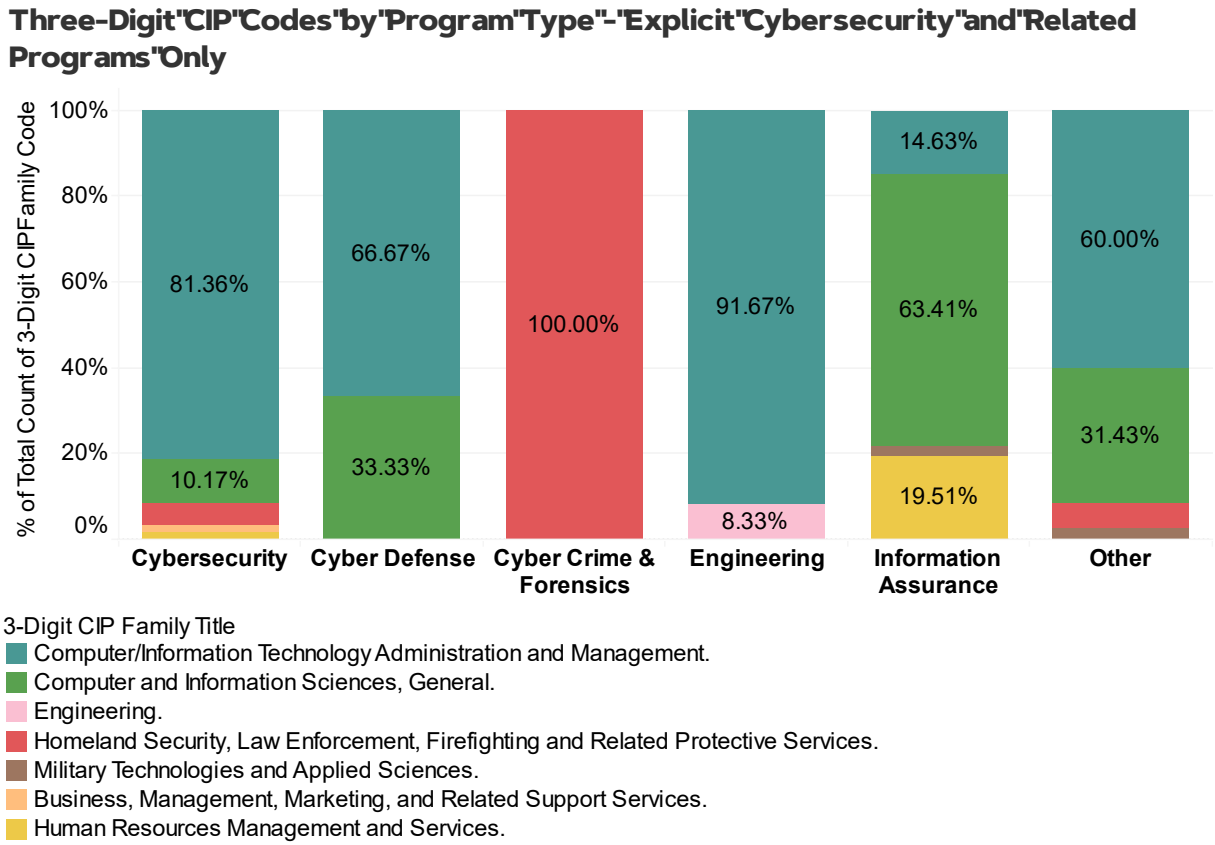

Figure 16. Non-CAE-Designated Program Three-Digit CIP Codes by Program Type

Other

Finally, the Other category includes a variety of programs, notably those in cyber operations, critical infrastructure, or cyber intelligence security. Almost all programs in this category use a CIP code from the "Computer and Information Sciences and Support Services" family, with again CIP Code 11.1003 "Computer and Information Systems Security/Auditing/Information Assurance" being the most common.

While critical infrastructure and cyber operations programs use this latter code, cyber intelligence security programs use "Cyber/Computer Forensics and Counterterrorism" instead. Finally, this category also has computer network and systems administration programs that unsurprisingly use the "Network and System Administration/Administrator" and "Computer Systems Networking and Telecommunications."

Work Role Alignment

The third part of the analysis consisted of comparing the work roles in the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF) to the established CIP and SOC categories to create a crosswalk between these classifications (see Appendix A for an

overview of these frameworks' structure). The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) was created to support the development of a workforce that can manage cybersecurity risks (Appendix). The DCWF was developed to support DOD's holistic workforce management by identifying, tracking, and reporting highly skilled priority cyber occupations. This framework comprises 71 work roles in seven categories (Appendix).

The DOD leveraged the work of NICE to create the DCWF. As a result, work roles in the DCWF significantly overlap with those in the NICE framework, as 46 out of the 48 roles in the NICE Framework can be found in the DCWF Framework (Figure 17). There are, however, a couple of categories that either only exist or are significantly more detailed in one system. For example, Data/AI only appears in DCWF, and there are no corresponding positions in NICE. Similarly, while Cyberspace Effects appear in both frameworks, DCWF work roles in this category are more varied and encompass a more diverse skill set.

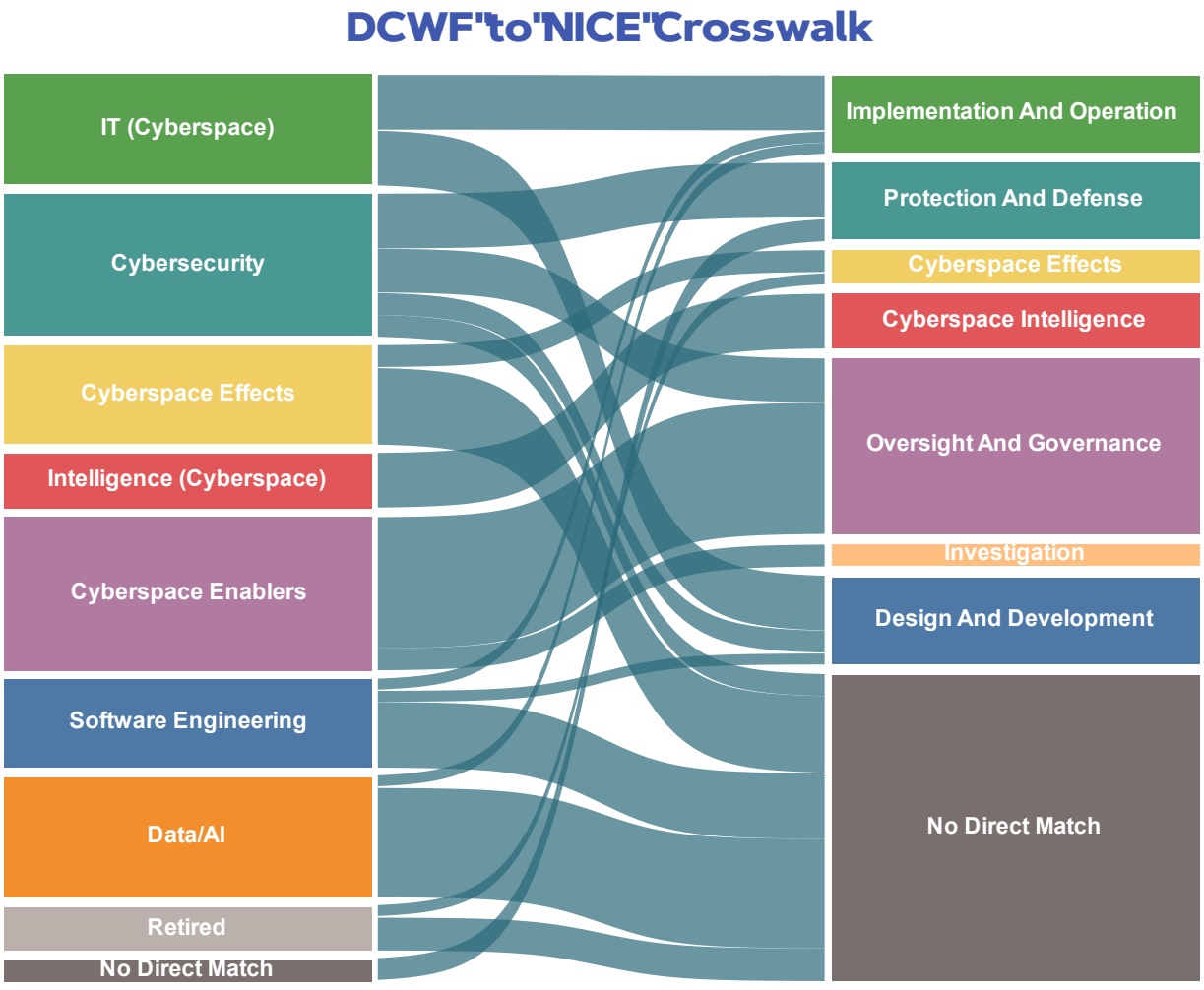

Figure 17. DCWF to NICE Framework Comparison

Work Roles with a Direct Match

The charts below show work roles in the NICE Framework and DCWF, which are straightforward and relatively direct matches in the SOC classification. A SOC code is considered a direct match if its official title is the same as the work role title, if the work role is included as an example job title in the SOC code's definition provided by the Department of Labor, or if the SOC code's definition describes the work role well (Figure 18).

Data/AI

The DCWF workforce category with the most direct matches is the Data/AI category. The roles in this category tend to be sector-agnostic, so their title does not indicate a direct link to cybersecurity and other related industries. For example, this category includes general roles such as Data Analysts, Data Scientists, or Data Architects. As a result, SOC codes already include and reflect a number of the Data/AI roles.

Cyberspace

Similarly, work roles in the IT (Cyberspace) are traditional roles that have long existed in the information technology space and are thus well represented in the SOC classification. Such codes include, for example, Systems Administrators and Database Administrators.

Regarding cyber-specific roles, only a couple have a strong, unique match in the SOC classification. These include Cyber Defense Infrastructure Support Specialist, Vulnerability Assessment Analyst, Secure Software Assessor, and Forensics Analyst. This could be explained by the fact that these roles have been used for years and widely adopted across industries.

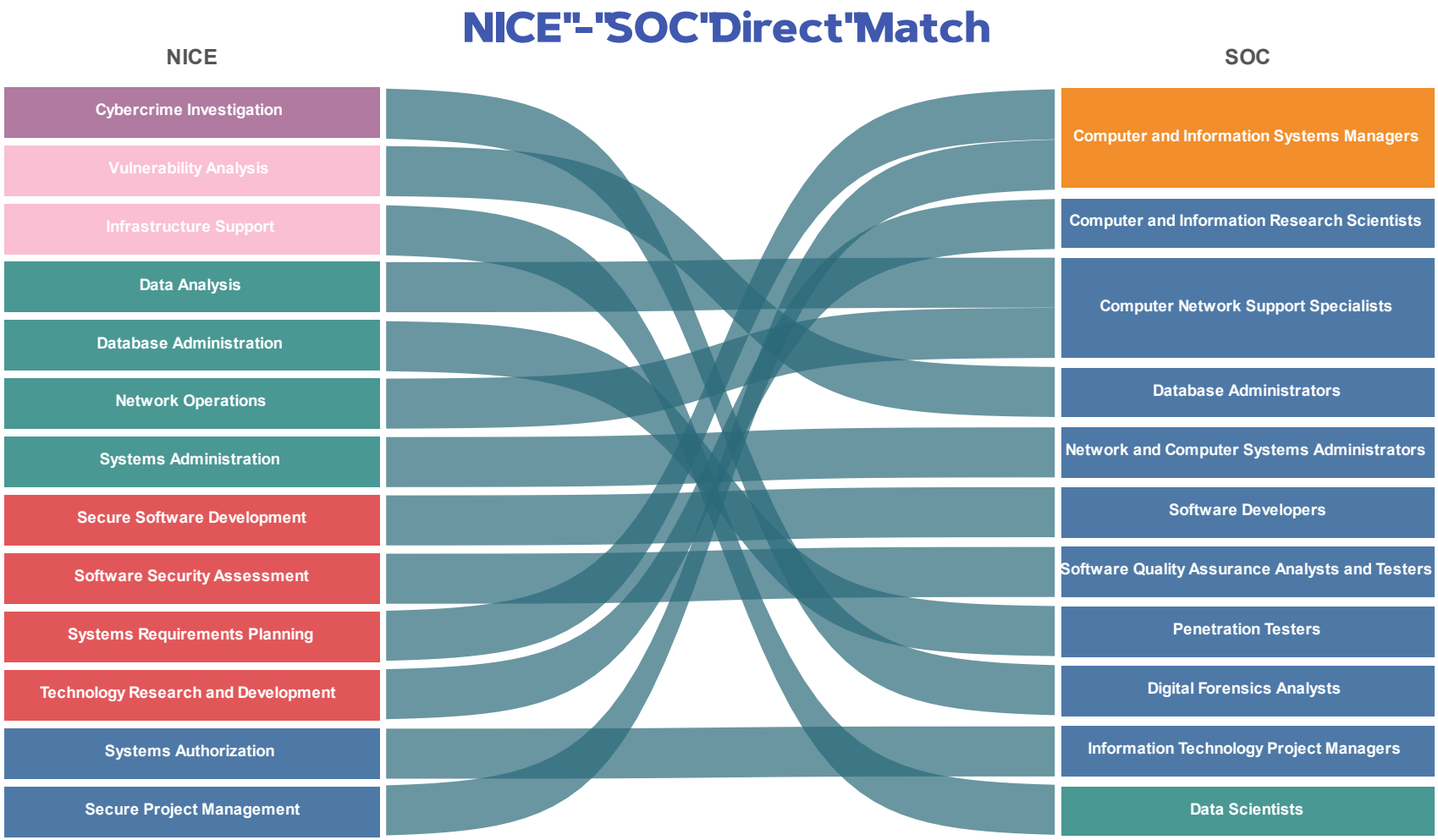

Figure 18. NICE Work Roles with Exact Match in SOC Classification

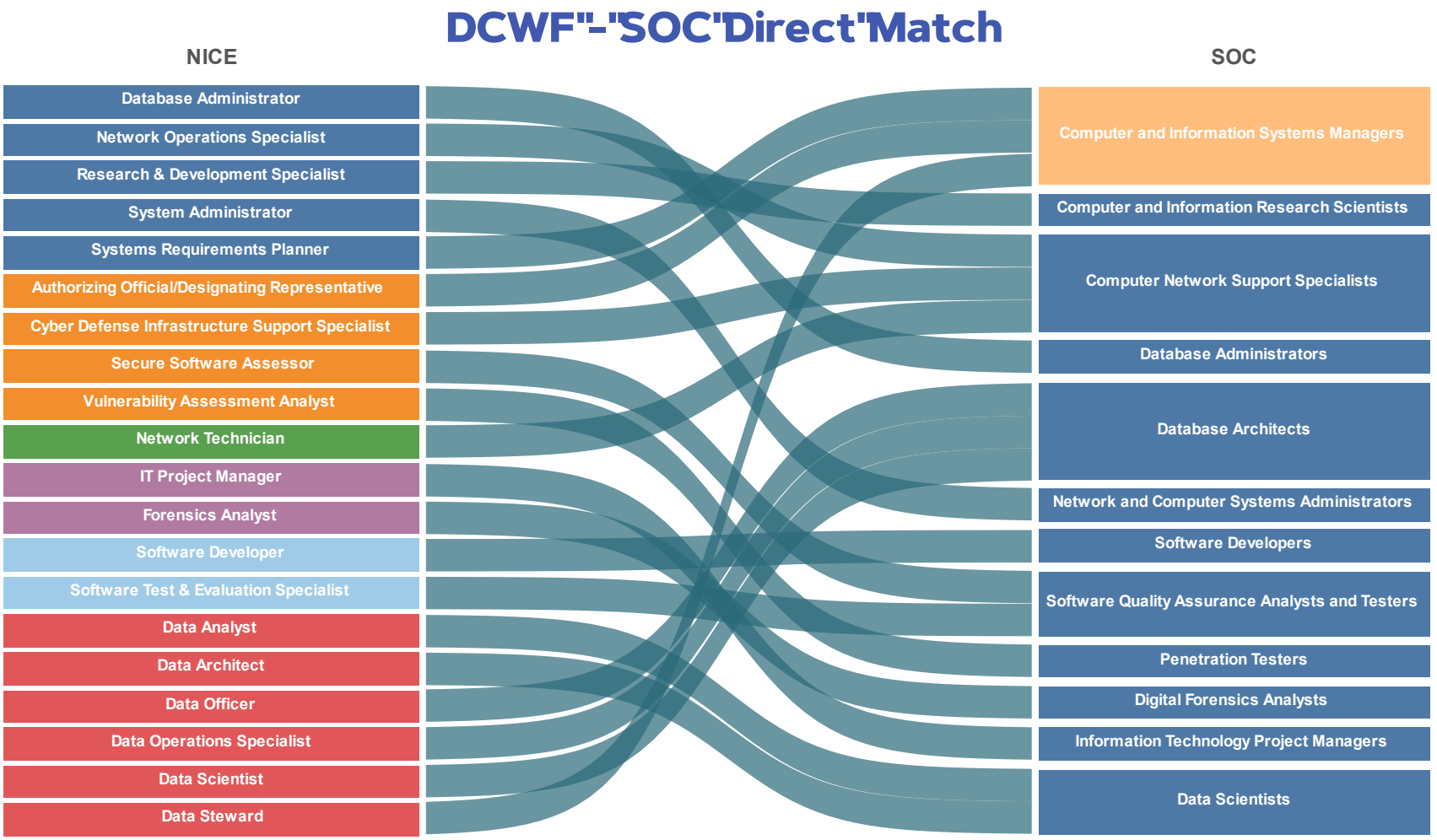

Figure 19. DCWF Work Roles with Exact Match in SOC Classification

Work Roles with Multiple Matches

Work roles in the NICE Framework and DCWF with more specific cybersecurity and nuanced focus do not have a direct counterpart in the SOC classification framework. Such roles were created more recently to better structure the cybersecurity workforce but often sit at the intersection of a technical sector-specific role and a more general administration or managerial role. Due to this intersection, these roles do not directly correspond to only one SOC code but potentially correspond to multiple SOC occupations.

Developers and Managers

"Cyber Workforce Developer and Manager" is a work role at the intersection of technical and managerial. It has five potential SOC code matches due to the various job requirements of this role. The DCWF description for this role is to:

> *[D]evelop cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training, and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.*

This role could be considered a technical human resources manager dedicated to developing an agency cyber workforce. It can thus be linked to multiple SOC occupations, including Human Resources Managers, Training and Development Managers, or Information Technology Project Managers.

Planners and Managers

Cyber-specific Planners and Managers also have a poor direct counterpart link to the SOC classification. Cyber Policy and Strategy Planners, AI Innovation Leaders, and All-Source Collection Managers have multiple potential SOC code matches due to their highly nuanced job description.

This lack of direct matches at the planning and management level echoes findings from the CIP code analysis. While codes already exist for post-secondary programs and occupations related to analysis work, this is not the case for management and administration work. Even though post-secondary programs and work roles in cyber management exist, similar CIP and SOC codes do not.

Specialist Roles

Finally, there are various highly specific codes like "AI Test & Evaluation Specialist," "Cyber Crime Investigator," "Target Analyst," or "Multi-Disciplined Language Analyst" that arose in recent years and do not yet have clear matches in the SOC classification. While SOC codes dedicated to law enforcement exist, they do not yet reflect a potential application to the cyber workforce.[2]

[2] SOC is revised every ten years. The last revision was published in 2018. The revision process takes several years; the 2028 revision process began in 2024. New occupations are determined when tasks, titles, education and training, and tools and technologies are adequately distinct from other occupations, and the number of workers in the proposed occupation and the types of employers are such that data can be adequately collected on the occupation.[12]

For example, SOC code 33-3021.00 is dedicated to Detectives and Criminal Investigators, which could potentially encompass “Cyber Crime Investigator.” Similarly, work roles more likely to be related to the public sector and military, such as Target Analyst, might not have a counterpart in

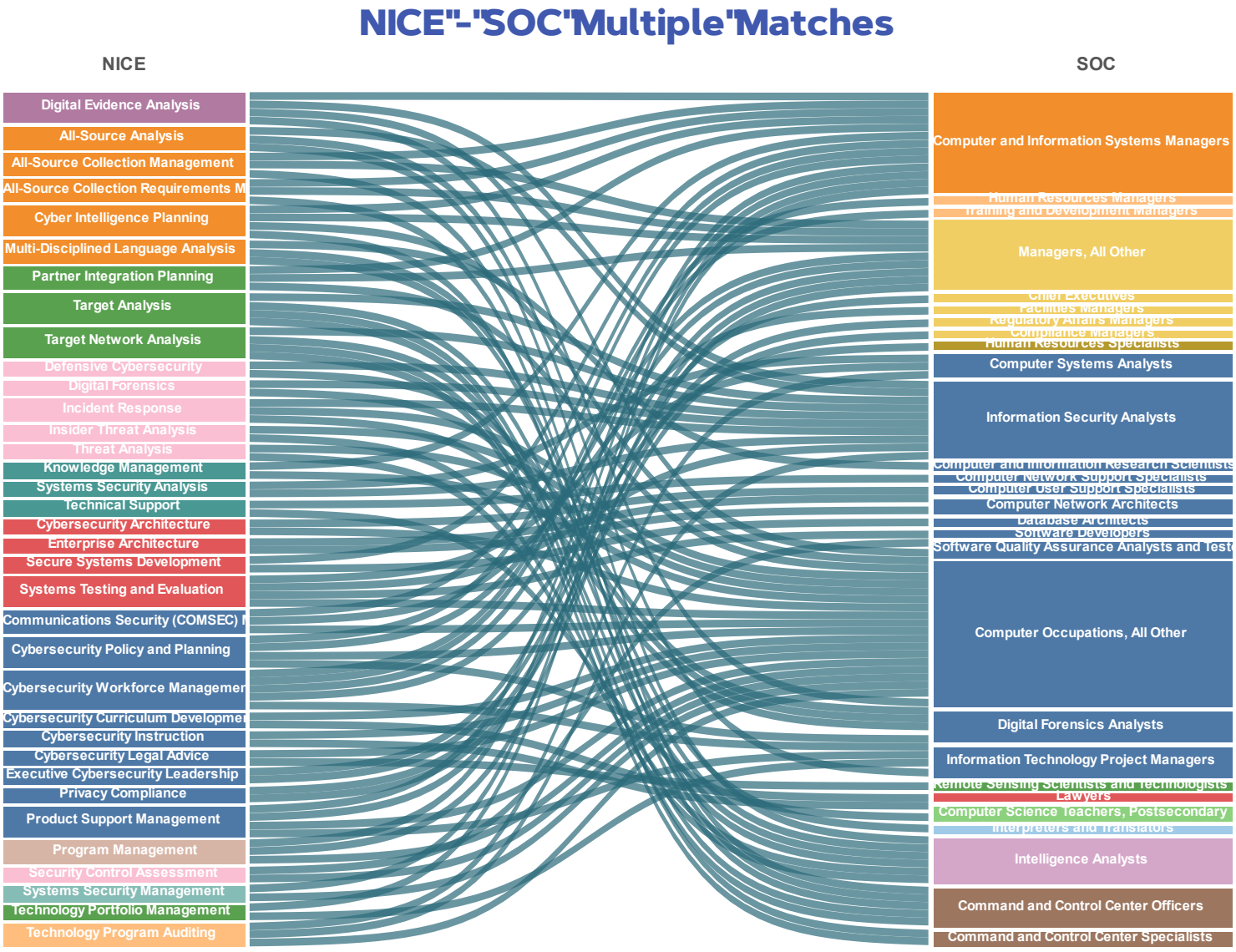

Figure 20. NICE Work Roles with Multiple Potential Matches in SOC Classification

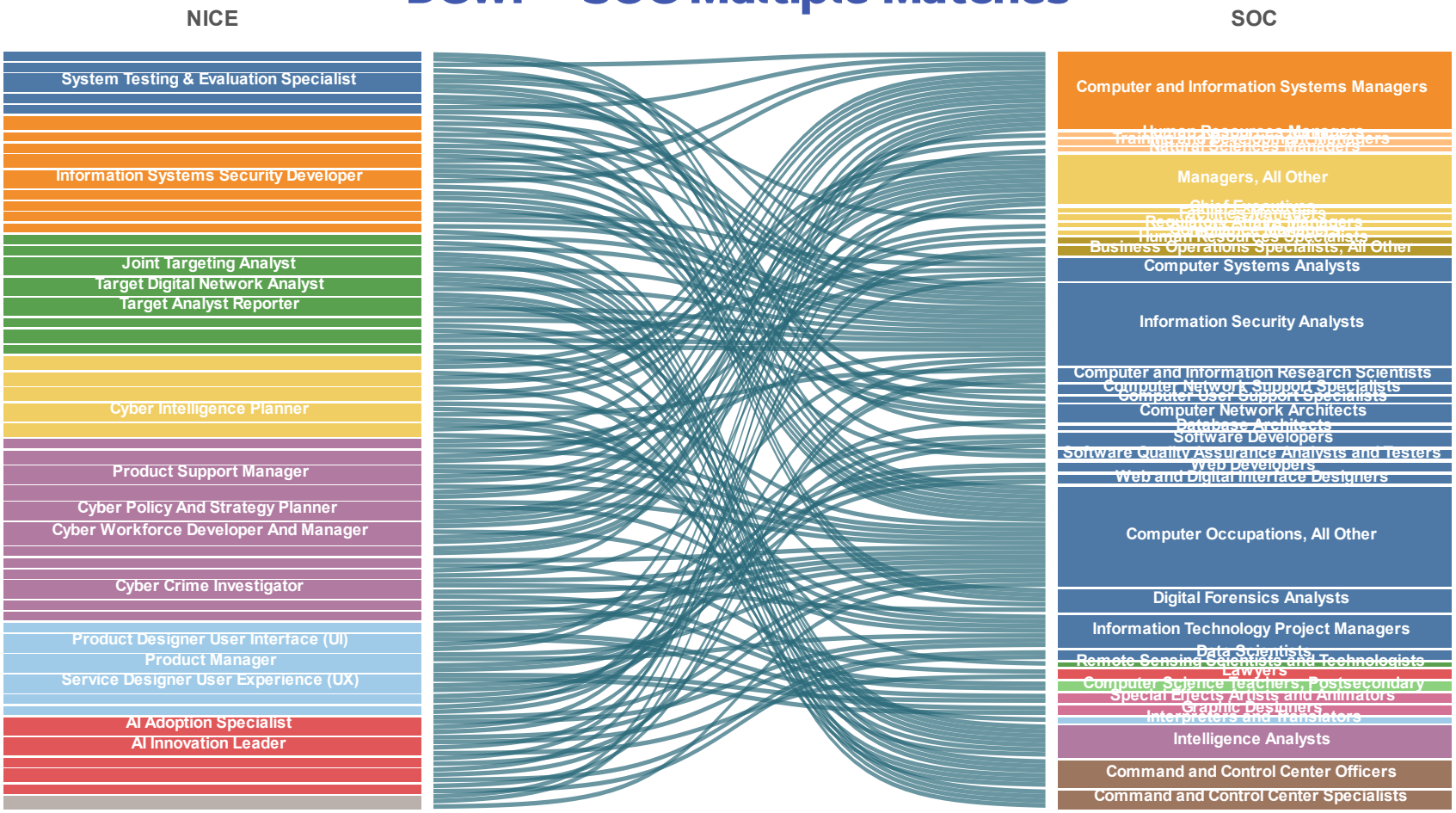

Figure 21. DCWF Work Roles with Multiple Potential Matches in SOC Classification

the SOC code classification and would instead be designated as “Military–Only Occupations” in most labor market data analytics platforms, severely limiting the ability to identify trends and retrieve labor estimates.

Conclusion

Approximately half of the CAE-designated programs use the “Computer and Information Systems Security/Auditing/Information Assurance” CIP code (11.1003). It is particularly used by programs most directly related to cybersecurity—Bachelor or Master of Science in Cybersecurity, for example—and is very common among information assurance or information security degrees. This is the most appropriate general-use cybersecurity code; thus, these programs are likely correctly coded.

Cyber-explicit CIP codes with cyber or cybersecurity in the title, such as “Cyber/Computer Forensics and Counterterrorism are much less common. Their description is more likely to point to military careers, but such programs are rarer among CAE-designated programs, explaining their infrequent occurrence in the dataset.

The “Computer Science” is also frequently assigned to CAE-designated programs, most of which are computer science degrees with a concentration or track in cybersecurity. Because graduates from these specialty tracks will fall under the umbrella of “Computer Science,” it becomes impossible to assess the number of computer science students with cyber-specific skills across postsecondary institutions in the United States. A similar situation occurs for a small number of business management programs that offer cybersecurity components but still use a more generic business-related CIP code.

Recommendations

Specialty Tracks

Post-secondary programs with cybersecurity tracks embedded in larger programs should be encouraged to use another more explicitly cyber-related code like “Computer and Information Systems Security/Auditing/Information Assurance.” Alternatively, creating a new CIP code in the 11.07 family (Computer Science) more explicitly related to cybersecurity could lead more institutions to use this new CIP code for their Computer Science students graduating with a concentration in cybersecurity.

Cybersecurity Management

More than half of the programs focusing on Business & Management or Compliance and Accounting also use the common “Computer and Information Systems Security/Auditing/Information Assurance.” Beyond two degrees in Cybersecurity Compliance and Business Administration with a Concentration in Cybersecurity, most of these programs are Cybersecurity Management programs. Currently, no CIP code specifically refers to these types of pathways.

Given the detailed management work roles in both the NICE and DCWF frameworks, it would potentially be beneficial to create such a code to categorize these related programs. This would help count students aiming to secure management positions in cybersecurity as distinct from students preparing to enter individual contributor roles. This may be of particular value if it is

important to distinguish incumbent cybersecurity workers seeking career advancement from cybersecurity graduates prepared for entry-level positions.

Though post-secondary programs and work roles in cyber management exist, there are no related CIP and SOC codes. This highlights an opportunity to create new codes in both classification systems (CIP and SOC) to fill this gap and better represent those leading and managing cybersecurity tasks and related workforce development.

Update CIP Codes Following Program Splits

Some explicitly cybersecurity-focused programs, like a Bachelor in Cybersecurity are assigned a “Computer Science” or “Computer Systems Networking and Telecommunications” code, which could indicate that they have spun out of another program but are still using the CIP code of this previous program. Encouraging and reminding program administrators to update CIP codes upon creating new programs and eventually providing a grid specifying the former and new program names and the most appropriate CIP codes for each could help avoid these cases.

Creating Cyber-Specific Codes in Law Enforcement Categories

Advocating for the inclusion of cyber-specific occupations, such as Target Analysts, Cyber Intelligence Planners, or Cybercrime Investigators, in the SOC classification would further support efforts to estimate the size of the cybersecurity workforce. Encouraging the Department of Labor to include these job titles as an example of the closest related SOC codes or create a separate code for these cyber-specific roles could bring additional clarity.

Appendix A

Classification and Framework Code Structures

Table 5. Classification and Framework Code Structures

Classification/ Framework	Name	Organization	Object of Classification	Scope	Structure	Family Indicator	Number of Families
CIP	Classification of Instructional Programs	National Center for Education Statistics	Instructional Programs	All US postsecondary programs	XX.XXXX	First 2 digits	50
SOC	Standard Occupational Classification	Bureau of Labor Statistics	Occupations	US Workforce	XX-XXXX.XX	First 2 digits	23
NICE	National Initiative on Cybersecurity Education	National Institute of Standards and Technology	Work Roles	US Cybersecurity Workforce	AA-AAA-XXX	First 2 letters	7
DCWF	Defense Cybersecurity Workforce Framework	Department of Defense	Work Roles	DOD Cybersecurity Workforce	XXX	N/A	7

Appendix "B"

CAE-Designated Institutions Survey

Section I: Contact Information

1) What is the name of the institution for which you are filling this out?

2) Please provide a primary point of contact for the cybersecurity program at your institution. Be sure to include the name, email, phone number, and department name.

Primary Contact Name: _____
Email: _____
Department Name: _____
Phone Number: _____

Section II: Institution Information

3) How would you categorize your academic institution? Please select one option. For more information on how to classify your institution, click here

- ○ Doctorate-Granting University
- ○ Master's College/University
- ○ Baccalaureate College
- ○ Associate College
- ○ Special Focus Institution
- ○ Tribal College
- ○ Other - Write In: _____

4) What is the CAE designation assigned to your institution? Please select all that apply.

- ☐ CAE-CD
- ☐ CAE-O
- ☐ CAE-R
- ☐ Validated but not designated
- ☐ None of the above

5) How many cybersecurity programs does your institution have?*: _____

Section III: Program Details

Note: this section was completed for each cybersecurity program based on the number entered in Q5

6) Please provide the following information for your cybersecurity program*:

- Program Name*: _____
- What is the six-digit CIP (Classification of Instructional Program) code of this program? For more information on CIP codes, click here*: _____
- What type of degree is awarded at the completion of your program?* Please select all that apply.
  - ☐ Certificate of Completion
  - ☐ AS - Associate of Science
  - ☐ AAS - Associate of Applied Science
  - ☐ BS - Bachelor of Science
  - ☐ MS - Master of Science
  - ☐ PhD - Doctorate
  - ☐ Other - Write In: _____
- Each branch of the military uses its own taxonomy for what is generally known as a Military Occupational Specialty (MOS) code. Does your institution grant credit for prior learning to military veterans based on their military occupational specialty (MOS) in this cybersecurity program? Please select one. For more details on MOS, click here *
  - ○ Yes
  - ○ No

If selected "Yes" to Q6-d above

7) What MOS credit(s) does this program provide? Please describe.

_____

_____

_____

Section IV: Program Transfer Pathways

NCyTE supports efforts by its member community colleges to develop transfer pathways. When two-year colleges make such agreements with four-year institutions, students graduating with an associate degree for transfer are able to transition smoothly into a related university program leading to a bachelor's degree. For more details on transfers and accreditation, click here.

8) Does your institution have a two-year college to four-year institution agreement for cybersecurity program transfer credit in your state? Please select one.

- ○ Yes
- ○ No

If selected "Yes" to Q8 above

9) If yes, how many two-year college to four-year institution agreements does your institution have for cybersecurity program transfer credit? _____

10) Does your institution currently have AP articulation agreements for cybersecurity program transfer credit with high schools in your state?

- ○ Yes
- ○ No

If selected "Yes" to Q10 above

11) If yes, how many high schools do you have AP articulation agreements with for cybersecurity program transfer credit? _____

Appendix "C"

Non-CAE Designated Institutions Selection Methodology

Obtaining Cyber Security Related CIP Codes

Researchers first identified CIP codes used by CAE-designated institutions from responses to the survey shown in Appendix A. A CIP code frequency distribution was then created to evaluate how often a CIP code was used by programs with clear cybersecurity content validated by the CAE designation. This frequency distribution was used to inform data collection for non-CAE-designated programs, assuming that non-CAE cybersecurity programs use CIP codes similar to those of CAE-designated programs.

This list was augmented by a careful review of the entire CIP code classification to identify other codes that were not reported in survey responses but could still be relevant to cybersecurity programs. For example, instructional programs preparing students for a career in public service and the military can be found in a handful of specialty institutions and are naturally scarce. As a result, survey responses from these programs were scant and did not represent the full variety of CIP codes used.

The research team then queried the IPEDS database using the abovementioned CIP codes. The database provided a wide range of data points for each 6-digit CIP code, including the institution name, the 2-digit CIP code family name, and each credential offered. Using the list of CIP codes above, the research team identified 15,448 unique, credentialed programs offered under these identified CIP codes in the United States.[3]

However, the IPEDS database does not provide specific program-level information. Thus, there is no way to determine whether a specific credential offered under an identified CIP code was a cyber security program using IPEDS data alone. To make this determination, the research team needed to obtain program-level data.

Obtaining Cyber Security Program-Level Data

The research team identified six state databases providing individual program and credential-level data organized by CIP codes: Georgia, Illinois, Michigan, Texas, and Virginia, while California's databases provided data only for community college programs. Each database was queried using the CIP codes identified above.

The results were then exported, compiled, and sorted by institution, program name, and credential. From these six states, 4,208 individual programs, from one-year certifications to doctoral research degrees, were identified under the queried CIP codes.

After compiling the program-level data from state databases, the research team then supplemented these data with CIP code data from other states, where some individual institutions sometimes make CIP code-level program information available. This approach produced program-level data for an additional 422 programs, resulting in 4,630 programs organized by institution, CIP code, and individual credentials.

[3] IPEDs CIP codes listed as double degree awards and programs with no credential-level data were excluded.

The compiled program-level data from the states was then merged into the original IPEDS CIP code data and sorted by institution, CIP code, and individual program name. Each program listed, whether cyber security or otherwise, was reviewed to ensure that the institution, CIP code, and credential listed on the IPEDs database matched those on the state database.

This allowed the research team to verify which programs listed on the IPEDs database were cyber security programs and which were not. This approach also allowed the team to capture cyber security credentials not listed on the IPEDs data.

Out of the original 15,448 unique programs listed under the identified CIP codes on the IPEDs database, the research team identified 399 cyber security programs, 217 of which were listed on the IPED database and 181 of which were not.

Researchers then leveraged the same classification methodology used for CAE-designated programs to sort non-designated programs according to their content and identify discrepancies between CIP code use and program content. It is important to note that while program titles and learning objectives were available for CAE-designated programs, researchers could only access program titles for non-CAE-designated programs and used these as a proxy for program content.

Appendix D

Common CAE-Designated Program CIP Codes[13]

CIP Code	Title and Description
11.1003	**Computer and Information Systems Security/Auditing/Information Assurance**
	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
11.0701	**Computer Science**
	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.
43.0404	**Cybersecurity Defense Strategy/Policy**
	A program that focuses on the study of strategy, policy, and standards regarding the security of and operations in cyberspace. Includes instruction in incident response, information assurance, recovery policies, vulnerability reduction, deterrence, threat reduction, and resiliency.
11.0101	**Computer and Information Sciences, General**
	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.
43.0403	**Cyber/Computer Forensics and Counterterrorism**
	A program focusing on the principles and techniques used to identify, search, seize and analyze digital media and to conduct cyber investigations against criminal and terrorist activity. Includes instruction in computer boot processes and drives, jumper setting, file access and reconstruction, hacking, network systems, cryptography, programming, investigative techniques, forensic imagery, web-based investigation methods, cyberterrorism, and applicable laws and administrative procedures.
29.0207	**Cyber/Electronic Operations and Warfare**
	A program that focuses on the technological and operation aspects of information warfare, including cyber attack and cyber defense. Includes instruction in computer and network security, cryptography, computer forensics, systems security

CIP Code	Title and Description
	engineering, software applications, threat and vulnerability assessment, wireless networks and satellite communications, tactical and strategic planning, legal and ethical issues, and cyber warfare systems development and acquisition.
11.0103	**Information Technology**
	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
11.0901	**Computer Systems Networking and Telecommunications**
	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.

Appendix "E"

NICE Work Roles

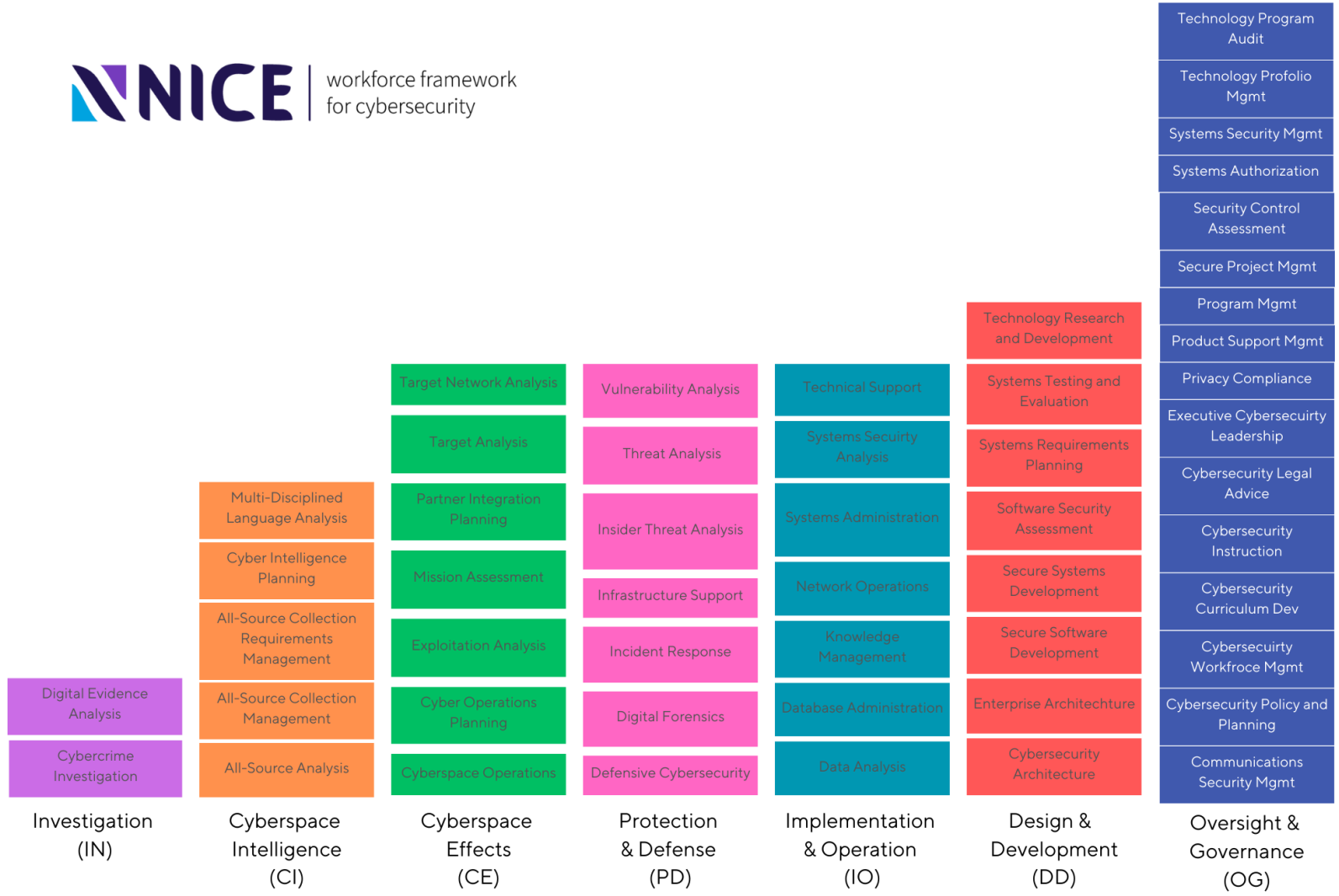

Figure 22. NICE Work Roles

Appendix F

DCWF Work Roles

Table 6. DCWF Work Roles

IT (Cyberspace)						
Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.						
(421) Database Administrator (651) Enterprise Architect	(431) Knowledge Manager (441) Network Operations Specialist	(661) Research & Development Specialist	(451) Systems Administrator (671) System Testing & Evaluation Specialist (632) Systems Developer	(641) Systems Requirements Planner (411) Technical Support Specialist		
Cybersecurity						
Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.						
(611) Authorizing Official Designating Representative (732) COMSEC Manager	(212) Cyber Defense Forensics Analyst (511) Cyber Defense Analyst	(521) Cyber Defense Infrastructure Support Specialist (531) Cyber Defense Incident Responder	(631) Information Systems Security Developer (722) Information Systems Security Manager	(622) Secure Software Assessor (652) Security Architect	(612) Security Control Assessor (462) Control Systems Security Specialist	(541) Vulnerability Assessment Analyst
Cyberspace Effects						
Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.						
(121) Exploitation Analyst (122) Digital Network Exploitation Analyst	(131) Joint Targeting Analyst (132) Target Digital Network Analyst	(442) Network Technician (133) Target Analyst Reporter	(443) Network Analyst (322) Cyberspace Operator (463) Host Analyst			

Intelligence (Cyberspace)						
Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.						
(111) All-Source Analyst (311) All-Source Collection Manager	(312) All-Source Collection Requirements Manager (331) Cyber Intelligence Planner	(151) Multi-Disciplined Language Analyst				
Cyberspace Enablers						
Personnel who perform work roles to support or facilitate the functions of cyber IT, cybersecurity, cyberspace effects, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training and leadership activities.						
Acquisition (804) IT Investment Portfolio Manager (805) IT Program Auditor (802) IT Project Manager	**Acquisition** (803) Product Support Manager (801) Program Manager	**Leadership** (752) Cyber Policy and Strategy Planner (751) Cyber Workforce Developer and Manager	**Leadership** (901) Executive Cyber Leader (732) Privacy Compliance Manager	**Legal & Law Enf.** (731) Legal Advisor (221) Cyber Crime Investigator	**Legal & Law Enf.** (211) Forensic Analyst	**Training & Education** (711) Curriculum Developer (712) Cyber Instructor
Software Engineering						
(627) DevSecOps Specialist (625) Product Designer User Interface (UI)	(806) Product manager (626) Service Designer User Experience (UX)	(628) Software Cloud Architect (621) Software Developer	(673) Software Test & Evaluation Specialist (461) Systems Security Analyst			
Data/AI						
(753) AI Adoption Specialist (902) AI Innovation Leader (733) AI Risk & Ethics Specialist	(672) AI Test & Evaluation Specialist (623) AL/ML Specialist	(422) Data Analyst (653) Data Architect (903) Data Officer	(624) Data Operations Specialist (423) Data Scientist	(424) Data Steward		

Appendix G

NICE Framework Roles with an Exact Match in SOC Classification

NICE Work Category	NICE Work Role ID	NICE Work Role	2018 SOC Code	2018 SOC Title
Investigation	IN-WRL-001	Cybercrime Investigation	15-1299.06	Digital Forensics Analysts
Protection & Defense	PD-WRL-004	Infrastructure Support	15-1231	Computer Network Support Specialists
	PD-WRL-007	Vulnerability Analysis	15-1299.04	Penetration Testers
Implementation & Operations	IO-WRL-001	Data Analysis	15-2051	Data Scientists
	IO-WRL-002	Database Administration	15-1242	Database Administrators
	IO-WRL-004	Network Operations	15-1231	Computer Network Support Specialists
	IO-WRL-005	Systems Administration	15-1244	Network and Computer Systems Administrators
Design & Development	DD-WRL-003	Secure Software Development	15-1252	Software Developers
	DD-WRL-005	Software Security Assessment	15-1253	Software Quality Assurance Analysts and Testers
	DD-WRL-006	Systems Requirements Planning	11-3021	Computer and Information Systems Managers
	DD-WRL-008	Technology Research and Development	15-1221	Computer and Information Research Scientists
Oversight & Governance	OG-WRL-011	Secure Project Management	15-1299.09	Information Technology Project Managers
	OG-WRL-013	Systems Authorization	11-3021	Computer and Information Systems Managers

Appendix H

DCWF Roles with an Exact Match in SOC Classification

DCWF Category	DCWF Code	DCWF Work Role	2018 SOC Code	2018 SOC Title
IT Cyberspace	421	Database Administrator	15-1242	Database Administrators
Cybersecurity	521	Cyber Defense Infrastructure Support Specialist	15-1231	Computer Network Support Specialists
	541	Vulnerability Assessment Analyst	15-1299.04	Penetration Testers
	611	Authorizing Official/Designating Representative	11-3021	Computer and Information Systems Managers
	622	Secure Software Assessor	15-1253	Software Quality Assurance Analysts and Testers
Cyberspace Effects	442	Network Technician	15-1231	Computer Network Support Specialists
Cyberspace Enablers	211	Forensics Analyst	15-1299.06	Digital Forensics Analysts
	802	IT Project Manager	15-1299.09	Information Technology Project Managers
Data/AI	422	Data Analyst	15-2051	Data Scientists
	423	Data Scientist	15-2051	Data Scientists
	424	Data Steward	11-3021	Computer and Information Systems Managers
	441	Network Operations Specialist	15-1231	Computer Network Support Specialists
	451	System Administrator	15-1244	Network and Computer Systems Administrators
	621	Software Developer	15-1252	Software Developers
	624	Data Operations Specialist	15-1243	Database Architects
	641	Systems Requirements Planner	11-3021	Computer and Information Systems Managers
	653	Data Architect	15-1243	Database Architects
	661	Research & Development Specialist	15-1221	Computer and Information Research Scientists
	673	Software Test & Evaluation Specialist	15-1253	Software Quality Assurance Analysts and Testers
	903	Data Officer	15-1243.00	Database Architects

Appendix 1

NICE Framework Roles with Multiple Matches

NICE Category Title	NICE Work Role ID	NICE Work Role	2018 SOC Code	2018 SOC Title
Investigation	IN-WRL-002	Digital Evidence Analysis	11-3021	Computer and Information Systems Managers
			15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other
			15-1299.06	Digital Forensics Analysts
Cyberspace Intelligence	CI-WRL-001	All-Source Analysis	15-1212	Information Security Analysts
			19-2099.01	Remote Sensing Scientists and Technologists
			33-3021.06	Intelligence Analysts
	CI-WRL-002	All-Source Collection Management	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			55-1015	Command and Control Center Officers
	CI-WRL-003	All-Source Collection Requirements Management	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			55-1015	Command and Control Center Officers
	CI-WRL-004	Cyber Intelligence Planning	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			55-1015	Command and Control Center Officers
	CI-WRL-005	Multi-Disciplined Language Analysis	15-1221	Computer and Information Research Scientists
			27-3091	Interpreters and Translators
			33-3021.06	Intelligence Analysts
Cyberspace Effects	CE-WRL-005	Partner Integration Planning	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
	CE-WRL-006	Target Analysis	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts

NICE Category Title	NICE Work Role ID	NICE Work Role	2018 SOC Code	2018 SOC Title
			55-1015	Command and Control Center Officers
			55-3015	Command and Control Center Specialists
	CE-WRL-007	Target Network Analysis	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
			55-1015	Command and Control Center Officers
			55-3015	Command and Control Center Specialists
Protection And Defense	PD-WRL-001	Defensive Cybersecurity	15-1212	Information Security Analysts
			15-1299.06	Digital Forensics Analysts
	PD-WRL-002	Digital Forensics	15-1212	Information Security Analysts
			15-1299.06	Digital Forensics Analysts
	PD-WRL-003	Incident Response	15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other
			15-1299.06	Digital Forensics Analysts
	PD-WRL-005	Insider Threat Analysis	15-1299	Computer Occupations, All Other
			33-3021.06	Intelligence Analysts
	PD-WRL-006	Threat Analysis	15-1299	Computer Occupations, All Other
			33-3021.06	Intelligence Analysts
Implementation And Operation	IO-WRL-003	Knowledge Management	11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
	IO-WRL-006	Systems Security Analysis	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
	IO-WRL-007	Technical Support	15-1231	Computer Network Support Specialists
			15-1232	Computer User Support Specialists
Design And Development	DD-WRL-001	Cybersecurity Architecture	15-1241	Computer Network Architects
			15-1299	Computer Occupations, All Other
	DD-WRL-002	Enterprise Architecture	15-1241	Computer Network Architects
			15-1243	Database Architects

NICE Category Title	NICE Work Role ID	NICE Work Role	2018 SOC Code	2018 SOC Title
	DD-WRL-004	Secure Systems Development	11-3021	Computer and Information Systems Managers
			15-1252	Software Developers
	DD-WRL-007	Systems Testing and Evaluation	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
			15-1253	Software Quality Assurance Analysts and Testers
			15-1299	Computer Occupations, All Other
Oversight And Governance	OG-WRL-001	Communications Security (COMSEC) Management	11-3013.00	Facilities Managers
			11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
	OG-WRL-004	Cybersecurity Curriculum Development	15-1299	Computer Occupations, All Other
			25-1021	Computer Science Teachers, Postsecondary
	OG-WRL-005	Cybersecurity Instruction	15-1299	Computer Occupations, All Other
			25-1021	Computer Science Teachers, Postsecondary
	OG-WRL-006	Cybersecurity Legal Advice	15-1299	Computer Occupations, All Other
			23-1011	Lawyers
	OG-WRL-002	Cybersecurity Policy and Planning	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
	OG-WRL-003	Cybersecurity Workforce Management	11-3121	Human Resources Managers
			11-3131	Training and Development Managers
			11-9199	Managers, All Other
			13-1071	Human Resources Specialists
			15-1299.09	Information Technology Project Managers
	OG-WRL-007	Executive Cybersecurity Leadership	11-1011	Chief Executives
			11-9199	Managers, All Other
	OG-WRL-008	Privacy Compliance	11-9199.01	Regulatory Affairs Managers

NICE Category Title	NICE Work Role ID	NICE Work Role	2018 SOC Code	2018 SOC Title
			11-9199.02	Compliance Managers
	OG-WRL-009	Product Support Management	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
	OG-WRL-010	Program Management	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
	OG-WRL-012	Security Control Assessment	15-1253	Software Quality Assurance Analysts and Testers
			15-1299	Computer Occupations, All Other
	OG-WRL-014	Systems Security Management	11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
	OG-WRL-015	Technology Portfolio Management	11-3021	Computer and Information Systems Managers
			15-1299.09	Information Technology Project Managers
	OG-WRL-016	Technology Program Auditing	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other

Appendix J

DCWF Framework Roles with Multiple Matches

DCWF Category	DCWF Code	DCWF Work Role	2018 SOC Code	2018 SOC Title
IT (Cyberspace)	411	Technical Support Specialist	15-1231	Computer Network Support Specialists
			15-1232	Computer User Support Specialists
	431	Knowledge Manager	11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
	632	Systems Developer	11-3021	Computer and Information Systems Managers
			15-1252	Software Developers
	651	Enterprise Architect	15-1241	Computer Network Architects
			15-1243	Database Architects
	671	System Testing & Evaluation Specialist	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
			15-1253	Software Quality Assurance Analysts and Testers
			15-1299	Computer Occupations, All Other
Cybersecurity	212	Cyber Defense Forensics Analyst	15-1212	Information Security Analysts
			15-1299.06	Digital Forensics Analysts
	462	Control Systems Security Specialist	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
	511	Cyber Defense Analyst	15-1212	Information Security Analysts
			15-1299.06	Digital Forensics Analysts
	531	Cyber Defense Incident Responder	15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other
			15-1299.06	Digital Forensics Analysts
	612	Security Control Assessor	15-1253	Software Quality Assurance Analysts and Testers
			15-1299	Computer Occupations, All Other
	631		11-3021	Computer and Information Systems Managers

		Information Systems Security Developer	15-1212	Information Security Analysts
			15-1241	Computer Network Architects
			15-1299	Computer Occupations, All Other
	652	Security Architect	15-1241	Computer Network Architects
			15-1299	Computer Occupations, All Other
	722	Information Systems Security Manager	11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
	723	ComSec Manager	11-3013.00	Facilities Managers
			11-3021	Computer and Information Systems Managers
			15-1299	Computer Occupations, All Other
Cyberspace Effects	121	Exploitation Analyst	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
	122	Digital Network Exploitation Analyst	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
	131	Joint Targeting Analyst	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
			55-1015	Command and Control Center Officers
			55-3015	Command and Control Center Specialists
	132	Target Digital Network Analyst	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
			55-1015	Command and Control Center Officers
			55-3015	Command and Control Center Specialists
	133	Target Analyst Reporter	15-1212	Information Security Analysts
			33-3021.06	Intelligence Analysts
			55-1015	Command and Control Center Officers
			55-3015	Command and Control Center Specialists
	322	Cyberspace Operator	15-1212	Information Security Analysts
			15-1299.06	Digital Forensics Analysts

			55-3015	Command and Control Center Specialists
	443	Network Analyst	15-1212	Information Security Analysts
			15-1231	Computer Network Support Specialists
	463	Host Analyst	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
Cyberspace Enablers	221	Cyber Crime Investigator	11-3021	Computer and Information Systems Managers
			15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other
			15-1299.06	Digital Forensics Analysts
	711	Cyber Instructional Curriculum Developer	15-1299	Computer Occupations, All Other
			25-1021	Computer Science Teachers, Postsecondary
	712	Cyber Instructor	15-1299	Computer Occupations, All Other
			25-1021	Computer Science Teachers, Postsecondary
	731	Cyber Legal Advisor	15-1299	Computer Occupations, All Other
			23-1011	Lawyers
	732	Privacy Compliance Manager	11-9199.01	Regulatory Affairs Managers
			11-9199.02	Compliance Managers
	751	Cyber Workforce Developer And Manager	11-3121	Human Resources Managers
			11-3131	Training and Development Managers
			11-9199	Managers, All Other
			13-1071	Human Resources Specialists
			15-1299.09	Information Technology Project Managers
	752	Cyber Policy And Strategy Planner	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
	801	Program Manager	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other

			15-1299	Computer Occupations, All Other
	803	Product Support Manager	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
	804	IT Investment/Portfolio Manager	11-3021	Computer and Information Systems Managers
			15-1299.09	Information Technology Project Managers
	805	IT Program Auditor	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
			15-1299	Computer Occupations, All Other
	901	Executive Cyber Leader	11-1011	Chief Executives
			11-9199	Managers, All Other
Intelligence (Cyberspace)	111	All-Source Analyst	15-1212	Information Security Analysts
			19-2099.01	Remote Sensing Scientists and Technologists
			33-3021.06	Intelligence Analysts
	151	Multi-Disciplined Language Analyst	15-1221	Computer and Information Research Scientists
			27-3091	Interpreters and Translators
			33-3021.06	Intelligence Analysts
	311	All-Source Collection Manager	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			55-1015	Command and Control Center Officers
	312	All-Source Collection Requirements Manager	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			55-1015	Command and Control Center Officers
	331	Cyber Intelligence Planner	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			55-1015	Command and Control Center Officers

Software Engineering	461	Systems Security Analyst	15-1211	Computer Systems Analysts
			15-1212	Information Security Analysts
	625	Product Designer User Interface (UI)	15-1254	Web Developers
			15-1255	Web and Digital Interface Designers
			27-1014	Special Effects Artists and Animators
			27-1024	Graphic Designers
	626	Service Designer User Experience (UX)	15-1254	Web Developers
			15-1255	Web and Digital Interface Designers
			27-1014	Special Effects Artists and Animators
			27-1024	Graphic Designers
	627	DevSecOps Specialist	15-1252	Software Developers
			15-1299	Computer Occupations, All Other
	628	Software/Cloud Architect	15-1241	Computer Network Architects
			15-1252	Software Developers
	806	Product Manager	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
Data/AI	623	AI/ML Specialist	15-1221	Computer and Information Research Scientists
			15-2051	Data Scientists
	672	AI Test & Evaluation Specialist	11-9121	Natural Sciences Managers
			15-1221	Computer and Information Research Scientists
			15-2051	Data Scientists
	733	AI Risk & Ethics Specialist	11-9199	Managers, All Other
			23-1011	Lawyers
	753	AI Adoption Specialist	11-3021	Computer and Information Systems Managers
			13-1199	Business Operations Specialists, All Other
			15-1299	Computer Occupations, All Other

			15-1299.09	Information Technology Project Managers
	902	AI Innovation Leader	11-3021	Computer and Information Systems Managers
			13-1199	Business Operations Specialists, All Other
			15-1299	Computer Occupations, All Other
			15-1299.09	Information Technology Project Managers
Retired	333	Partner Integration Planner	11-3021	Computer and Information Systems Managers
			11-9199	Managers, All Other
			15-1299	Computer Occupations, All Other