NICE Team,

A happy New Year to you all!

Per the recent invitation to offer comments and feedback on the NICE Cybersecurity Workforce Framework, By Light has drafted the attached response. Thank you for the opportunity to contribute to this discussion, and please do not hesitate to reach out with any questions you may have.

All the best,

Bradley Wolfenden
Business Development & Marketing Strategy
By Light, LLC. | EmberSec
Boulder, CO

National Initiative for Cybersecurity Education (NICE) Request for Comment

As a strong proponent for national standards in cybersecurity, By Light IT Professional Services LLC is pleased to provide our comments and lessons learned on the NICE Framework. We think everyone acknowledges that a general cybersecurity framework describing relevant work roles and skills for careers is necessary to help facilitate entry into and movement within the workforce, and we applaud the hard work by NIST and the community to champion that.

We feel that the domain of cyber is uniquely broad and deep, as well as constantly evolving, and that contributes to a myriad of confusing and sometimes intimidating barriers to the field. As instructors (of cybersecurity training and education for Military, Commercial and University courses), we found it helpful to create technical disciplines or specialty pathways that guide students (and fellow instructors) on how to approach cyber learning, and ultimately, to one of the many job openings as described in the NICE Cyber Workforce Framework. In the comments to specific questions posed in the RFC, we explain our use of the cyber technical disciplines as it relates to the NICE framework and other related standards.

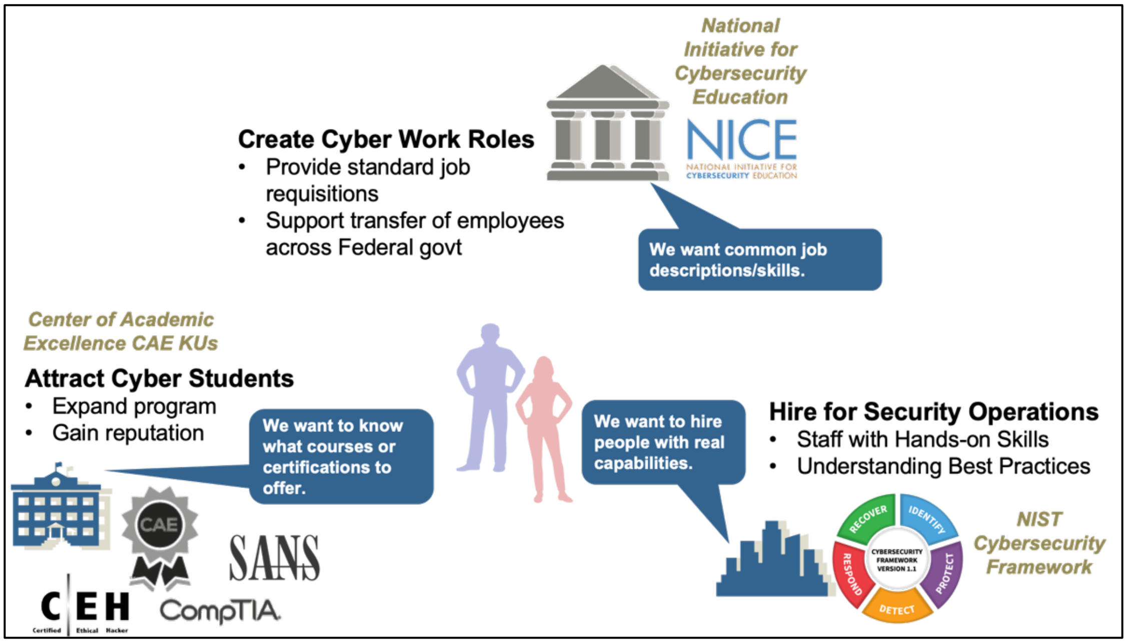
1. **What components of the NICE Framework have been most useful to you and why?**

   There are three related standards in Cybersecurity: the NICE Cybersecurity Workforce Framework, NIST Cybersecurity Framework and the DHS/NSA Center for Academic Excellence – Cyber Defense Education (CAE-CDE) with associated NSA Knowledge Units. These are all very helpful to industry, academia and students, but could be much closer aligned to reduce confusion. Figure 1 illustrates what the originators of each standard were working to accomplish.

   We consider the NICE Framework to be the authoritative source regarding job descriptions for government and industry. The common lexicon provided by the NICE Framework is helpful in standardizing cyber to support the consistent dialogue that is needed to defend our enterprises and organizational assets and enables mobility in the workforce across organizations (e.g., common reference of what an Incident Responder does). Standardized work roles with required KSAs and demonstrated Tasks, tied to what are best practices from NIST CSF, helps educators prepare a well-qualified workforce to match the personnel needed by hiring organizations.

   Workflow for Organizations Hiring in Cybersecurity: They want applicants to understand the best practices in cyber (from NIST CSF) and gain relevant performance hands-on in education (from CAE-CDE Schools) so that they can perform the various jobs/tasks in each work roll (from NICE).

   Best Practices → Performance of Hands-on Tasks → Work Roles → Job Descriptions



National Initiative for Cybersecurity Education

Create Cyber Work Roles

- Provide standard job requisitions
- Support transfer of employees across Federal govt

We want common job descriptions/skills.

Center of Academic Excellence CAE KUs

Attract Cyber Students

- Expand program
- Gain reputation

We want to know what courses or certifications to offer.

We want to hire people with real capabilities.

Hire for Security Operations

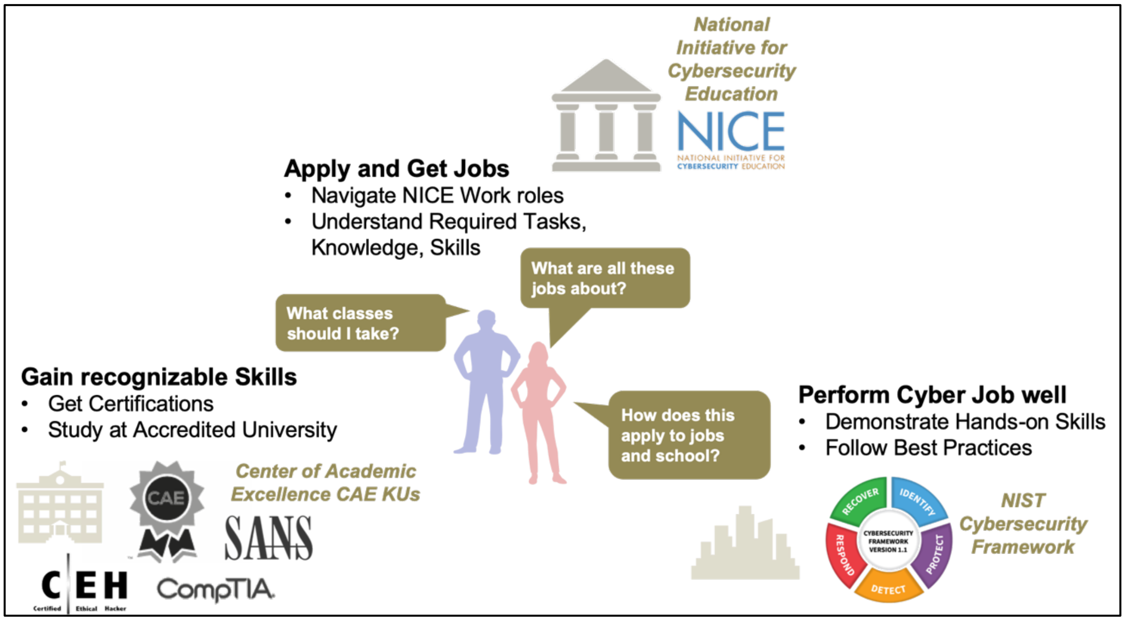
- Staff with Hands-on Skills
- Understanding Best Practices

NIST Cybersecurity Framework

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
CAE
SANS
CEH Certified Ethical Hacker
CompTIA
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Figure 1: Organizational Perspective on Standards

In the academic space, the NICE Framework can be used to help guide students towards various tracks or disciplines of study with a collection of courses (validated against the NSA KUs) that ultimately guides them to the jobs.



National Initiative for Cybersecurity Education

Apply and Get Jobs

- Navigate NICE Work roles
- Understand Required Tasks, Knowledge, Skills

What classes should I take?

What are all these jobs about?

Gain recognizable Skills

- Get Certifications
- Study at Accredited University

How does this apply to jobs and school?

Perform Cyber Job well

- Demonstrate Hands-on Skills
- Follow Best Practices

Center of Academic Excellence CAE KUs

NIST Cybersecurity Framework

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
CAE
SANS
CEH Certified Ethical Hacker
CompTIA
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Figure 2: Student Perspective

Students want to understand what the cyber field is about, what courses to take (from CAE-CDE), gain hands on-experience doing best practices and get the right job.

Cyber Disciplines → Courses → Hands-On Tasks to Perform → Work Roles

The challenge for students, instructors and academic institutions, is how all three standards relate. The Competencies Areas of NICE are useful in getting the high-level perspective on what is covered in the Framework. They're helpful to map from NICE to individual course topics/ NICE to NSA Center of Academic Excellence for Cyber Defense Education (CAE-CDE) Knowledge Units/NICE to the ACM Knowledge Areas and Curricula, but revisiting the NICE Competency Areas to focus on cybersecurity specifically, while leaving the general areas to other frameworks, would make mapping a more tractable problem (discussed further below).

2. **Describe what components of the NICE Framework have been least useful to you and why.**

The cybersecurity career pathway (Cyberseek.org) done in conjunction with NICE is a great idea to illustrate the various pathways to jobs, however, it doesn't align with the NICE work roles and therefore is confusing. With up-to-date mapping to NICE, it could be very helpful to students and educators.

3. **Share any key concepts or topics that you believe are missing from the NICE Framework. Please explain what they are and why they merit special attention.**

The individual tasks and associated KSAs are incredibly important as a method to check if an applicant is able to perform on the job (or to build assessment measures to certify them). **An explicit mapping of the NICE Work Roles and Tasks to the NIST Cybersecurity Framework (NIST CSF) subcategories** would help organizations (and practitioners) better apply Tasks to best practices in cyber. That mapping also helps organizations see how a cyber defense team in a Security Operations Center (SOC) might be aligned with NICE Work Roles. A similar mapping of NICE Competency Areas to CAE-CDE KUs (and the inverse of CAE-CDE KUs to NICE Work Roles) would be helpful as a supporting product on the website (there is a hard to find spreadsheet titled NICE_KU_Mapping_SME_Final_20_Mar_2015.xls that could be updated and made part of the standard NICE documentation).

4. **Describe how the NICE Framework can be more useful to a variety of audiences (i.e., employers, employees, education and training providers, learners, small enterprises, etc.).**

For Hiring Organizations in Industry:

It would be useful for organizations to be able to see example structures and work roles (so they could hire the right types of people using the NICE Work Roles, Tasks and KSAs). For example, a typical SOC is organized as shown in Figure 3. The total size of the SOC can vary from 1-50 people or more – all working together to meet the best practices defined by the NIST CSF.

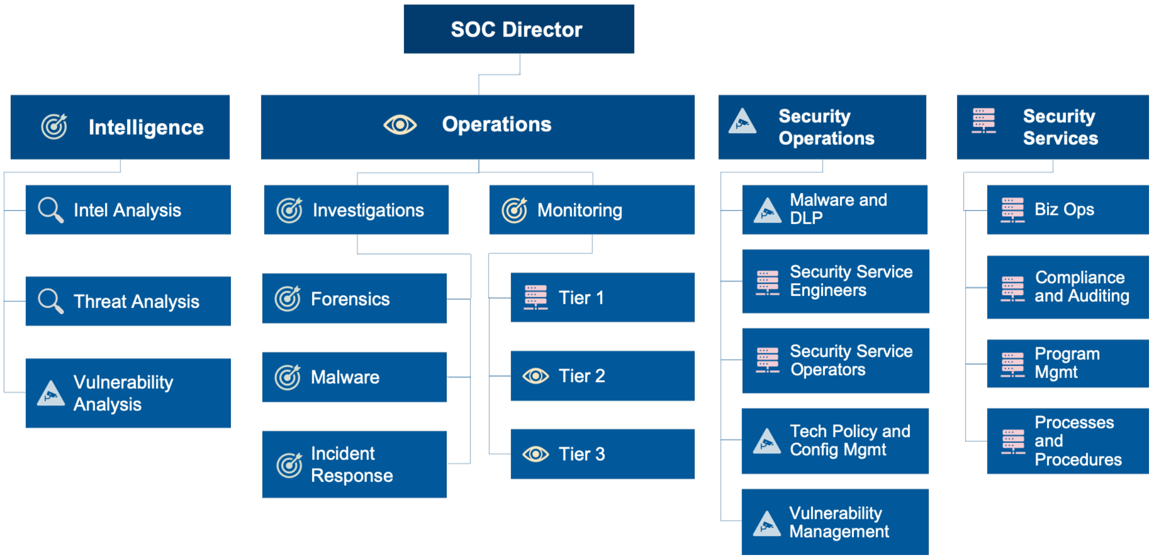


Figure 3. Typical Security Operations Center (SOC) Structure

For Academia:

As instructors, we want to relate the courses we teach to the real-world operations that students will be in once they enter the job market. We also want them to understand the international standards incorporated through the NIST CSF as represented in Figure 4.

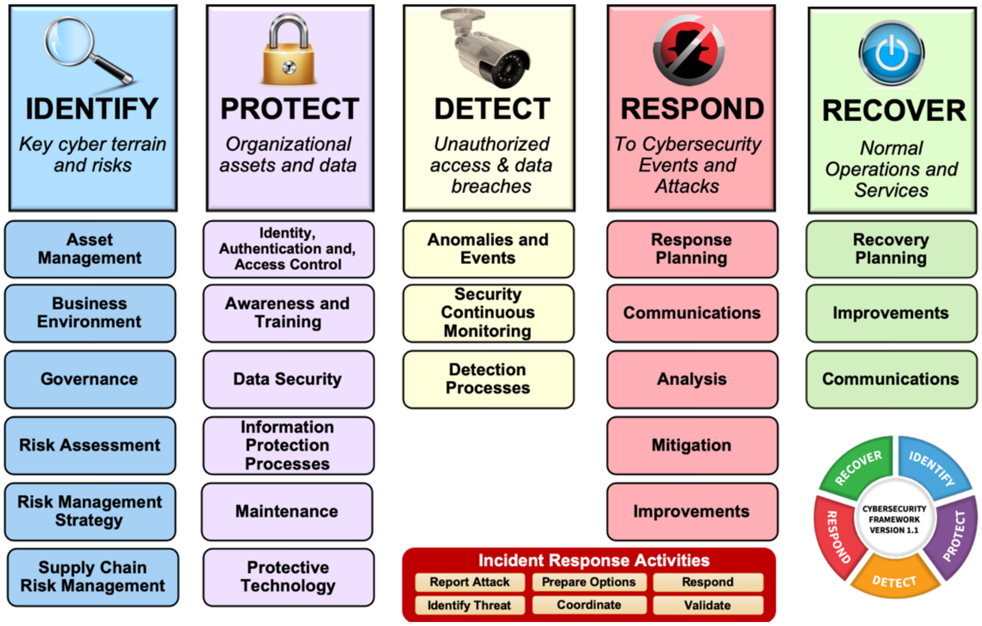


Figure 4: Summary of the NIST Cybersecurity Framework

To bring these two concepts together (i.e., real-world SOC operations with NIST CSF best practices), we propose four main cyber sub-disciplines as technical areas of concentration. Similar to the history of engineering, as it matured in the mid-1900's disciplines for civil engineering, mechanical engineering, aerospace engineering and computer engineering helped focus on the subset of skills needed for each sub-discipline.

The proposed four sub-disciplines for Cyber Defense: **Monitor-Harden-Pursue-Coordinate** (Lead/Intel) represent the entirety of tasks required to meet the best practices defined in the NIST CSF. Even a team of one person must *monitor* everything (e.g., networks, hosts, printers, cameras, routers) and *harden* everything and *pursue* the adversary everywhere. They must also bring in intelligence data from the community and *coordinate* with law enforcement in the event of an incident. This strategy applies to teams of 1 or teams of 50+ and it removes common gaps or seams that naturally form in a SOC. Figure 5 illustrates these four sub-disciplines of cyber as organized in a SOC.

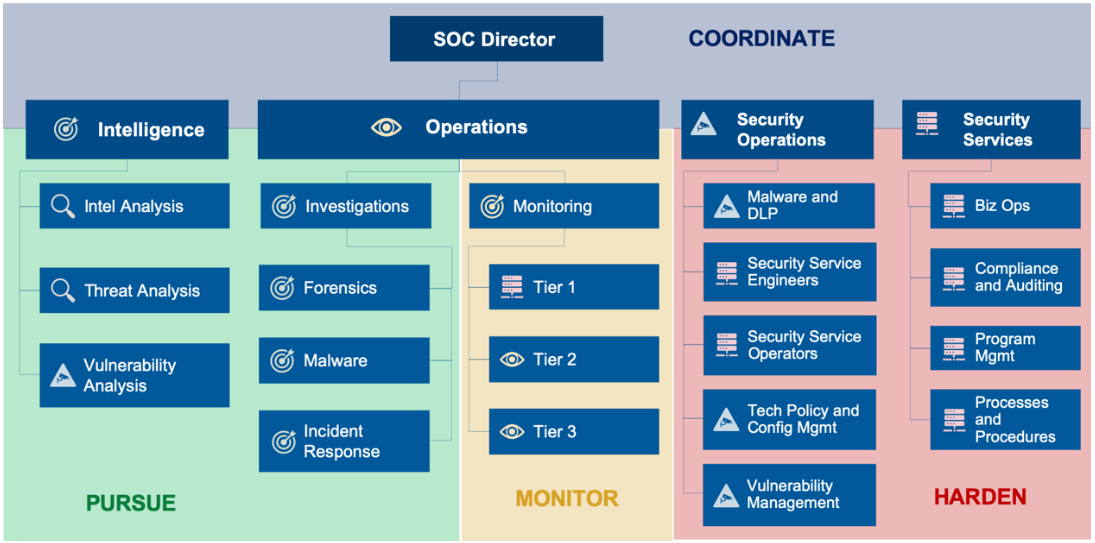
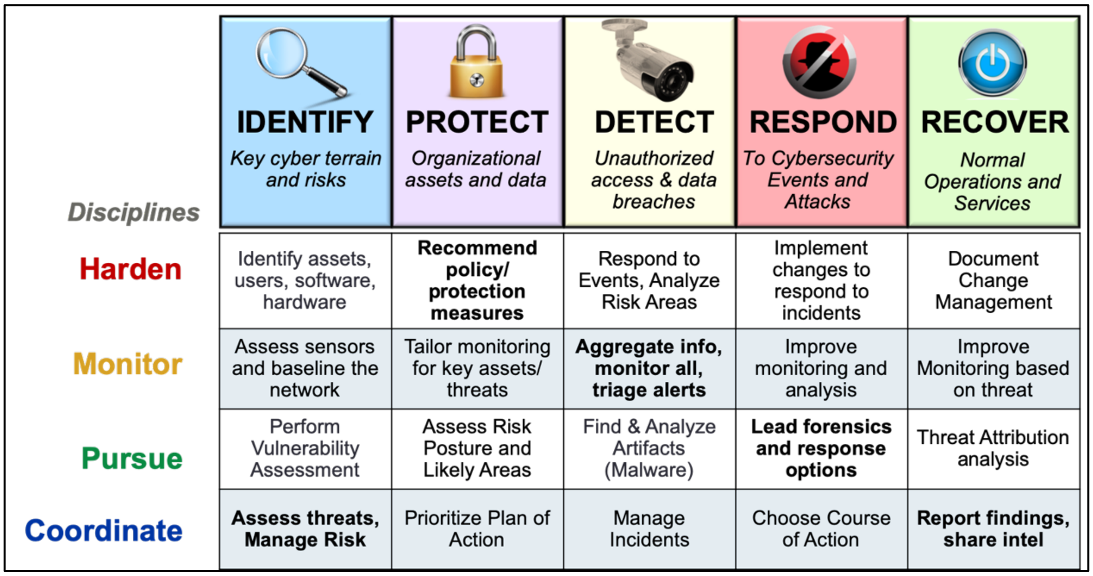


Figure 5: Cyber Disciplines (Monitor-Harden-Pursue-Coordinate) in a Typical SOC

These disciplines are easily found in the NIST CSF and, as shown in Figure 6, it is helpful to see what each discipline contributes overall. In any NIST Function (Identify – Protect – Detect – Respond – Recover), all the disciplines are present, although one is more dominant, as represented in the bold.

Courses are naturally aligned to the disciplines and it has been easy for students to see what they should focus on and how it leads to NICE work roles for future employment. Table 1 illustrates how specific courses in a discipline can align to NICE work roles.



Disciplines	**IDENTIFY** *Key cyber terrain and risks*	**PROTECT** *Organizational assets and data*	**DETECT** *Unauthorized access & data breaches*	**RESPOND** *To Cybersecurity Events and Attacks*	**RECOVER** *Normal Operations and Services*
Harden	Identify assets, users, software, hardware	**Recommend policy/ protection measures**	Respond to Events, Analyze Risk Areas	Implement changes to respond to incidents	Document Change Management
Monitor	Assess sensors and baseline the network	Tailor monitoring for key assets/ threats	**Aggregate info, monitor all, triage alerts**	Improve monitoring and analysis	Improve Monitoring based on threat
Pursue	Perform Vulnerability Assessment	Assess Risk Posture and Likely Areas	Find & Analyze Artifacts (Malware)	**Lead forensics and response options**	Threat Attribution analysis
Coordinate	**Assess threats, Manage Risk**	Prioritize Plan of Action	Manage Incidents	Choose Course of Action	**Report findings, share intel**

Figure 6: Cyber Disciplines (Monitor-Harden-Pursue-Coordinate) in NIST CSF

Courses should be aligned by sub-discipline and lead to a group of related work roles.

Table 1: Cybersecurity Disciplines with Example Courses and NICE Work Roles

Educational Cybersecurity Sub-Disciplines	Key Courses to address scope of NIST CSF	NICE Work Roles (Job Descriptions)
Harden	Core (Cybersecurity, Windows, Linux, Network Fundamentals, Offensive Tactics) PowerShell Scripting, Reconnaissance, Active Directory, Firewalls, Secure Mail and Web	CD Infrastructure Support Specialist, Security Control Assessor, Security Architect, Vulnerability Assessment Analyst
Monitor	Core (Cybersecurity, Windows, Linux, Network Fundamentals, Offensive Tactics), Python Scripting, Packet Analysis, Intrusion Detection, Network Security Monitoring	Cyber Defense Analyst, CD Incident Responder, Software Developer, Security Architect
Pursue	Core (Cybersecurity, Windows, Linux, Network Fundamentals, Offensive Tactics), PowerShell Scripting, Vulnerability Analysis, Reconnaissance, Hunt, Risk Assessment, Forensics	Vulnerability Assessment Analyst, CD Forensic Analyst, Secure Software Assessor, Mission Assessment Analyst, Target Network Analyst Counter Intel/LE Analyst
Coordinate (Lead/Intel)	Core (Cybersecurity, Windows, Linux, Network Fundamentals, Offensive), Key Terrain, Risk Management, Incident Response, Legal/Policy, Threat and Intel Analysis	CD Incident Responder, Counter Intel/LE Analyst, All Source Analyst, Threat Warning Analyst, Cyber Defense Analyst

For example, as shown in Figure 7, the cyber disciplines of Harden-Monitor-Pursue-Coordinate lead to different NICE workroles. A student in the harden sub-discipline, would be ready for jobs as a CD Infrastructure support specialist, a Security control assessor, and potentially well suited for a Security Architect (shown as orange as that work role should also have skills in monitor). Using this approach, students can have course tracks laid out that support careers using the NICE framework.

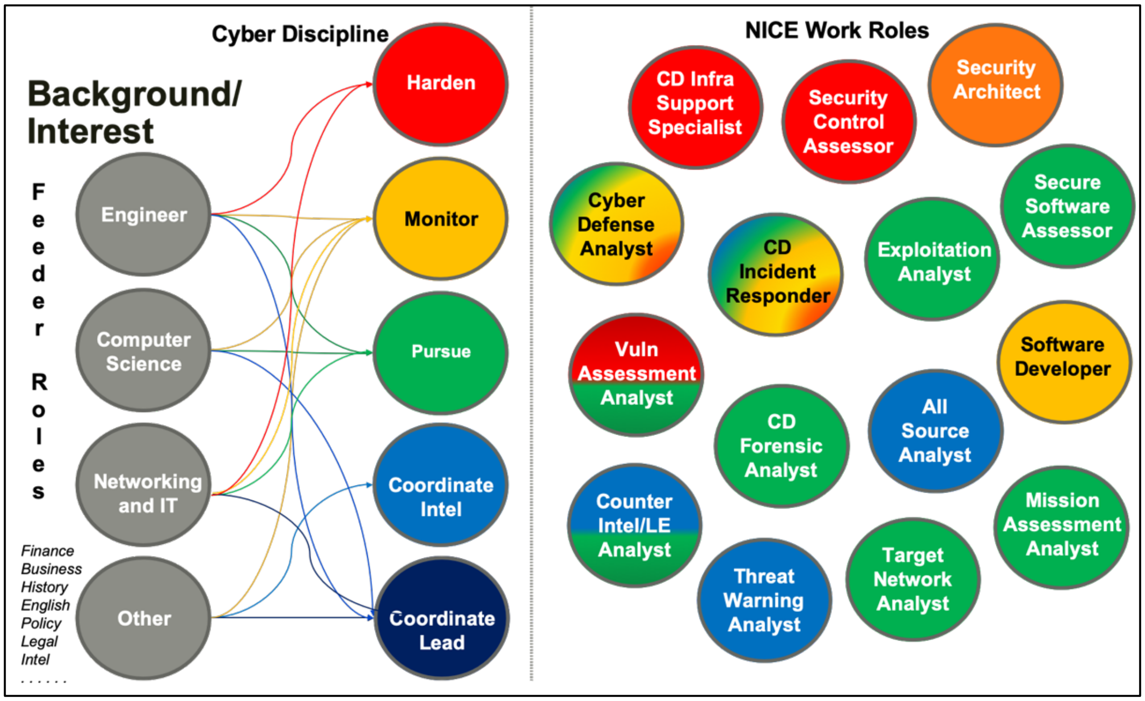


Figure 7: Cyber Disciplines can be aligned to groups of similar skill sets in NICE.

We believe that having cyber defense disciplines will be helpful to students and instructors and sets a longer career pathway in cyber.

5. **Describe the potential benefits or challenges experienced when aligning the NICE Framework more closely with other related standards, guidance, or resources (e.g., NIST Framework for Critical Infrastructure Cybersecurity, NIST Privacy Framework, other NIST Special Publications, etc.).**

The NIST CSF provides the best practices in performing cyber defense in an enterprise. This can be written in the form of tasks to perform or skills to achieve. The NIST CSF contains all the functions that must be addressed by one or more person (work role) and provides the full scope of the set of work roles needed (for example, in a SOC). A closer alignment of NICE to NIST would help explain what specific tasks in NIST are related to the KSA/Tasks of NICE. In Table 2, we show two Competency Areas (Asset Management and Business Continuity. We wrote new sklll statements (SKXXX) related to the NICE skills but written in terms related to the NIST CSF best practices. We believe that the detail and clarity in NIST CSF Skills to NICE will be beneficial to practitioners and students new to the field.

Table 2. Example of Close Alignment of NIST CSF Skills to NICE Framework

NICE Comp Area	**Related NSA Knowledge Units (KUs)**	**Skills Required for NIST CSF (Best Practices)**	**NICE Skills Per Competency Area**
Asset / Inventory Management	Network Defense, IT Systems Components, Forensic Accounting	SK001 - Identify Assets (devices, users, software, hardware) on network SK002 - Map communication and data flows SK003 - Gather device configurations SK004 - Catalog external information systems.	S0304 - Skill to access information on current assets available, usage.
Business Continuity	Cybersecurity Planning and Management, Network Security Administration	SK005 - Prioritize business functions SK006 - Identify critical services and mission dependencies SK007 - Evaluate continuity options (hot/warm/cold/alt sites) SK008 - Develop recovery plan (includes data backups)	S0032 - Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. S0150 - Skill in implementing and testing network infrastructure contingency and recovery plans. S0186 - Skill in applying crisis planning procedures. S0201 - Skill in creating plans in support of remote operations. (i.e., hot/warm/cold/alternative sites, disaster recovery).

6. **Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted.**

The NICE Competency Areas that go beyond cyber specifics are not that useful in this framework and seem unnecessary. That's not to say these skills aren't important in developing well-qualified cybersecurity professionals, but they are oftentimes already built into degree requirements via electives and other mandated coursework – this is especially true for adoption by certificate and other non-degree seeking programs. We recommend that NICE reference other sites that cover general science (e.g., mathematical analysis) and other Professional, Leadership or Operational areas (e.g., oral communication) if needed. By cutting the 60 Competency Areas in existence across the NICE Framework into the 30 that are required to understand the cyber domain, the mapping is becomes much more approachable and relevant.

Table 3 shows the proposed changes to the Competency Areas and the rationale for each proposed change. This table contains a total of 30 remaining competency areas

(27 for NICE and 3 additional ones for the DCWF that are DoD/Military specific) along with a small number of name changes to better reflect community terms.

Table 3. Recommended NICE Competency Areas with changes in red.

Existing NICE Competency Area	Recommended NICE Competency Area	Rationale for Proposed Change
Asset / Inventory Management	Asset Management	Asset Management includes inventory process
Business Continuity	Business Continuity	
~~**Client Relationship Management**~~		Non-cyber area (handle in other frameworks)
Collection Operations		Offensive Mission (Military - put in DCWF only)
Computer Forensics	Digital Forensics	Digital is broader than computer and a more common term
Computer Languages	Computer Languages	
Computer Network Defense	Network Security Monitoring	The tasks are really Network Security Monitoring, a subset of overall Computer Network Defense
Computers and Electronics	Computers and Electronics	
~~**Conflict Management**~~		Non-cyber area (handle in other frameworks)
~~**Contracting/Procurement**~~		Non-cyber area (handle in other frameworks)
~~**Critical Thinking**~~		Non-cyber area (handle in other frameworks)
~~**Data Analysis**~~		General computer science skill not specific to cyber
Data Management	Data Management	Combine cyber data issues into one
~~**Data Privacy and Protection**~~		Covered in Data Management
~~**Database Administration**~~		General Computer science skill not specific to cyber
~~**Database Management Systems**~~		General Computerscience skill not specific to cyber
Encryption	Cryptography	More generalized topic with encryption being one part
Enterprise Architecture	Enterprise Architecture	
~~**External Awareness**~~		Non-cyber area (handle in other frameworks)
Identity Management	Identity Management	
Incident Management	Incident Response	More common term in the community
Information Assurance	Information Assurance	

~~**Information Management**~~		General Computerscience skill not specific to cyber
Information Systems/Network Security	Information Security Architecture	More common term in the community. Network is a part of it.
~~**Information Technology Assessment**~~		General IT skill not specific to cyber
Infrastructure Design	Network Design	More descriptive of what the tasks are
Intelligence Analysis	Intelligence Analysis	
~~**Interpersonal Skills**~~		Non-cyber area (handle in other frameworks)
~~**Knowledge Management**~~		General IT skill not specific to cyber
Legal, Government, and Jurisprudence	Cybersecurity Law	More descriptive of what the tasks are - relates to cyber
~~**Mathematical Reasoning**~~		General science skill not specific to cyber
~~**Modeling and Simulation**~~		General science skill not specific to cyber
Network Management	Network Management	
Operating Systems	Operating Systems	
Operational Support		Offensive Mission term (used in Military only - put in DCWF only)
~~**Oral Communication**~~		Non-cyber area (handle in other frameworks)
~~**Organizational Awareness**~~		Non-cyber area (handle in other frameworks)
~~**Policy Management**~~		General IT skill with CYBER policy handled with cybersecurity legal area
~~**Presenting Effectively**~~		Non-cyber area (handle in other frameworks)
~~**Problem Solving**~~		Non-cyber area (handle in other frameworks)
~~**Process Control**~~		General science skill not specific to cyber
~~**Project Management**~~		Non-cyber area (handle in other frameworks)
~~**Requirements Analysis**~~		General science skill not specific to cyber
Risk Management	Risk Management	Can be general but unique and critical to cyber
~~**Software Development**~~		General computer science skill not specific to cyber (Secure coding handled in other areas)
Software Testing and Evaluation	Software Testing and Evaluation	Can be general but unique and critical to cyber
~~**Strategic Planning**~~		Non-cyber area (handle in other frameworks)
System Administration	System Administration	Can be general but unique aspects and critical to cyber

Systems Integration	Systems Integration	Can be general but unique aspects and critical to cyber
Systems Testing and Evaluation	Systems Testing and Evaluation	Can be general but unique aspects and critical to cyber
Target Development		Offensive Mission (Military - put in DCWF only)
~~Teaching Others~~		Non-cyber area (handle in other frameworks)
~~Technology Awareness~~		General IT skill not specific to cyber
~~Telecommunications~~		General IT skill not specific to cyber
Threat Analysis	Offensive Tactics and Tools	More common term in the community
~~TPO (Third Party Oversight)~~		Non-cyber area (handle in other frameworks)
Vulnerabilities Assessment	Vulnerability Assessment	Minor word change to reflect common community terms
Web Technology	Web Technology	Can be general but unique aspects and critical to cyber
~~Workforce Management~~		Non-cyber area (handle in other frameworks)
~~Written Communication~~		Non-cyber area (handle in other frameworks)
New	Hunting Adversaries	Critical in cyber and should not be buried. Hunt is a key competency area.

7. **Describe any improvements that might be made in the current organization of the NICE Framework and its major components such as Categories, Specialty Areas, Work Roles, Knowledge, Skills, Abilities, and Tasks.**

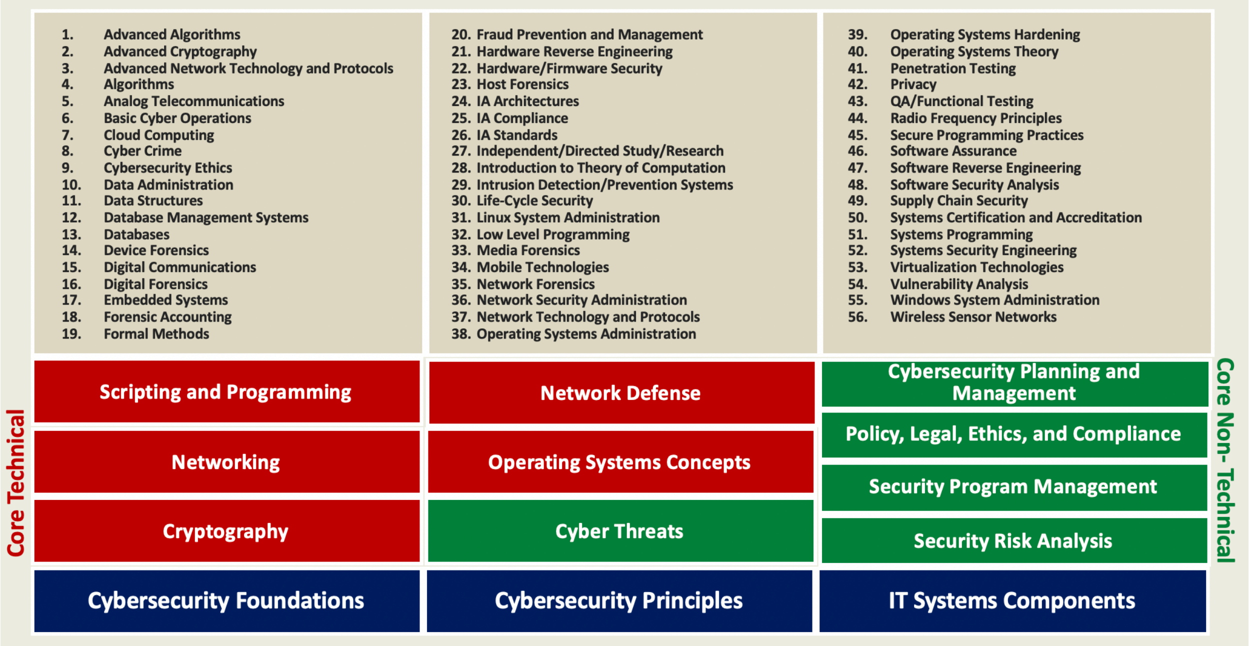
   As discussed above, streamlining the NICE Framework to those competency areas that are cyber specific will help the community focus on the KSAs/Tasks need to perform in this domain. The resulting reduction of Competency Areas from 60 to the proposed 30 makes the overall problem of mapping and understanding NICE more tractable.

   The Specialty Areas should be reconsidered with the reduced subset of Competency Areas and the proposed cyber sub-disciplines (Harden – Monitor – Pursue – Coordinate) in order to group work roles (and jobs) by similar skills. Overall skills and tasks from NICE should be written to more closely align with the NIST CSF best practices as illustrated in Table 2.

8. **Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas.**

9. **Explain whether the NICE Framework indicates which Knowledge, Skills, and Abilities could be considered as foundational for all workforces that regularly interact with networks, systems, and data in cyberspace.**

The NICE Framework does not yet provide insight into foundational KSAs. However, the NSA Knowledge Units do provide information that can assist in that area. The NSA CAE-CDE for 2020 identifies 69 KUs, shown in Figure 8, and breaks them into foundational, technical and non-technical core units and optional KUs (requiring a subset of optional KUs in the curriculum for an academic institution to be accredited).



1. Advanced Algorithms
2. Advanced Cryptography
3. Advanced Network Technology and Protocols
4. Algorithms
5. Analog Telecommunications
6. Basic Cyber Operations
7. Cloud Computing
8. Cyber Crime
9. Cybersecurity Ethics
10. Data Administration
11. Data Structures
12. Database Management Systems
13. Databases
14. Device Forensics
15. Digital Communications
16. Digital Forensics
17. Embedded Systems
18. Forensic Accounting
19. Formal Methods
20. Fraud Prevention and Management
21. Hardware Reverse Engineering
22. Hardware/Firmware Security
23. Host Forensics
24. IA Architectures
25. IA Compliance
26. IA Standards
27. Independent/Directed Study/Research
28. Introduction to Theory of Computation
29. Intrusion Detection/Prevention Systems
30. Life-Cycle Security
31. Linux System Administration
32. Low Level Programming
33. Media Forensics
34. Mobile Technologies
35. Network Forensics
36. Network Security Administration
37. Network Technology and Protocols
38. Operating Systems Administration
39. Operating Systems Hardening
40. Operating Systems Theory
41. Penetration Testing
42. Privacy
43. QA/Functional Testing
44. Radio Frequency Principles
45. Secure Programming Practices
46. Software Assurance
47. Software Reverse Engineering
48. Software Security Analysis
49. Supply Chain Security
50. Systems Certification and Accreditation
51. Systems Programming
52. Systems Security Engineering
53. Virtualization Technologies
54. Vulnerability Analysis
55. Windows System Administration
56. Wireless Sensor Networks

Core Technical

Scripting and Programming

Network Defense

Cybersecurity Planning and Management

Policy, Legal, Ethics, and Compliance

Networking

Operating Systems Concepts

Security Program Management

Cryptography

Cyber Threats

Security Risk Analysis

Core Non- Technical

Cybersecurity Foundations

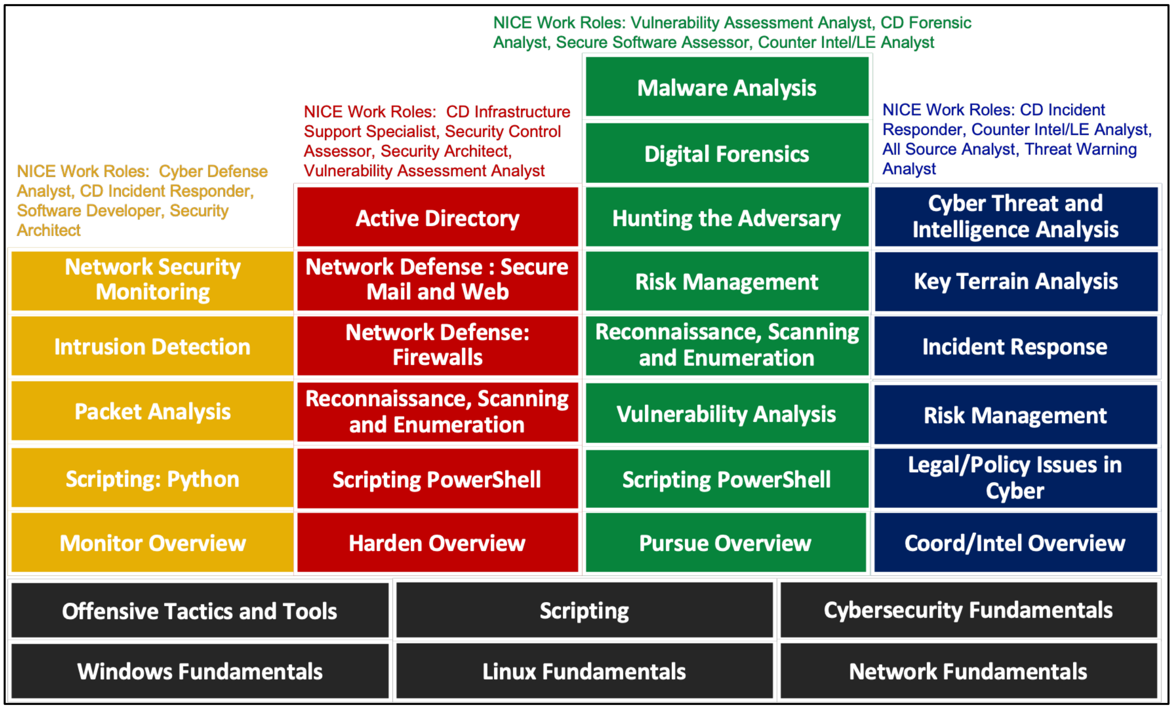
Cybersecurity Principles

IT Systems Components

Figure 8: NSA Knowledge Units for CAE-CDE Accreditation in 2020

Each of these KUs contains learning outcomes and hands-on lab requirements that can be used to create courses in cybersecurity. All professionals in cybersecurity must understand cybersecurity foundations and principles along with basic IT system components. The core KUs (both technical and non-technical) can be allocated to courses of various disciplines that can be mapped to the NICE work roles.

To take this a step further, we have created six core *courses* in academia that cover the three core NSA KUs. We then mapped the core and optional NSA KUs to the NIST CSF to develop the cyber sub-disciplines or “academic tracks” leading to NICE work roles. In Figure 9, we provide an example of that approach of courses aligned to NIST CSF, mapped to the NSA KUs that lead to NICE Work Roles. We believe that this type of layout could be very helpful to academic institutions wanting to provide cybersecurity and students who want to pursue this field.



NICE Work Roles: Cyber Defense Analyst, CD Incident Responder, Software Developer, Security Architect	NICE Work Roles: CD Infrastructure Support Specialist, Security Control Assessor, Security Architect, Vulnerability Assessment Analyst	NICE Work Roles: Vulnerability Assessment Analyst, CD Forensic Analyst, Secure Software Assessor, Counter Intel/LE Analyst	NICE Work Roles: CD Incident Responder, Counter Intel/LE Analyst, All Source Analyst, Threat Warning Analyst
		Malware Analysis	
		Digital Forensics	
	Active Directory	Hunting the Adversary	Cyber Threat and Intelligence Analysis
Network Security Monitoring	Network Defense : Secure Mail and Web	Risk Management	Key Terrain Analysis
Intrusion Detection	Network Defense: Firewalls	Reconnaissance, Scanning and Enumeration	Incident Response
Packet Analysis	Reconnaissance, Scanning and Enumeration	Vulnerability Analysis	Risk Management
Scripting: Python	Scripting PowerShell	Scripting PowerShell	Legal/Policy Issues in Cyber
Monitor Overview	Harden Overview	Pursue Overview	Coord/Intel Overview

Offensive Tactics and Tools	Scripting	Cybersecurity Fundamentals
Windows Fundamentals	Linux Fundamentals	Network Fundamentals

Figure 9: Example foundational and core courses leading to NICE work roles.

10. **For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference.**

    Not addressed.

11. **Describe which components of the NICE Framework you think are best left as static content and would not change until the next revision and which components could be managed as dynamic content (i.e., more frequent changes or updates to accommodate new information as it becomes available).**

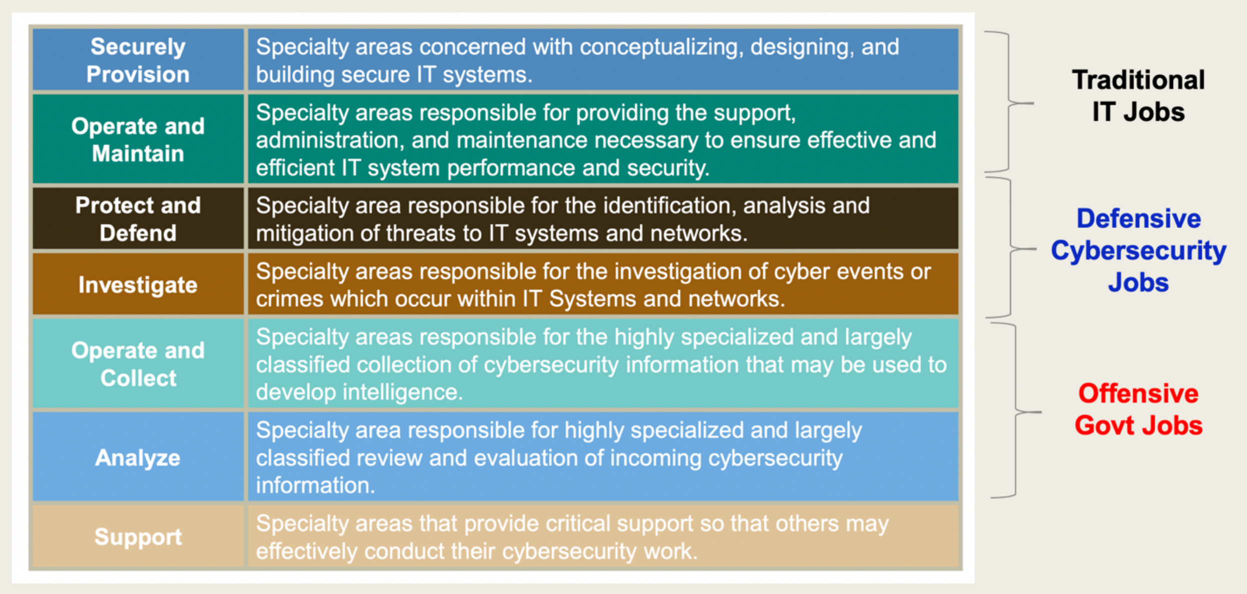
    Competency Areas or topics generally are static, but the KSA/T can improve and evolve over time.

12. **Describe the value or risk in different organizations, sectors of the economy, or organizations with classified versus unclassified workforces to develop customized versions of the NICE Framework tailored to their specific circumstances.**

    We believe that all cyber defense work roles can be unclassified and standardized across Military, commercial organizations and academic institutions. These should be standardized per the requirements of best practices from the NIST CSF.

Work roles doing general offensive tactics are found in the Pursue discipline, most notably for penetration testing and hunt. These are also unclassified and should be part of the standard, as these tasks are also part of the NIST CSF.

There are three competency areas that are predominantly classified and should be customized by the specific organization. As shown in Figure 10, it appears that the NICE Framework was an amalgamation of traditional IT, defensive cybersecurity and offensive (Military/Government) jobs. We believe that creating ONE national standard in NICE that identifies all work roles necessary to meet the **best practices of the NIST CSF** would be help reduce some of the confusion in this field and lead to more students able to study the right topics to meet the job requirements. The tasks related to the three offensive Competency Areas (Collection Operations, Operations Support and Target Development) should be removed from the NICE Framework an allocated to a separate DoD version (DCWF) and customized for their specific circumstances.



Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Operate and Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Support	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

Figure 10: Offensive Areas relate to collection operations and target development