

CyberWatch K12 Cybersecurity
Educator Academy: CTE Track



Expanding Knowledge in
Cyberawareness and Careers in
Cybersecurity

MAKE A DIFFERENCE



9:00 - 9:45 AM	Sign-in Welcome and Meet and Greet Drink orders Understanding the MSDE Cybersecurity CTE Option CyberSTEM Option More about the K12 Cybersecurity Educator Academy
9:45 - 10:00 AM	Brief Stretch Break
10:00-11:30 AM	Option 1: Setting up your Own Lab Q & A
11:30-12:00 PM	LUNCH: will be provided- cohort networking
12:00-12:30 PM	Virtual Tour and Q and A regarding online course access
12:30- 1:45 PM	Getting students ready for Cyber Dense Competitions- or just fun exercises to use in your classroom-guest speaker
1:45- 2:00 PM	Evaluation, next steps, where to find additional resources



National CyberWatch Center



About NCW

Mission:

To advance cybersecurity education by leading collaborative efforts to strengthen the national cybersecurity workforce

About NCW

- National Science Foundation funded Advanced Technology Education Center
 - Cybersecurity education at all levels
 - elementary through graduate school
 - curriculum development
 - faculty professional development
 - student development
 - career pathways, and public awareness

About NCW

- Model IA curricula, including complete courses for A.A.S. and A.S. degrees and for two IA certificates;
- Assist member institutions in mapping their Cybersecurity courses
- Lead Centers of Academic Excellence in Information Security Education for Community Colleges (CAE2Y) with NSF, NSA, and DHS

NCW K12 Division

- **Leverage** the **network and collaboration** capacity of the National CyberWatch Center to advance K12 Cybersecurity educational efforts
- **Promote access** to shared high quality resources across government, industry, academia, and non-profits to enhance K12 cybersecurity education
- **Foster collaboration** between cybersecurity discipline STEM programs by sharing exemplary programs, models, curricula, research and evaluation
- **Provide research based solutions** that will allow all stakeholders including policymakers to advocate for a holistic approach to K12 Cybersecurity education

NCW K-12 Programs



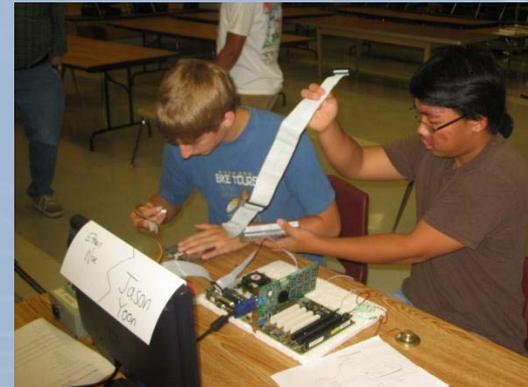
Areas of Focus

- The Cybersecurity workforce pipeline
- Community awareness of the Cybersecurity workforce
- Community awareness of C3- Cyberethics, Safety and Security, and
- Security of K-12 IT systems



K-12 Pipeline

- Annual Cyberethics, Cybersafety and Cybersecurity (C3) Conference
- Cool Careers in Cybersecurity for Girls Workshop
- Careers in Cybersecurity for Guidance Counselors Workshop
- After School/Enrichment
 - Cyber Clubs
 - MINDTOOLS
 - CyberSTEM
- Summer Cyber Academies
- CW K12 CyberSTEM Content
- Competitions
- SECURE IT: *Strategies to Encourage Careers in Cybersecurity and IT*
- CTE Cybersecurity Track
- Mid-Atlantic CCDC High School Activities



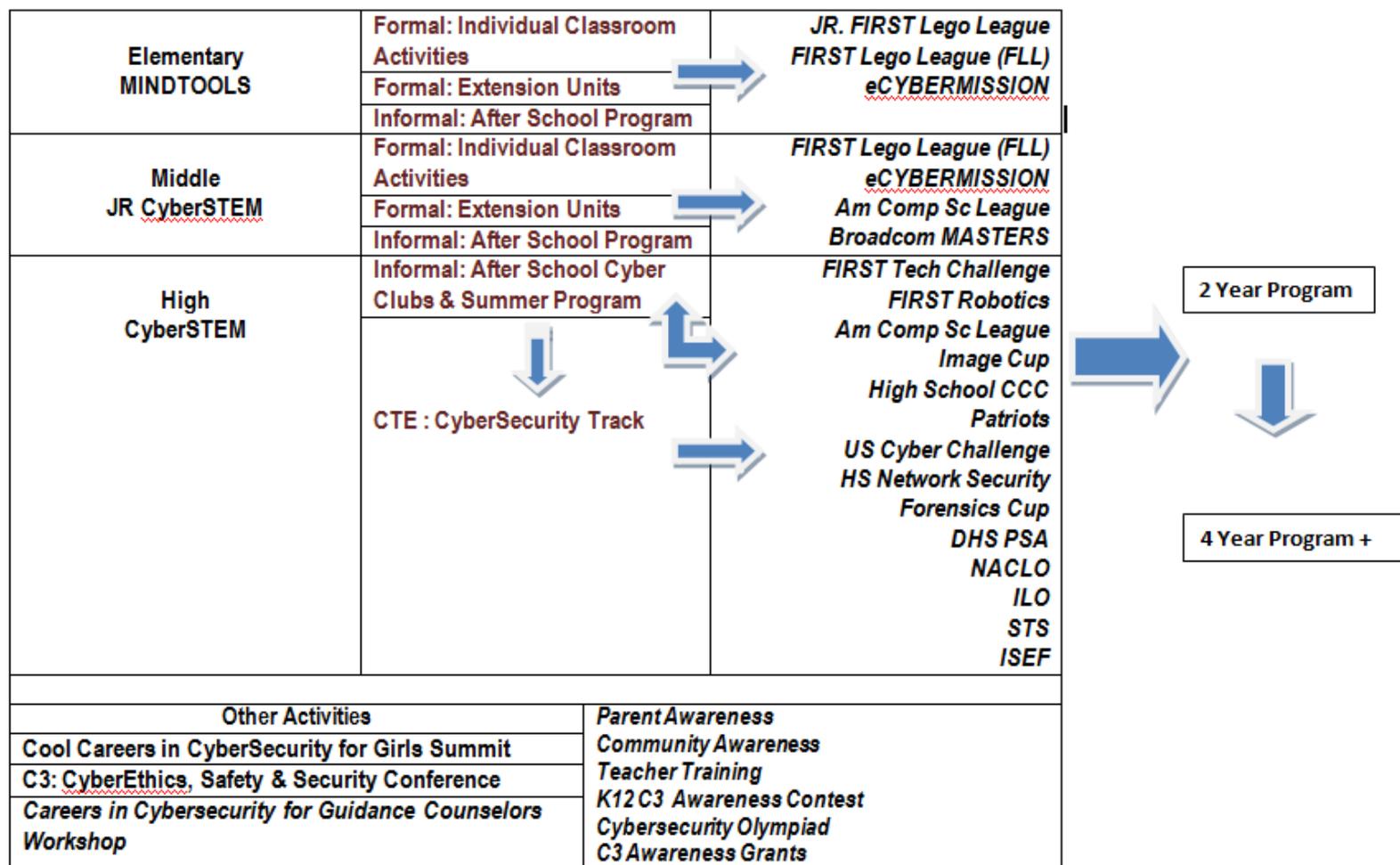
New Efforts in 2013

- **MD Cyber Defense Boot Camp**
- **K12 Cybersecurity Educator Academy: CTE**
- **K12 Cybersecurity Educator Academy: CyberSTEM**

- **C3 Schools Initiative (Cyber Schools)**
- **Cybersecurity Collaborative Project**
 - **Programs**
 - **Lessons/Content**
- **Moodle**

SECURE IT OVERVIEW

Strategies to Encourage Careers in CyberSecurity and Informational Technology



Summer Programs in Cybersecurity!

Cyber Defense Boot Camp: July 7-13, 2013

**For students entering
11th or 12th grade in
Fall 2013**

**University of Maryland
College Park, MD**

**Technical experience
is recommended,
including networking,
Cisco Academy, and/
or Java programming**

Cyber Defense Boot Camp is an intermediate level seven day summer program for high school men and women (rising juniors and seniors). Students will live on campus for one week and expand their knowledge of Cyber Defense and Cybersecurity. Students will learn about these fields, visit local sites and hear from a variety of speakers to learn more about the skills needed for this exciting profession! Topics include Operating System, System Administration, Networking, Programming, as well as a Computer-Based "Capture-the-flag" competition!

CyberSTEM Camp: July 22-26, 2013

**For female students
entering 7th or 8th grade
in Fall 2013**

**University of Maryland
College Park, MD**

**Monday-Friday
9:00am-3:30pm**

CyberSTEM camp is a one-week commuter summer program for middle school (incoming 7th and 8th grade) girls who are interested in the growing field of Cybersecurity. This five day experience provides hands-on activities focused on STEM and Cybersecurity topics. Students will learn and apply basic concepts of programming, forensics, cryptography, and program management from a series of gaming, modeling, and simulation activities, which explore the interconnections of science, math, technology, and computers.

For more information, contact:

Cristin Caparotta

Graduate Assistant

Maryland Cybersecurity Center

ccapa@umiacs.umd.edu

(301)-405-6735



VISIT [HTTP://CYBER.UMD.EDU/EDUCATION](http://cyber.umd.edu/education) FOR INFORMATION & UPDATES!

<http://www.edtechpolicy.org/cyberk12/>

2013 Summer Programs



<p>Session 1 – Howard County ARL</p> <p>CyberSTEM I</p> <p>Grades 9-12</p> <p>Monday, June 24 – Friday, July 5, 2013 9:00am - 2:00pm (Monday-Friday)</p> <p>Class does not meet on July 4th</p> <ul style="list-style-type: none"> The program is open to current HCPSS students grades 9-12 and is limited to the first 25 students registered. Students must provide their own transportation and lunch. All HCPSS policies will be strictly enforced <p>More Information</p> <p>Registration coming soon</p>	<p>Session 2 – University of Maryland Maryland Cybersecurity Center</p> <p>CyberSTEM I</p> <p>Rising 7th and 8th grades girls</p> <p>Monday, July 22 – Friday, July 26, 2013 9:00am - 3:30pm (Monday-Friday)</p> <p>Contact Info http://www.cyber.umd.edu/education/cyber-stem</p> <p>All UMD policies will be strictly enforced</p> <p>Apply Here</p>
<p>Session 3 – Northern Virginia Middle School Girls Northern Virginia Community College Alexandria Campus</p> <p>Room 477 in the Bisdorf Building NVCC Women in Information Technology Group Science and Technology (SAT) Division</p> <p>CyberSTEM I</p> <p>Monday, August 12-August 16, 2013 9:00am - 2:00 pm Cost: \$200</p> <p>Registration Deadline: June 1, 2013</p> <ul style="list-style-type: none"> The program is open to all middle school aged girls and is limited to the first 18 students registered. Students must provide their own transportation and lunch. All NVCC policies will be strictly enforced. <p>More Information</p>	<p>Session 4 – University of Maryland Maryland Cybersecurity Center</p> <p>Cyber Defense Training Camp Residential Rising Juniors and Seniors</p> <p>Sunday, July 7 – Saturday, July 13, 2013 Application Deadline: May 15, 2013</p> <p>Eligibility: Technical experience is recommended, including networking, Cisco Academy, and/or Java programming.</p> <p>Contact Info http://www.cyber.umd.edu/education/cyber-stem</p> <p>All UMD policies will be strictly enforced</p> <p>Apply Here</p>
<p>Session 5 – Harford County Joppatowne High School</p> <p>CyberSTEM I</p> <p>Coming Soon</p>	<p>Session 6 – Prince George's Co Public Schools</p> <p>CyberSTEM I</p> <p>Coming Soon</p>
<p>Session 7 – Anne Arundel County</p> <p>CyberSTEM I</p> <p>Coming Soon</p>	<p>Session 8 – Baltimore County</p> <p>CyberSTEM I</p> <p>Coming Soon</p>
<p>Session 9 – St Mary's County</p> <p>CyberSTEM I</p> <p>Coming Soon</p>	<p>Session 10 – Howard County Elementary</p> <ul style="list-style-type: none"> Invitation Only Transportation and lunch will be provided. All HCPSS policies will be strictly enforced

**NATIONAL CYBERWATCH
MID-ATLANTIC
CCDC 2013**
APRIL 10-13

REGISTRATION OPEN THROUGH MARCH 1
REGIONAL QUALIFIERS MARCH 18-23
REGIONAL FINALS APRIL 10-13

ARE YOU GAME?

VOTE

Recent News

[2013 Mid-Atlantic CCDC Registration](#)

[2013 Mid-Atlantic CCDC: Save the Dates](#)

[2012 Mid-Atlantic CCDC Video](#)

STUDENTS

REGISTER

YOUR TEAM

SPONSORS

PARTICIPATE

& RECRUIT

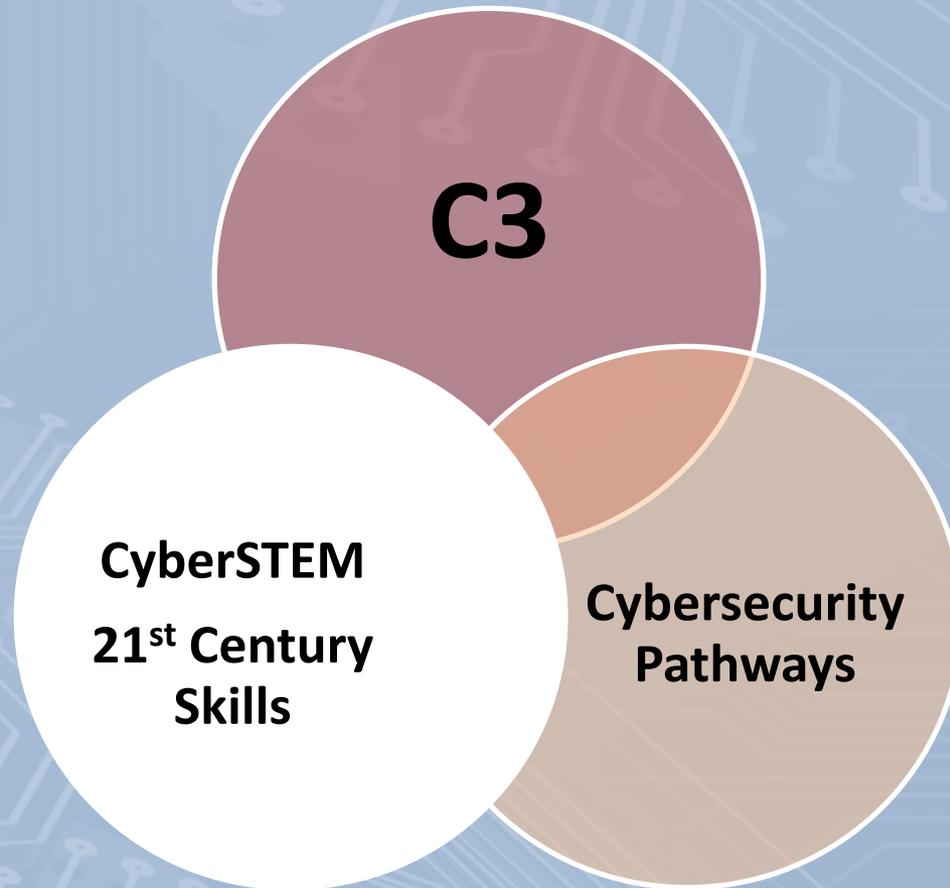
MACCDC

2012 EVENT

Organizers, Partners, and Sponsors



Design



Students

- After-school programs
- In-School Modules
- Cool Careers for Girls Summit
- Summer Cyber Academies
- CTE Track – Cybersecurity

Educators

- Training for Teachers
- Annual C3 Conference
- Guidance Counselor Workshop
- Curriculum

Two and Four Year

- Articulation Agreements
- Collaborative Curriculum Development and Refresh

MSDE Approved CTE

CCNA Discovery I

CCNA Discovery II

CW 160/Security+

CW 130 OS

CCENT Cert

SEC+ Cert

+ Ethics

NICE NIST

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



Home

About

Awareness

Education

Workforce Structure

Training & Professional Development

National Cybersecurity Workforce Framework

Executive Summary

The National Initiative for Cybersecurity Education (NICE) has published the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work. Defining the cybersecurity population consistently, using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce.

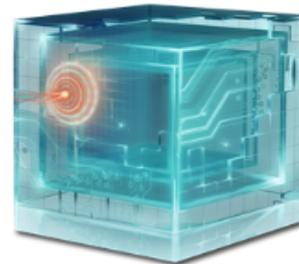
Framework Overview

In designing the Framework, "Categories" and "Specialty Areas" were used as an organizing construct to group similar types of work. The categories, serving as an overarching structure for the Framework, group related specialty areas together. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories.

The intention of the Framework is to describe cybersecurity work regardless of organizational structures, job titles, or other potentially idiosyncratic conventions. For example, under this structure an individual may perform tasks in more than one specialty area, or all of an individual's work may fall within a single specialty area. Similarly, large agencies may have many individuals devoted to a single specialty area while smaller agencies may need individuals to cross multiple specialty areas. Within any given organization, the way these groupings are organized into positions, career fields, or work roles depends on a number of factors including organizational characteristics (e.g., geographic location), constraints (e.g., limited personnel), and mission. Thus, due to the variety of jobs, occupations, cultures, structures within any given agency or organization, there may not always be a "one-to-one" crosswalk of jobs or career fields to individual specialty areas.

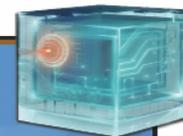
Documents

- **NEW Framework - Interactive How-To and Implementation Guide**
- **Framework - Interactive**
- **Framework - Printable**
- **Framework Development**
- **The Use and Usefulness of the Cybersecurity Data Element**
 - **Cybersecurity Data Element - OPM Guide to Data Standards (see Page A-106)**



7 Categories

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

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

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

DEFINING CYBERSECURITY

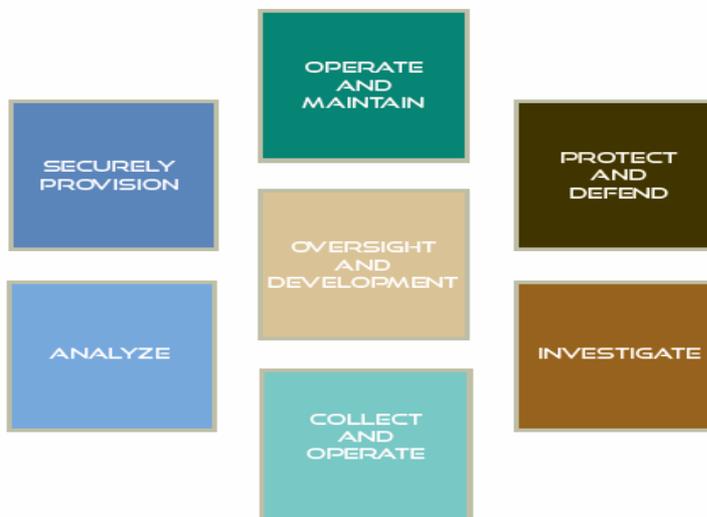
Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration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

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

THE CALL TO ACTION

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

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



Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development
------	---------------------	-------------------	--------------------	----------------------	--------------------	-------------	---------------------	---------	---------------------------

7 Categories

What are the 7 Categories?

The Framework establishes a common taxonomy and lexicon for cybersecurity workers. The 7 categories, serving as an overarching structure for the Framework, group related specialty areas together.

The categories of cybersecurity work, and their definitions, are in the table below.

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 areas responsible for identifying, analyzing, and mitigating threats to IT systems.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Collect and Operate	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.
Oversight and Development	Specialty areas that provide critical support so others may conduct their cybersecurity work.

31 Specialty Areas

What are the 31 Specialty Areas?

Each specialty area represents an area of concentrated work, or function, within cybersecurity. The Framework provides the typical tasks and knowledge, skills and abilities (KSAs) within each specialty area.

Securely Provision

- Systems Requirements Planning
- Systems Development
- Software Assurance and Security Engineering
- Systems Security Architecture
- Test and Evaluation
- Technology Research and Development
- Information Assurance (IA) Compliance

Operate and Maintain

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management

Collect and Operate

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Protect and Defend

- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Analysis
- Computer Network Defense (CND) Infrastructure Support

Investigate

- Investigation
- Digital Forensics

Analyze

- Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Oversight and Development

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development
- Information Systems Security Operations (ISSO)
- Security Program Management (Chief Information Security Officer [CISO])

OPERATE AND MAINTAIN

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

Data Administration

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

Knowledge Management

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

Customer Service and Technical Support

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

Network Services

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

System Administration

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

Systems Security Analysis

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

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

PROTECT AND DEFEND

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

Computer Network Defense (CND) Analysis

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

Incident Response

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Computer Network Defense (CND) Infrastructure Support

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

Vulnerability Assessment and Management

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

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

INVESTIGATE

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

Digital Forensics

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

Investigation

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Digital Forensics		Investigation							
Home	Using This Document	Sample Job Titles	Securely Provision	Operate and Maintain	Protect and Defend	Investigate	Collect and Operate	Analyze	Oversight and Development

```
graph TD; Training[Training] <--> Articulation[Articulation]; Training <--> Approval[Approval]; Articulation <--> Approval;
```

Training

Articulation

Approval

Other Dates

- **Security+ training**
- **Boot camp for certification**
- **CCDC April 13 ARL workshop**
- **TBD**