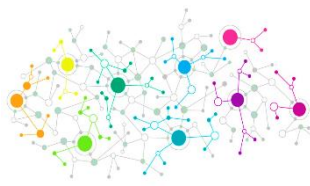




# **Interagency Federal Cyber Career Pathways Initiative**

*Megan Caposell - Chris Paris - Matt Isnor  
NICE 2019 Conference & Expo*

# Working Group Tri-Chairs



**Megan  
Caposell**

***Sr. Cybersecurity Strategic  
Workforce Planner,  
DHS Cybersecurity and  
Infrastructure Security Agency  
(CISA)***



**Chris  
Paris**

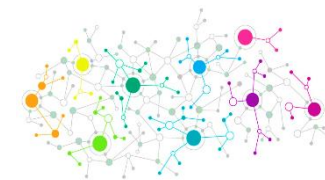
***Senior Advisor,  
Cybersecurity Workforce  
Management  
Department of Veterans Affairs  
(VA)***



**Matthew  
Isnor**

***Program Lead,  
Cyber Workforce  
Department of Defense (DoD)***

# The Cyber Workforce Challenge



## Globally



- According (ISC)<sup>2</sup>, the **global cyber workforce shortage** is projected to reach **1.8 million by 2022**
- That's more than **1 new cyber expert needed every minute\***

## Domestically



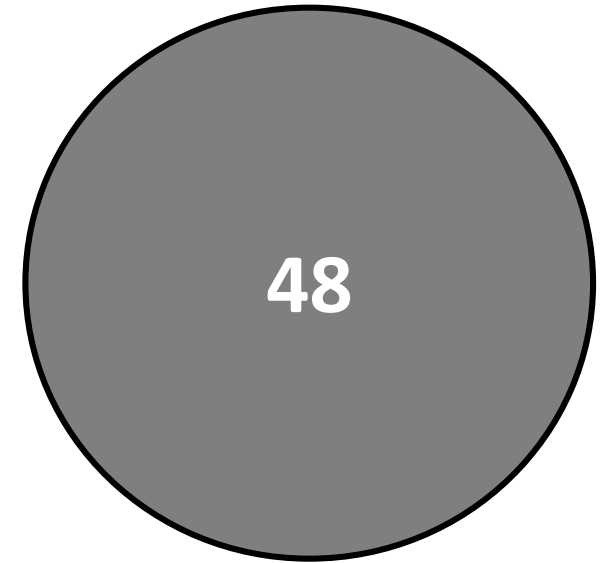
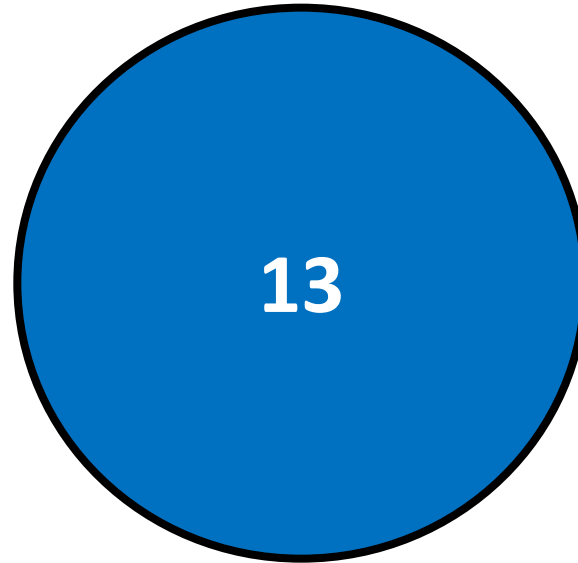
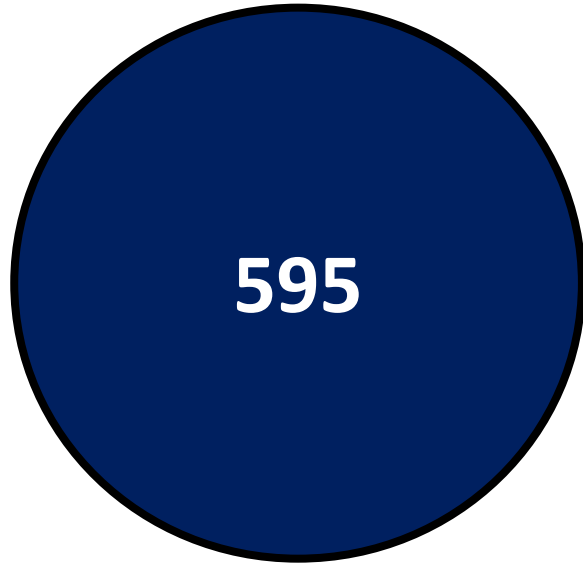
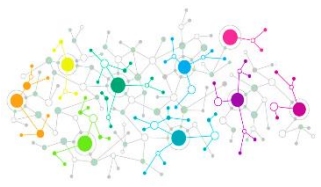
There are over **313,000 vacant cyber jobs** in the United States

## Locally



- There are over **60,000** vacant jobs in **DC, MD, and VA**
- The need for **cyber jobs in our geographic area** makes up **20%** of the **need of the nation**

# These 3 Numbers Tell a Story...

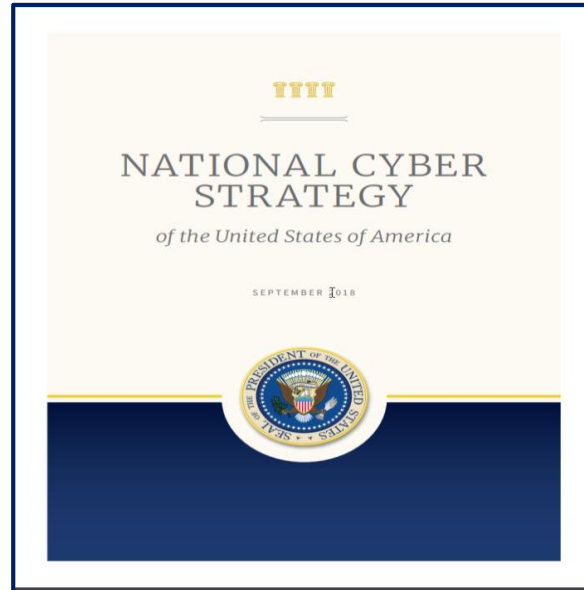


# Key Cyber Workforce Drivers

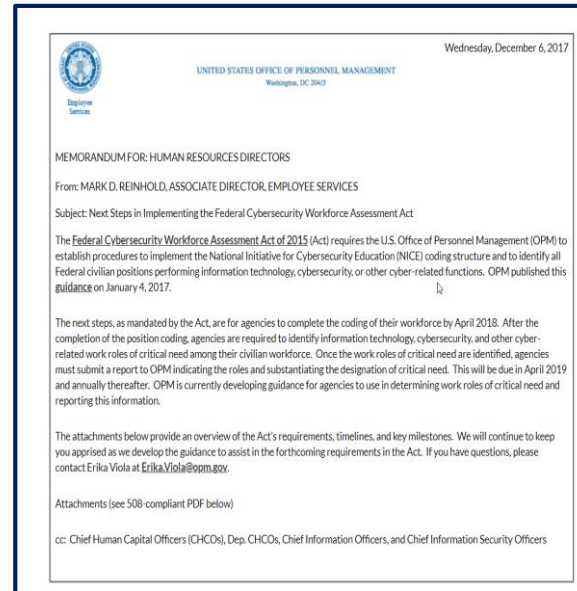


Developing and managing a strong cyber workforce is a growing issue within the private and public sector. Because of this, there are many drivers that are propelling cyber workforce transformation activities, as outlined below:

## National Cyber Strategy



## Federal Cybersecurity Workforce Assessment Act



## EO on America's Cybersecurity Workforce

### Executive Order on America's Cybersecurity Workforce

ECONOMY & JOBS | Issued on: May 2, 2019

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to better ensure continued American economic prosperity and national security, it is hereby ordered as follows:

**Section 1. Policy.** (a) America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), each emphasize that a superior cybersecurity workforce will promote American prosperity and preserve peace. America's cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and maintain the data, systems, and networks on which our economy and way of life depend. Whether they are employed in the public or private sectors, they are guardians of our national and economic security.

b) The United States Government must enhance the workforce mobility of America's cybersecurity practitioners to improve America's national

## Cybersecurity Talent Initiative

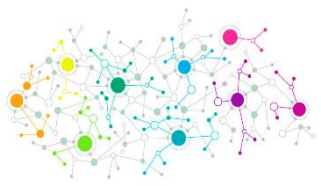


CIOP.GOV

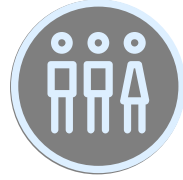
## Federal Cybersecurity Reskilling Academy



FEDERAL CYBER  
RESKILLING ACADEMY



# The Inter-Agency Federal Cyber Career Pathways Initiative



## WHO?

---

Working Group of cyber workforce representatives from the **24 CFO Act Federal agencies**.



## WHAT?

---

A **standard Federal career pathway framework** unique to each NICE Framework Work Role.

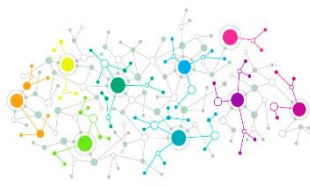


## WHY?

---

- **Merge disparate efforts.**
- **Standardize** implementation of the NICE Framework
- **Recruit, retain, and develop** the cyber workforce of the future
- Foster the Federal Government's **brand** as a competitive and desirable **employer for cyber talent**.

# WG Participants and Benefits



20 of 24 CFO Act D/As

### Decentralized Model

- **9** Technical SMEs @ 16 hours / work role
- **3** Cyber Workforce Managers @ 148 hours / work role

**X 52** Work Roles  
**X 24** Agencies  
=

- **689k** hours of **SME / WF Manager Time**

**X \$56/hour** (est. GS-14, Step 1)  
=

\$
**Total Federal-wide spend = \$38.7M**

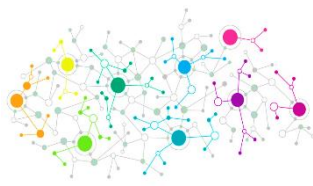
### Centralized Model

- **2** Technical SMEs @ 16 hours / work role  
**X 52** Work Roles
- **3** Cyber Workforce Managers @ 136 hours  
**X 2** work roles  
=
- **60k** hours of **SME / WF Manager Time**

**X \$56/hour** (est. GS-14, Step 1)  
=

💰
**Total Federal-wide spend = \$3.3M,**

**Cost Avoidance:  
\$35M and 629k hours of effort**



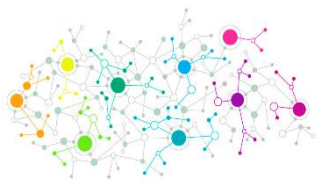
# Why are we Developing Career Paths?

Career paths are designed to support cyber professionals, their supervisors, and human capital professionals with a range of workforce related activities, as outlined below:



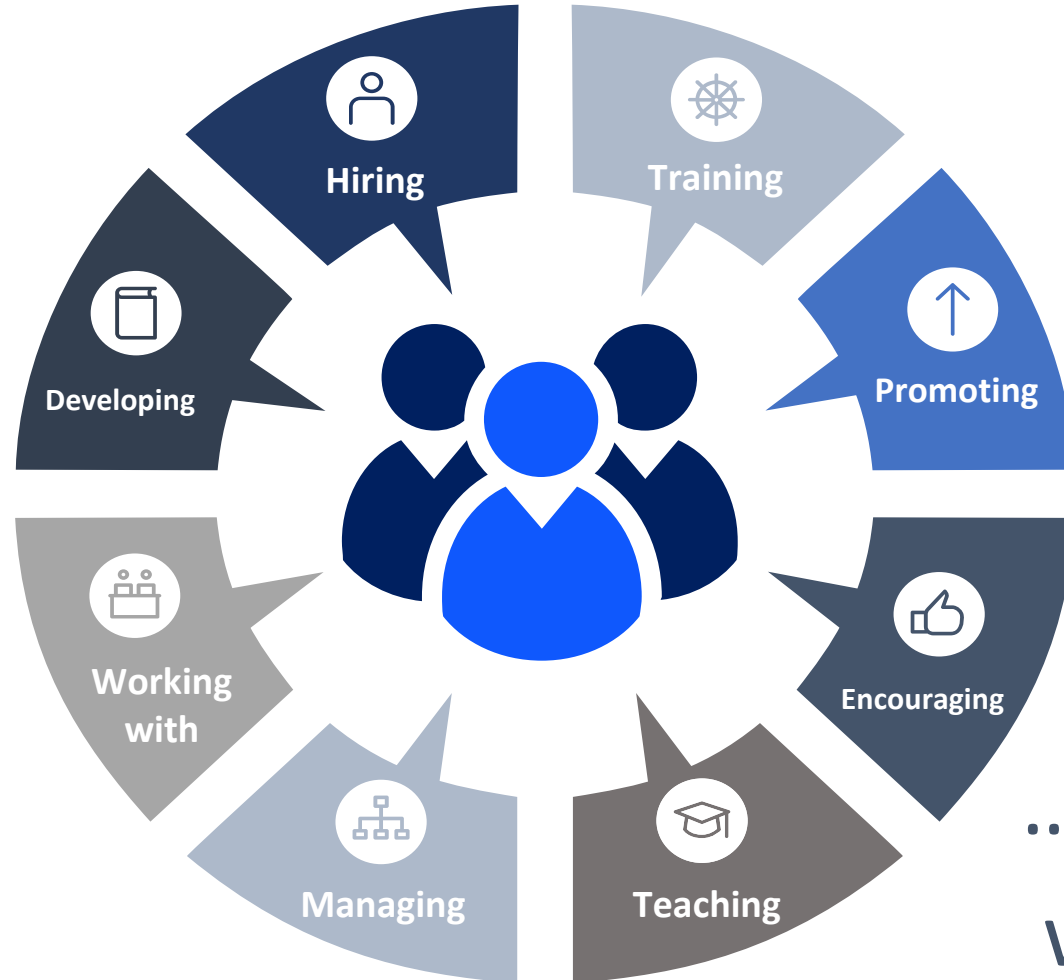
★ Note: These career paths are meant to be a framework; and can be tailored to meet the needs of each individual agency's workforce.





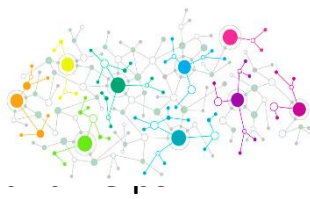
# Who does this benefit?

Everyone involved in....



...people in a  
work role.

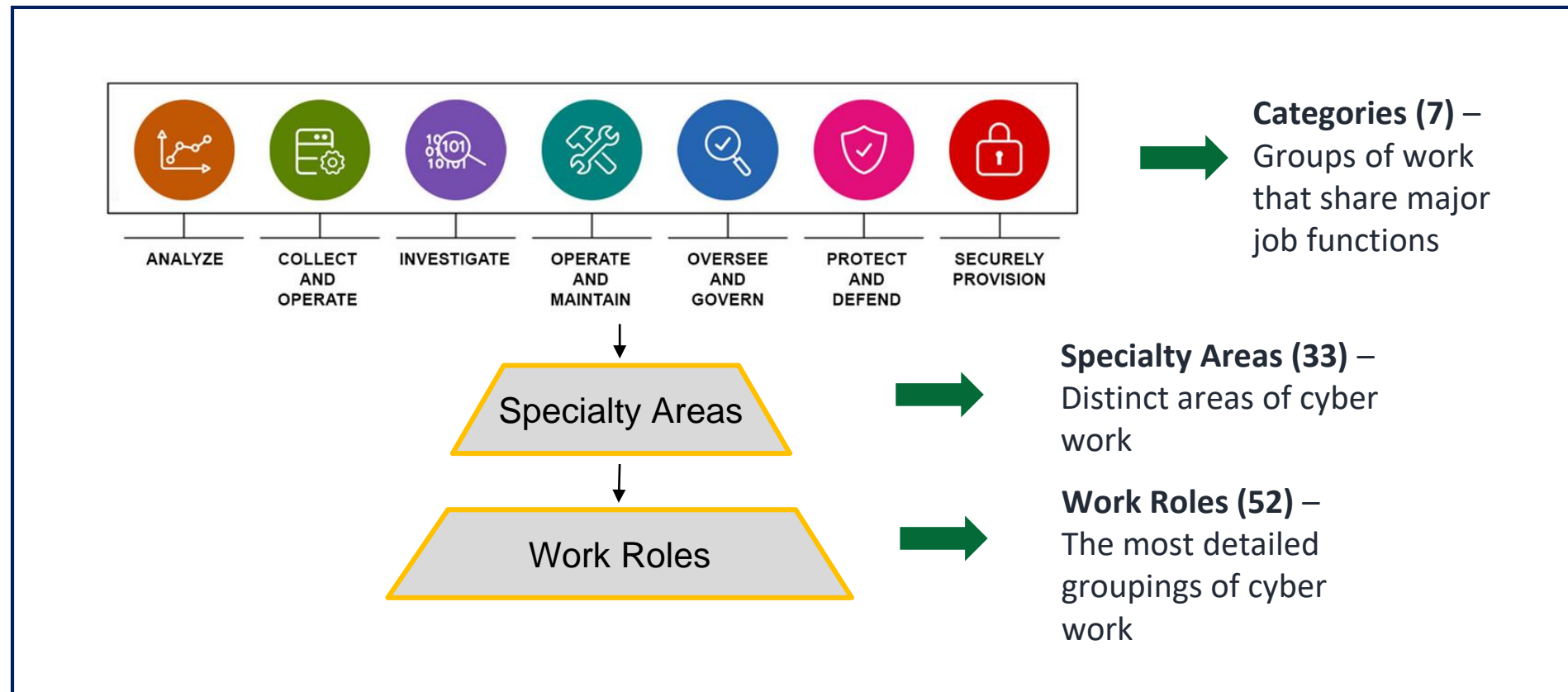
# Defining the Cyber Workforce



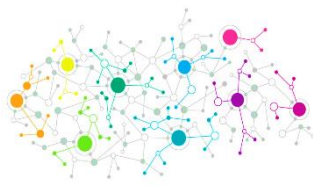
The National Initiative for Cybersecurity Education (NICE) Framework provides a common language to describe cyber positions and define professional requirements in cyber. OPM requires all departments and agencies to map all cyber positions using the NICE Framework's work role codes.



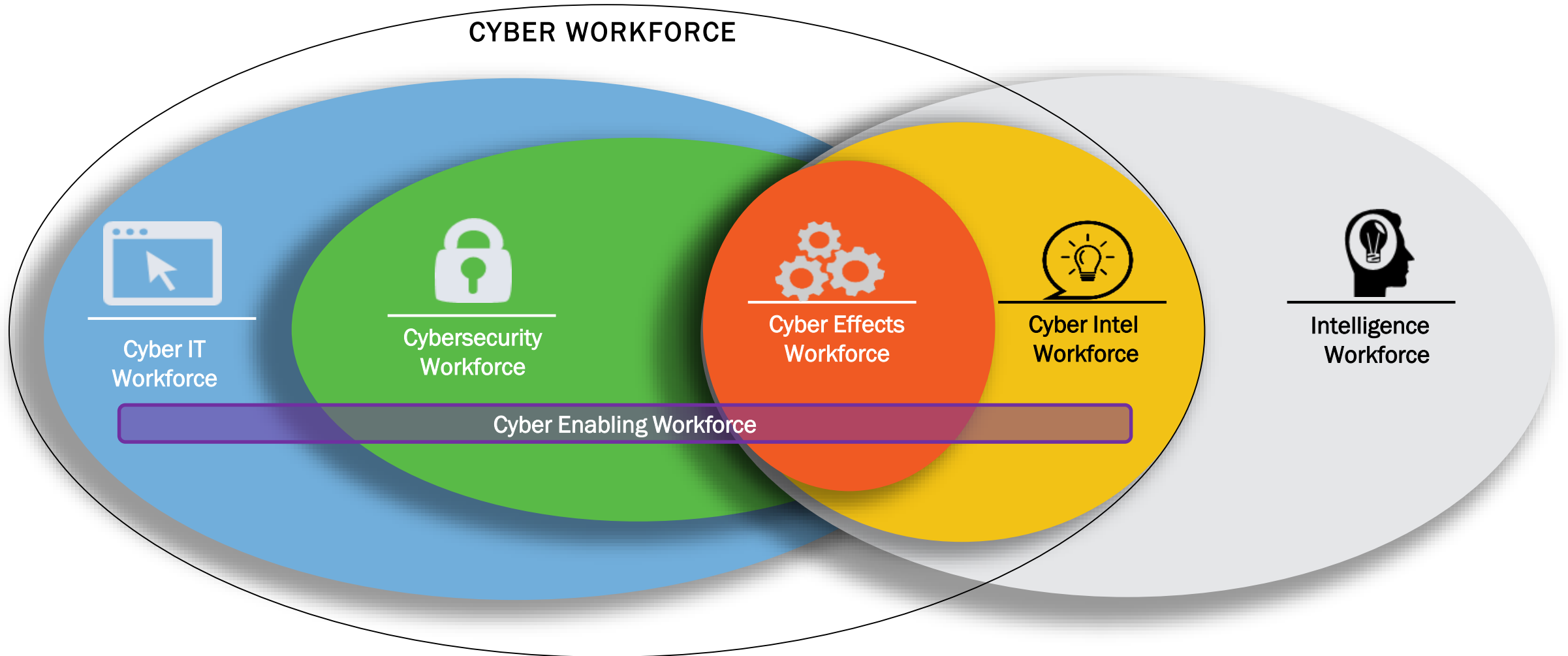
The Framework organizes the cyber workforce as outlined below:



# Cyber Communities



Moving forward, focus groups will be completed community by community, as depicted by the graphic below.



# Cyber Communities, Continued



## Cyber IT

- Data Analyst (422)
- Database Administrator (421)
- Enterprise Architect (651)
- Knowledge Manager (431)
- Network Ops Specialist (441)
- Requirements Planner (641)
- R&D Specialist (661)
- Software Developer (621)
- System Administrator (451)
- Systems Developer (632)
- Tech Support Specialist (411)
- T&E Specialist (671)

12

## Cybersecurity

- Authorizing Official (611)
- COMSEC Manager (723)
- Cyber Defense Analyst (511)
- Cyber Def Forensics Analyst (212)
- Cyber Def. Incident Res. (531)
- Cyber Def. Infra Spt Spec. (521)
- Info Sys Sec Developer (631)
- Info Sys Sec Mgr (722)
- Secure SW Assessor (622)
- Security Architect (652)
- Security Control Assessor (612)
- Systems Security Analyst (461)
- Vulnerability Analyst (541)

13

## Cyber Effects

- Cyber Operator (321)
- Cyber Ops Planner (332)
- Exploitation Analyst (121)
- Partner Integr. Planner (333)
- Mission Assess. Spec. (112)
- Target Network Analyst (132)
- Target Developer (131)
- Threat/Warning Analyst (141)

8

## Intel

- All Source Analyst (111)
- All Source Collection Mgr (311)
- All Source Collection Reqs Mgr. (312)
- Cyber Intelligence Planner (331)
- Multi Disc Language Analyst (151)

5

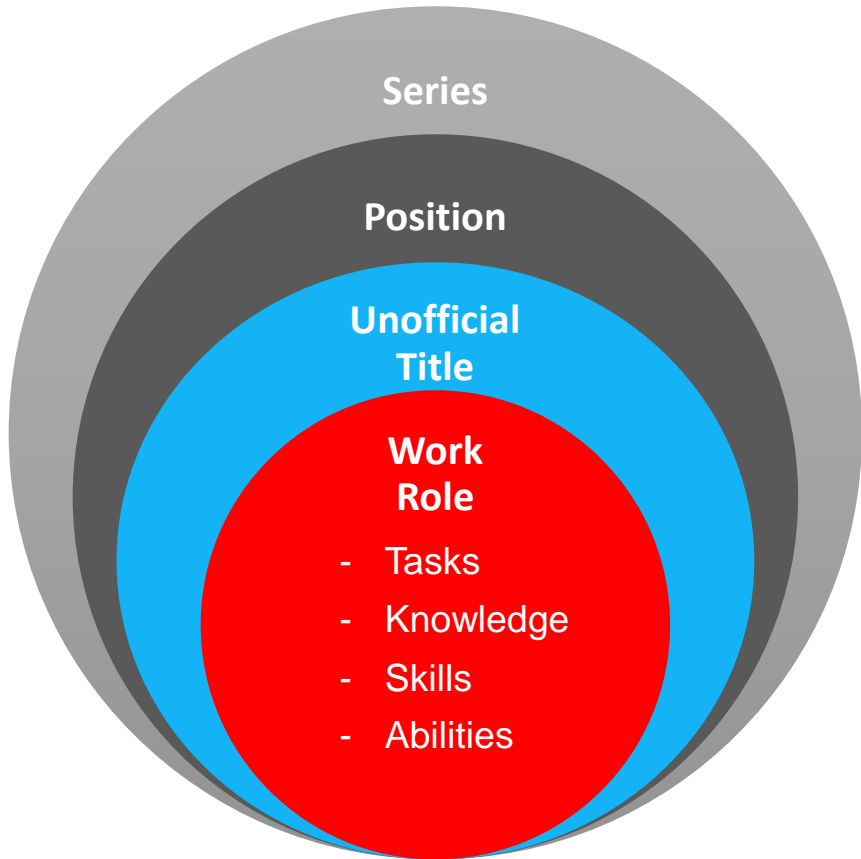
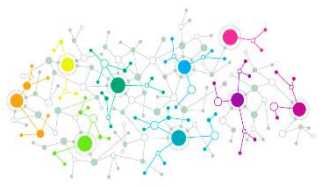
**Acquisition/Program Integration:** IT Invest/Portfolio Manager (804), IT Project Manager (802), Program Manager (801), Product Support Manager (803), IT Program Auditor (805) 5

**Training & Education:** Cyber Instructor (712), Cyber Instr./Curriculum Dev. (711), Cyber WF Developer & Manager (751) 3

**Legal/Law Enforcement:** Legal Advisor (731), Cyber Crime Investigator (221), Forensics Analyst (211) 3

**Leadership:** Cyber Policy/Strat Planner (752), Executive Cyber Leadership (901), Privacy Compliance Manager (732) 3

# Work Roles



Hi, I'm Charlene.  
Let me tell you a little bit about myself...

**Charlene Bailey**

**Series:** 2210 Information Technology Management Series

**Position:** IT Specialist (INFOSEC)

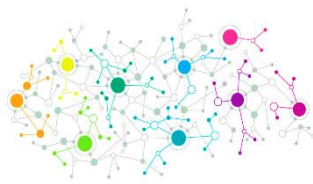
**Unofficial Title:** Cyber Analyst

**Cyber Community:** Cybersecurity

**Work Role:** Cyber Defense Analyst

**Task(s):** Reconstruct a malicious attack or activity based off network traffic.

**Fun Fact:** I recently won a Hack-a-thon!



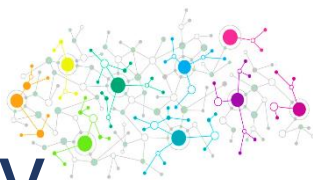
# Role Overview

# Core Tasks

Cyber Defense Analyst Work Role Overview	
<b>NICE Role Description</b>	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
<b>Description Enhancements</b>	<p><b>Additions from focus group:</b></p> <ul style="list-style-type: none"> <li>Conduct analysis based on trends and intelligence data</li> <li>Analyze processes and procedures</li> <li>Continuously update processes and procedures</li> </ul> <p><b>Proposed new definition:</b> Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to continuously analyze events and identify trends that occur within their environments in order to enhance defensive capabilities, processes, and procedures for purposes of mitigating threats.</p>

<b>OPM Occupational Series</b>	The 511-Cyber Defense Analyst work role is most likely found within the following Occupational Series: <ul style="list-style-type: none"> <li>2210-Information Technology (INFOSEC)</li> </ul>
<b>Complimentary Roles</b>	The 511-Cyber Defense Analyst work role shares similar Tasks, Knowledge, Skills, and Abilities, or functions with the following NICE Framework work roles: <ul style="list-style-type: none"> <li>461-Systems Security Analyst</li> <li>531-Cyber Defense Incident Responder</li> <li>212-Cyber Defense Infrastructure Support Specialist</li> <li>541-Vulnerability Assessment Analyst</li> </ul>
<b>General Schedule (GS)</b>	Personnel performing the 511-Cyber Defense Analyst work role most likely occupy the following General Schedule grades: <ul style="list-style-type: none"> <li>GS-11 through GS-14</li> </ul>
<b>Unofficial / Also-Known-As Titles</b>	Personnel performing the 511-Cyber Defense Analyst work role may unofficially or alternatively be called: <ul style="list-style-type: none"> <li>Computer Network Defense (CND) Analyst</li> <li>Cybersecurity Analyst</li> <li>Incident Analyst</li> <li>Network Defense Technician</li> <li>Network Security Engineer</li> <li>Security Analyst</li> <li>Security Operator</li> <li>Sensor Analyst</li> <li>Senior Network Security Engineer</li> <li>Focused Operations Security Analyst</li> </ul>

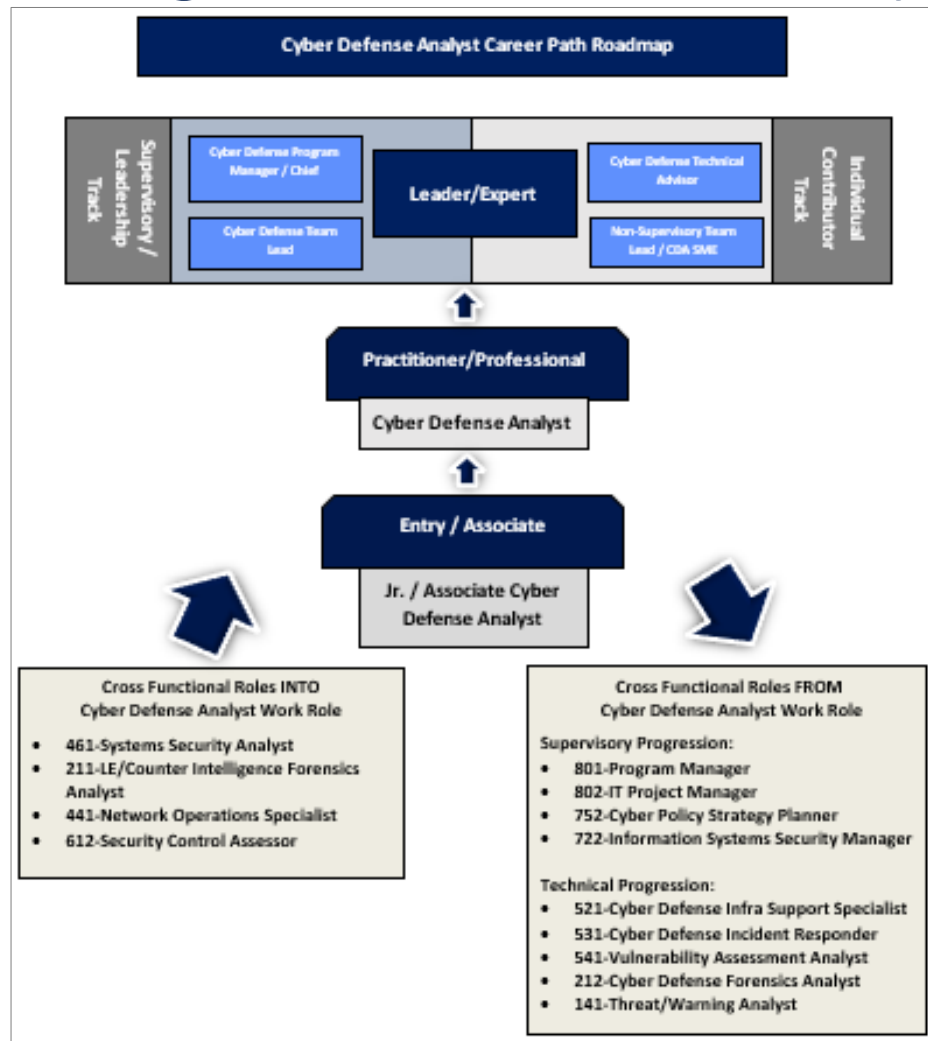
Task ID	Cyber Defense Analyst - Core Tasks	Importance
T0258	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Core
T0259	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Core
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Core
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Core
T0166	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	Core
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Core
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Core
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Core
T0164	Perform cyber defense trend analysis and reporting.	Core
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Core
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Core
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Core
T0293	Identify and analyze anomalies in network traffic using metadata.	Core
T0332	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	Core
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Core
T0299	Identify network mapping and operating system (OS) fingerprinting activities.	Additional
T0310	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.	Additional
T0298	Reconstruct a malicious attack or activity based off network traffic.	Additional
T0290	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Additional

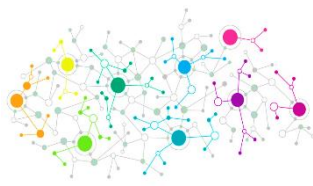


# Core Competencies

511-Cyber Defense Analyst Technical Competencies				
Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Threat Analysis	C055	KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks.	<ul style="list-style-type: none"> <li>- Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.</li> <li>- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).</li> <li>- Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).</li> <li>- Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).</li> <li>- Knowledge of countermeasure design for identified security risks.</li> <li>- Ability to analyze malware.</li> </ul>	Core
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	<ul style="list-style-type: none"> <li>- Knowledge of cyber threats and vulnerabilities.</li> <li>- Knowledge of specific operational impacts of cybersecurity lapses.</li> <li>- Knowledge of cyber defense and vulnerability assessment tools and their capabilities.</li> <li>- Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).</li> <li>- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).</li> <li>- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.</li> <li>- Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).</li> <li>- Knowledge of how to use network analysis tools to identify vulnerabilities.</li> <li>- Knowledge of penetration testing principles, tools, and techniques.</li> <li>- Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)</li> <li>- Skill in evaluating the adequacy of security designs.</li> <li>- Skill in using protocol analyzers.</li> </ul>	Core

# Progression & Mobility





# Suggested Qualifications

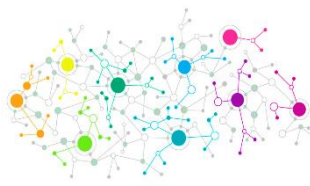
## Example of how to qualify the cyber workforce:

- Focus on demonstration of capability and increase flexibility for efficient implementation.
- Allow for a range of alternatives for achieving qualification.

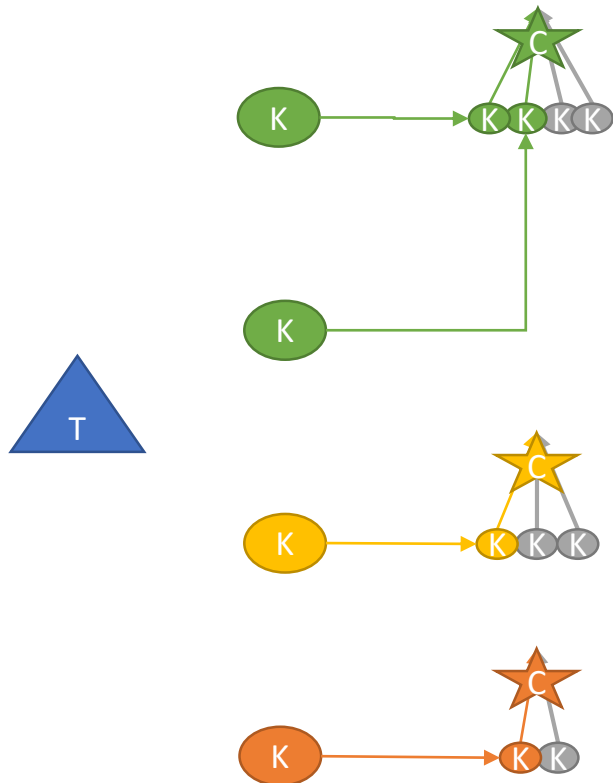
	Basic	Intermediate	Advanced
Education	Option	Option	Option
Training	Option	Option	Option
Personnel Certification	Option	Option	Option
On-the-Job Qualification	Always Required	Always Required	Always Required
Environment Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Continuous Professional Development	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.



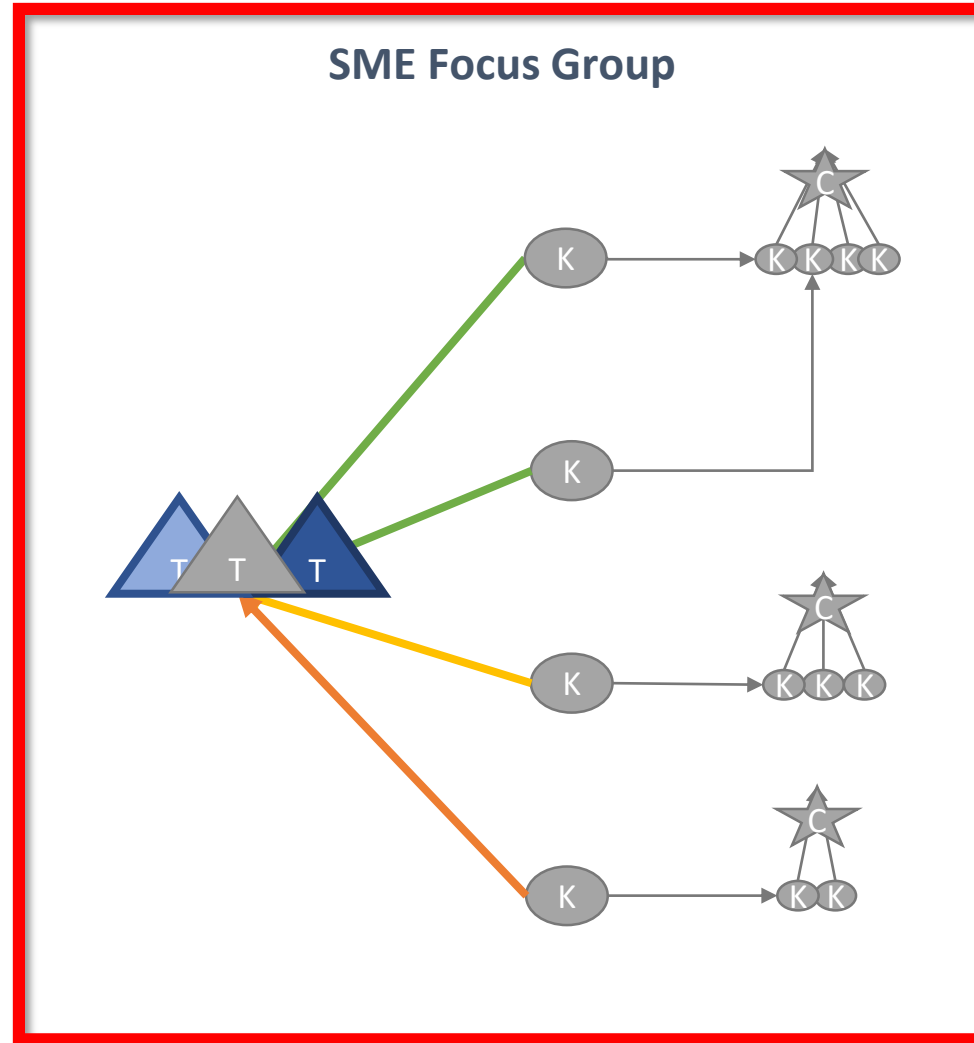
# Building the Bridge

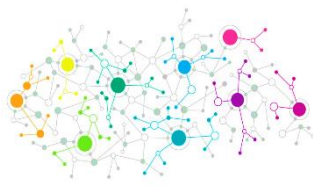


Current



SME Focus Group





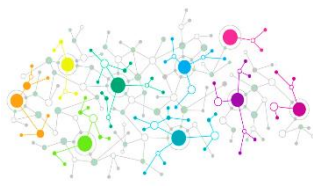
# Competency Profiles

# Task Analysis

Computer Network Defense Competency		
CD07	Competency Definition: KSAs that relate to the defensive measures to detect, respond, and protect information, information systems, and networks from threats.	Core
<b>Knowledge, Skills, and Abilities of this Competency within the work role.</b> <ul style="list-style-type: none"> <li>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.</li> <li>Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.</li> <li>Knowledge of adversarial tactics, techniques, and procedures.</li> <li>Knowledge of cyber defense and information security policies, procedures, and regulations.</li> <li>Knowledge of the common attack vectors on the network layer.</li> <li>Knowledge of signature implementation impact for viruses, malware, and attacks.</li> <li>Knowledge of intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.</li> <li>Skill in developing and deploying signatures.</li> <li>Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).</li> <li>Skill in reading and interpreting signatures (e.g., snort).</li> <li>Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).</li> <li>Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.</li> <li>Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.</li> </ul>		
<b>Tasks through which this Competency manifests itself within the Cyber Defense Analyst work role:</b> <ul style="list-style-type: none"> <li>Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity [T0259]</li> <li>Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities [T0258].</li> <li>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts [T0214].</li> </ul>		
<b>Behavioral Indicators</b> <i>(Describes how the competency manifests itself through observable work role tasks at varying proficiency levels)</i>		
<b>0</b> No Foundational Understanding	<ul style="list-style-type: none"> <li>I do not possess sufficient knowledge or skills within this Competency for use in simple or routine work situations. Any awareness, knowledge, or understanding I do have would be considered common, similar to that of a layperson. Considered "no proficiency" for purposes of accomplishing work.</li> </ul>	
<b>1</b> Entry	<ul style="list-style-type: none"> <li>Use cyber defense tools for continual monitoring and basic analysis of system activity to identify/escalate potential malicious activity.</li> <li>Support the timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these rudimentary incidents and events from benign activities.</li> <li>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.</li> </ul>	
<b>2</b> Intermediate	<ul style="list-style-type: none"> <li>Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.</li> <li>Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.</li> <li>Receive and analyze network alerts from various sources within the enterprise and determine causes of such alerts.</li> </ul>	
<b>3</b> Advanced	<ul style="list-style-type: none"> <li>Use cyber defense tools for continual monitoring and advanced analysis of system activity to identify malicious activity.</li> <li>Oversee timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these complex incidents and events from benign activities.</li> <li>Receive and analyze network alerts from various sources within the enterprise, determine causes of such alerts, and identify items for trend analysis.</li> </ul>	

Task Analysis - T0259		
Proficiency	Task Statement	Importance
As Written within Framework	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Core
Entry	Use cyber defense tools for continual monitoring and basic analysis of system activity to identify/escalate potential malicious activity.	
Intermediate	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	
Advanced	Use cyber defense tools for continual monitoring and advanced analysis of system activity to identify malicious activity.	
Primary Knowledge, Skills, and Abilities Required to Perform T0259		
KSA ID	Description	Competency
*K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
*K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense

# Process for Developing Career Pathways



## Step 1:

One of the Tri-Chair Departments will lead the focus group, and one participating agency from the Working Group will co-facilitate.



## Step 2:

SMEs from agencies across the government will participate in the focus group.



## Step 3:

The Department / Agency that hosted the focus group will synthesize the results of the session to develop a career pathway for that work role.



## Step 4:

The career pathway will be distributed to SMEs in that work role across the government for V&V.

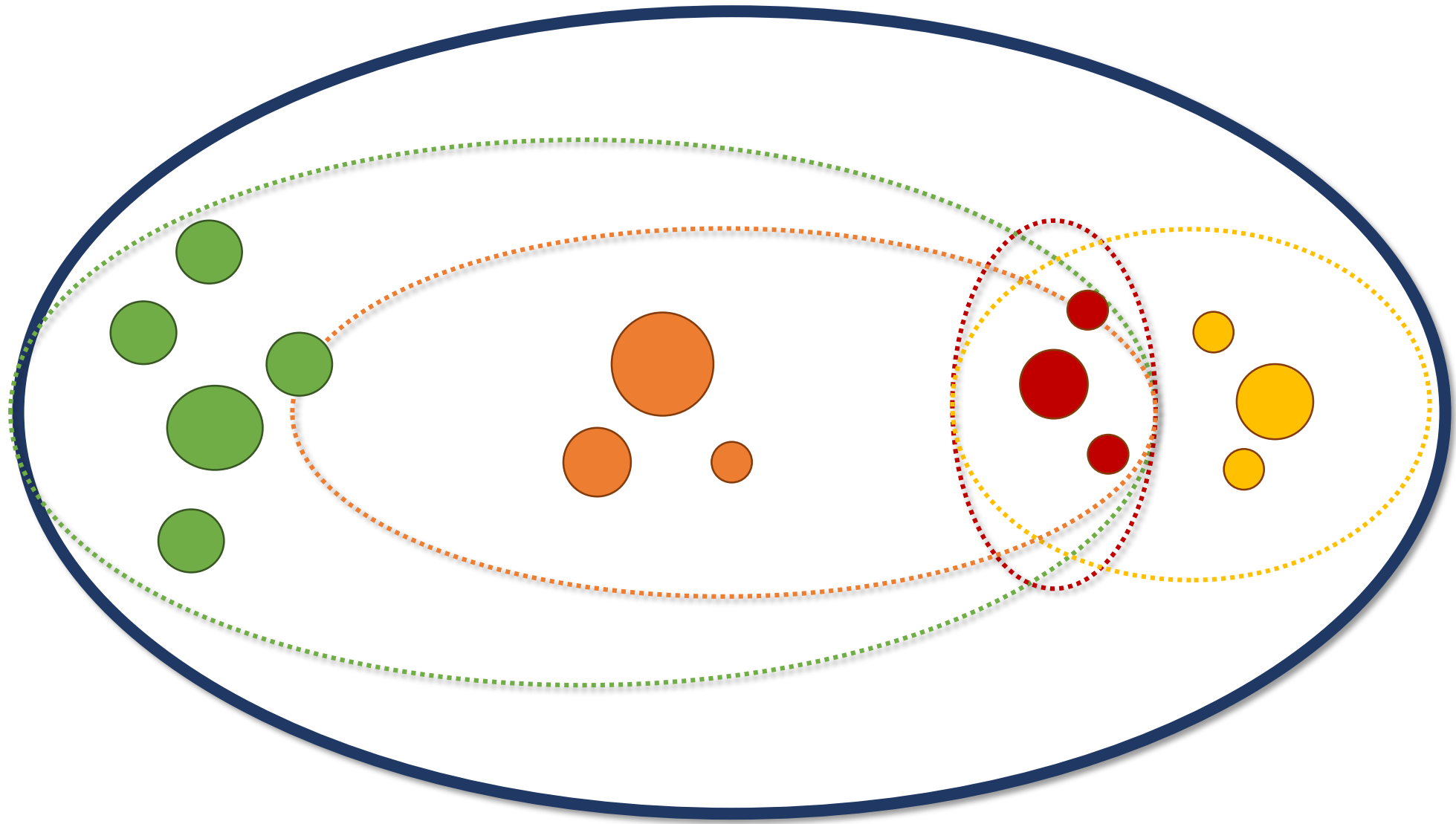
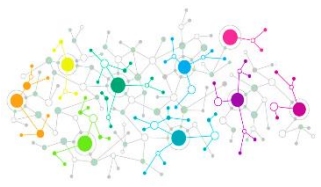


## Step 5:

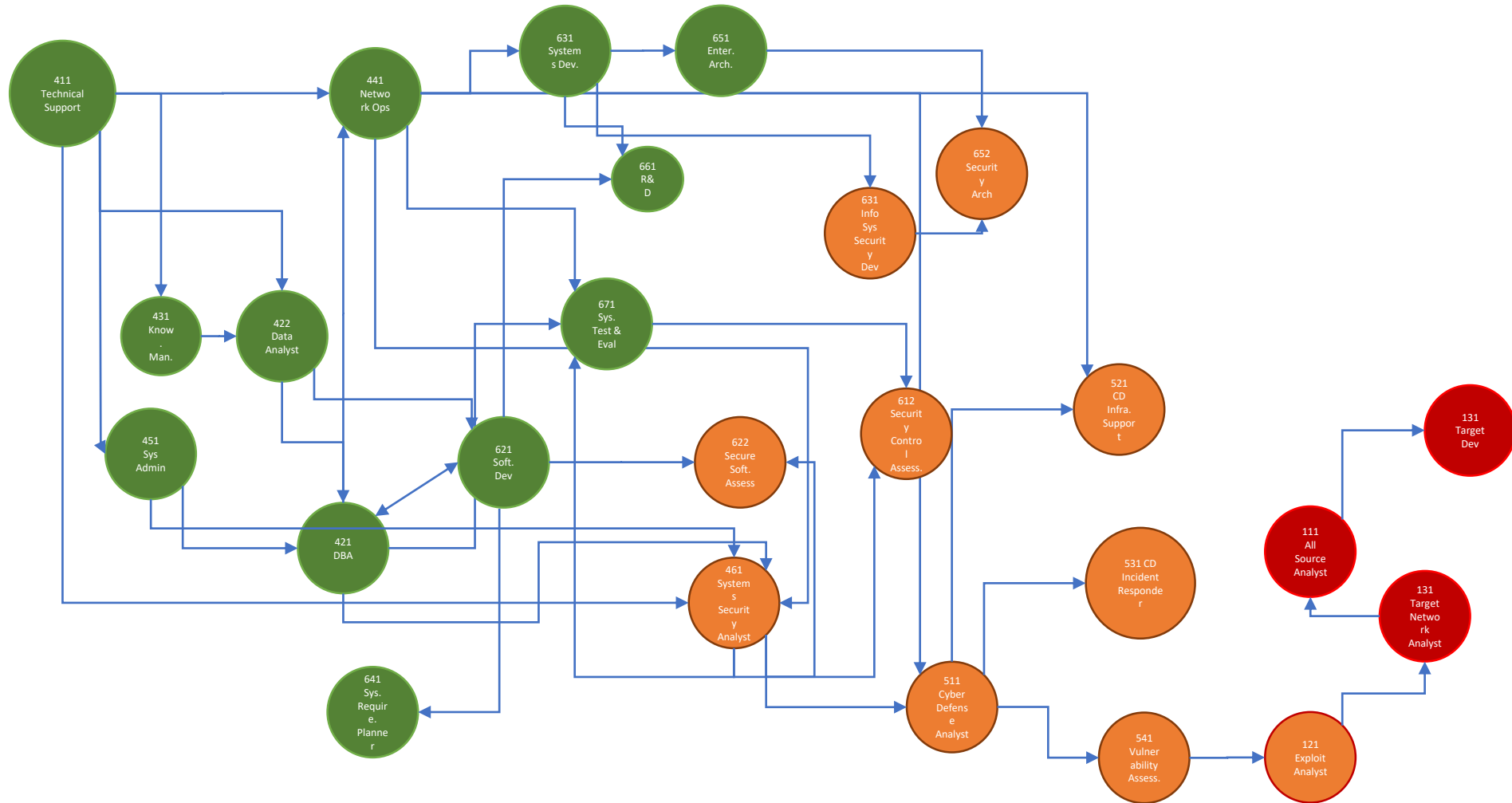
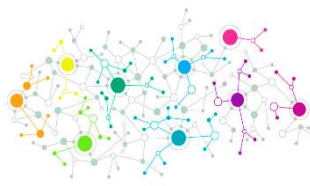
Revised career pathway will be posted on the NICCS portal for government-wide use.



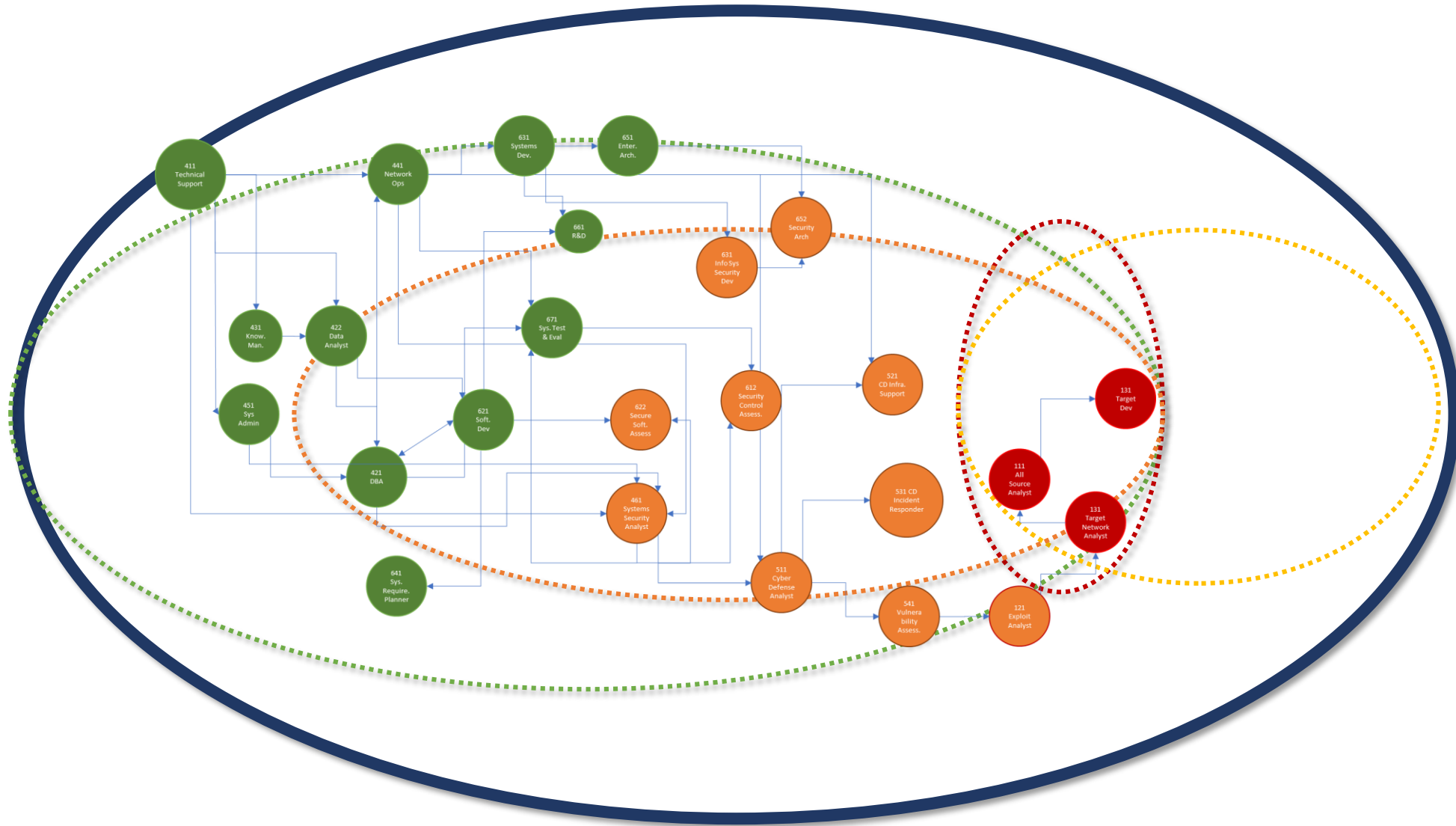
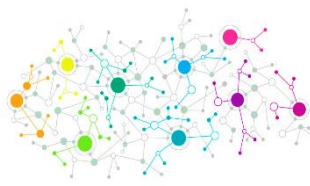
# Work Role – Community Alignment



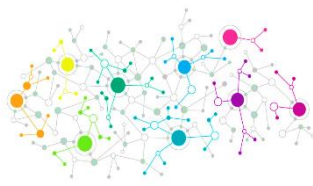
# Building the Roadmap



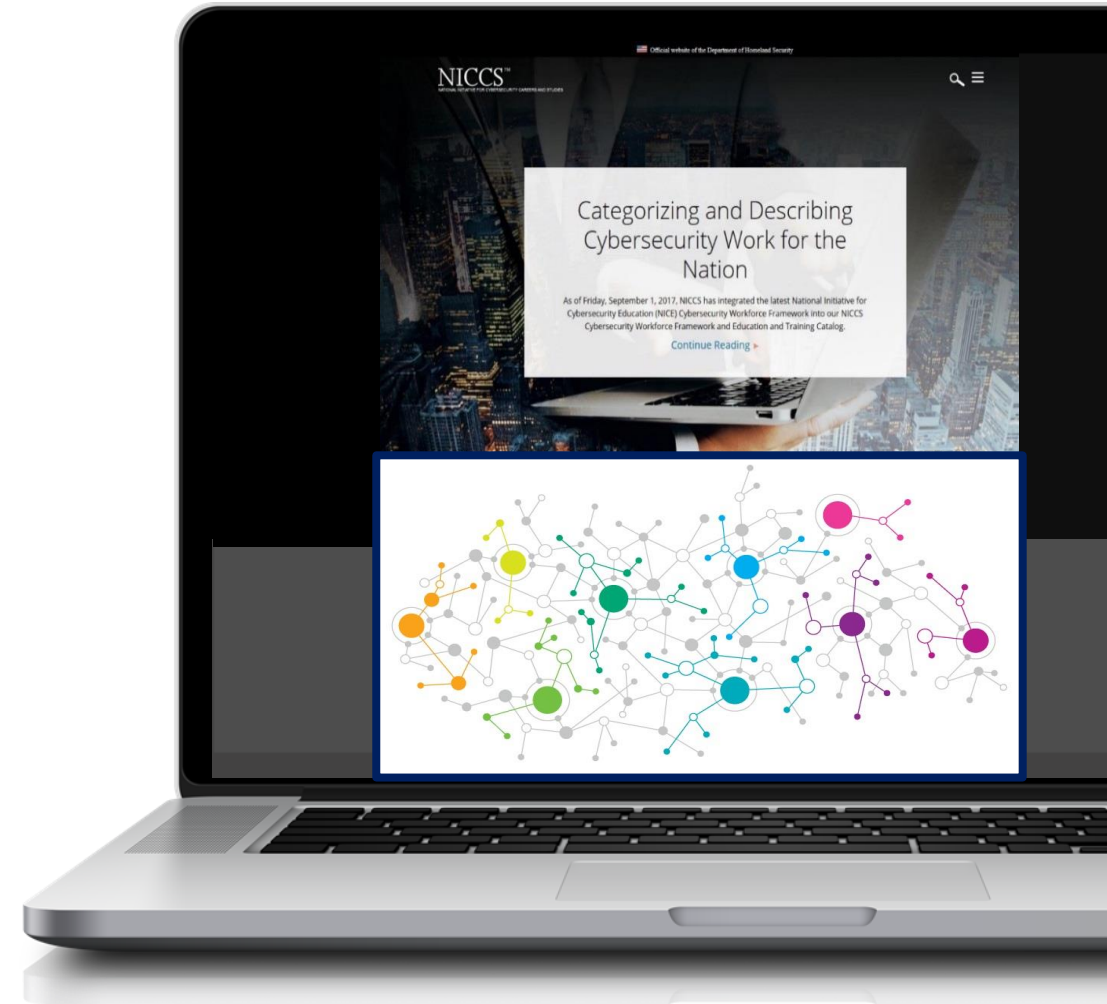
# Cyber Galaxy



# NICCS Website

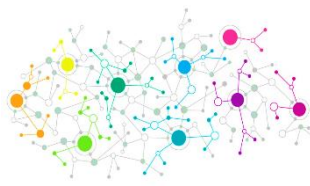


- Career pathways will be published on the National Initiative for Cybersecurity Careers and Studies (NICCS) website.
  - Website managed by the DHS CISA Cyber Education and Awareness (CE&A) team.
  - Pathways will be available for all to view.
- Quick Hits
  - 30,000+ unique visitors a month
  - 4k courses in the Training Catalogue mapped to NICE Framework
  - 100+ links to cyber resources



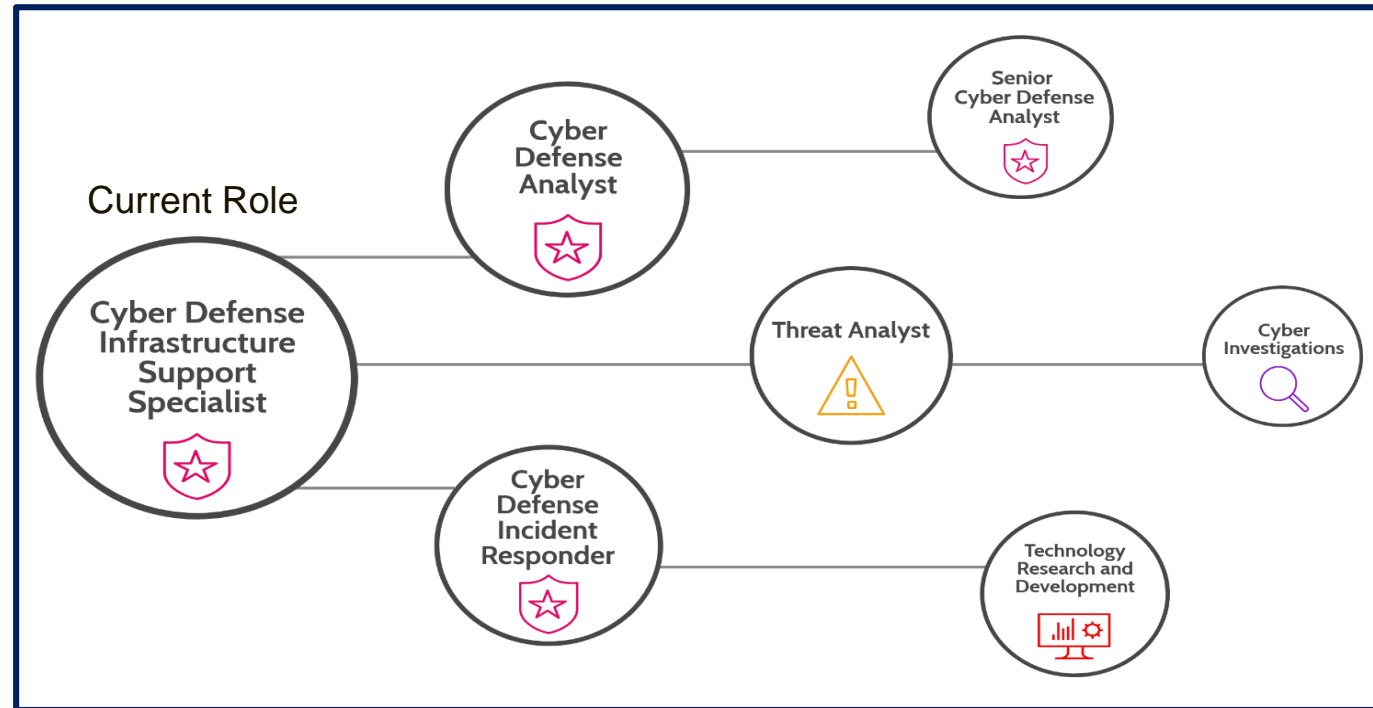
<https://niccs.us-cert.gov/>

# Cybersecurity Career Roadmaps Will Help You Plan Your Future



**COMING SOON to the NICCS website**

- ✓ Plot your current role based on your knowledge, skills, abilities, and capabilities
- ✓ Find similar Work Roles and learn the types of education, experience, and learning you will need to get there
- ✓ Plan your next career milestone using the data provided to enhance your skillset!

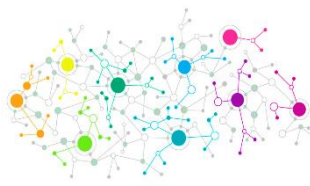



Relational alignment with current role






# Contact Us




 Christopher.Paris@va.gov



 Megan.Caposell@hq.dhs.gov



 Matthew.M.Isnor.civ@mail.mil

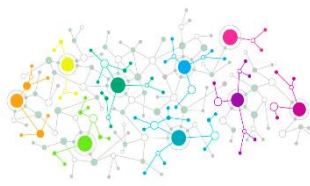
**For more information on the Inter-Agency Federal Career Path Working Group, visit our page on the OMB Max Portal:**

<https://community.max.gov/pages/viewpage.action?spaceKey=Management&title=Federal+Cybersecurity+Workforce+Interagency+Career+Path+Planning+Working+Group>

# Backup Slides



# Cyber Communities, Continued



## CYBER WORKFORCE

Personnel who **build, secure, operate, defend and protect** cyberspace resources; **conduct** related **intelligence** activities; enable **future operations**; and **protect power** in or through cyberspace. It is comprised of personnel assigned to the areas of **Cyber Effect, Cybersecurity, Cyber IT**, and portions of the **Cyber Intelligence Workforce**.

**CYBER IT:** Personnel, who **design, build, configure, operate, and maintain** IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

**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.

**CYBER 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.

**CYBER INTEL:** Personnel who **collect, process, analyze, and disseminate information** from all sources of **intelligence** on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

**CYBER ENABLERS:** Work roles employed to **support or facilitate** the functions of **cyber IT, cybersecurity, cyber effects, and/or cyber intelligence** work roles.