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 to (ISC)², 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…

595

13

48
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**
- **Cybersecurity Talent Initiative**
- **Federal Cybersecurity 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

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

### Decentralized Model
- 9 Technical SMEs @ 16 hours / work role
- 3 Cyber Workforce Managers @ 148 hours / work role

\[
\begin{align*}
\text{X 52 Work Roles} \\
\text{X 24 Agencies} \\
\text{= 689k hours of SME / WF Manager Time} \\
\text{X $56/hour (est. GS-14, Step 1)} \\
\text{= Total Federal-wide spend = $38.7M}
\end{align*}
\]

### Centralized Model
- 2 Technical SMEs @ 16 hours / work role
- 3 Cyber Workforce Managers @ 136 hours

\[
\begin{align*}
\text{X 52 Work Roles} \\
\text{X 2 work roles} \\
\text{= 60k hours of SME / WF Manager Time} \\
\text{X $56/hour (est. GS-14, Step 1)} \\
\text{= Total Federal-wide spend = $3.3M, Cost Avoidance: $35M and 629k hours of effort}
\end{align*}
\]

20 of 24 CFO Act D/As
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:

- Conducting workforce assessment & planning activities
- Creating position descriptions (PDs)
- Identifying current training needs & professional development opportunities
- Enhancing recruitment and retention initiatives
- Improving job satisfaction through rewarding & challenging career opportunities

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:

- Hiring
- Training
- Promoting
- Developing
- Working with
- Encouraging
- Managing
- Teaching

...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:

- **Categories (7)** – Groups of work that share major job functions
- **Specialty Areas (33)** – Distinct areas of cyber work
- **Work Roles (52)** – The most detailed groupings of cyber work
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)

**Cybersecurity**
- Authorizing Official (611)
- COMSEC Manager (723)
- Cyber Defense Analyst (511)
- Cyber Def. Forensics Analyst (212)
- Cyber Def. Incident Res. (531)
- Cyber Def. Infra Sot 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)

**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)

**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)

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

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

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

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Cyber Defense Analyst - Core Tasks</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0256</td>
<td>Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.</td>
<td>Core</td>
</tr>
<tr>
<td>T0255</td>
<td>Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.</td>
<td>Core</td>
</tr>
<tr>
<td>T0155</td>
<td>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.</td>
<td>Core</td>
</tr>
<tr>
<td>T0260</td>
<td>Analyze identified malicious activity to determine weaknesses-exploited or exploitation methods, effects on system and information.</td>
<td>Core</td>
</tr>
<tr>
<td>T0166</td>
<td>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.</td>
<td>Core</td>
</tr>
<tr>
<td>T0294</td>
<td>Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warning).</td>
<td>Core</td>
</tr>
<tr>
<td>T0214</td>
<td>Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.</td>
<td>Core</td>
</tr>
<tr>
<td>T0526</td>
<td>Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.</td>
<td>Core</td>
</tr>
<tr>
<td>T0164</td>
<td>Perform cyber defense trend analysis and reporting.</td>
<td>Core</td>
</tr>
<tr>
<td>T0545</td>
<td>Work with stakeholders to resolve computer security incidents and vulnerability compliance.</td>
<td>Core</td>
</tr>
<tr>
<td>T0023</td>
<td>Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.</td>
<td>Core</td>
</tr>
<tr>
<td>T0043</td>
<td>Coordinate with enterprise-wide cyber defense staff to validate network alerts.</td>
<td>Core</td>
</tr>
<tr>
<td>T0293</td>
<td>Identify and analyze anomalies in network traffic using metadata.</td>
<td>Core</td>
</tr>
<tr>
<td>T0332</td>
<td>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.</td>
<td>Core</td>
</tr>
<tr>
<td>T0295</td>
<td>Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.</td>
<td>Core</td>
</tr>
<tr>
<td>T0306</td>
<td>Identify network mapping and operating system (OS) fingerprinting activities.</td>
<td>Additional</td>
</tr>
<tr>
<td>T0310</td>
<td>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.</td>
<td>Additional</td>
</tr>
<tr>
<td>T0296</td>
<td>Reconstruct a malicious attack or activity based on network traffic.</td>
<td>Additional</td>
</tr>
<tr>
<td>T0290</td>
<td>Determine tactics, techniques, and procedures (TTPs) for intrusion sets.</td>
<td>Additional</td>
</tr>
</tbody>
</table>
## Core Competencies

### 511-Cyber Defense Analyst Technical Competencies

<table>
<thead>
<tr>
<th>Technical Competency</th>
<th>Comp ID</th>
<th>Definition</th>
<th>Work Role Related KSAa</th>
<th>Importance</th>
</tr>
</thead>
</table>
| Threat Analysis      | 0555    | KSAa that relate to the process in which the knowledge of internal and external vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks. | - Knowledge of insider threat investigations, reporting, investigative tools and laws/regulations.  
- Knowledge of different classes of attacks (e.g., passive, active, insider, denial of service attacks).  
- Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-state sponsored, and nation-sponsored).  
- Knowledge of cyber attack stages (e.g., reconnaissance, scanning, execution, gain access, escalation of privileges, maintaining access, network exploitation, covering tracks).  
- Knowledge of countermeasure design for identified security risks.  
- Ability to analyze malware. | Core |
| Vulnerabilities      | 0557    | KSAa that relate to the principles, methods, and tools for assessing vulnerabilities and detecting or recommending appropriate mitigation countermeasures. | - Knowledge of cyber threats and vulnerabilities.  
- Knowledge of specific operational impacts of cybersecurity issues.  
- Knowledge of cyber defense and vulnerability assessment tools and their capabilities.  
- Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).  
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflows, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injection, race conditions, covert channels, replay, return-oriented attacks, malicious code).  
- Knowledge of what constitutes a network attack and a network attacker’s relationship to both threats and vulnerabilities.  
- Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark (updated)).  
- Knowledge of how to use network analysis tools to identify vulnerabilities.  
- Knowledge of penetration testing principles, tools, and techniques.  
- Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list).  
- Skills in evaluating the adequacy of security designs.  
- Skills in using penetration analyzers. | Core |

## Progression & Mobility

### Cyber Defense Analyst Career Path Roadmap

#### Entry / Associate
- Jr. / Associate Cyber Defense Analyst

#### Practitioner / Professional
- Cyber Defense Analyst

#### Leader / Expert
- Cyber Defense Technical Analyst
- Cyber Defense Team Lead
- Cyber Defense Manager / Chief

### Cross Functional Roles INTO Cyber Defense Analyst Work Role
- 461-Systems Security Analyst
- 211-14/Counter Intelligence Forensics Analyst
- 461-Network Operations Specialist
- 612-Security Control Assessor

### Cross Functional Roles FROM Cyber Defense Analyst Work Role

#### Supervisory Progressions:
- 101-Program Manager
- 601-IT Project Manager
- 752-Cyber Policy Strategy Planner
- 722-Information Systems Security Manager

#### Technical Progressions:
- 321-Cyber Defense Infra Support Specialist
- 322-Cyber Defense Incident Responder
- 142-Vulnerability Assessment Analyst
- 212-Cyber Forensics Analyst
- 161-Threat / Intrusion Analyst
## 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.

<table>
<thead>
<tr>
<th></th>
<th>Basic</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>Option</td>
<td>Option</td>
<td>Option</td>
</tr>
<tr>
<td>Training</td>
<td>Option</td>
<td>Option</td>
<td>Option</td>
</tr>
<tr>
<td>Personnel Certification</td>
<td>Option</td>
<td>Option</td>
<td>Option</td>
</tr>
<tr>
<td>On-the-Job Qualification</td>
<td>Always Required</td>
<td>Always Required</td>
<td>Always Required</td>
</tr>
<tr>
<td>Environment Specific Requirements</td>
<td>Component Discretion</td>
<td>Component Discretion</td>
<td>Component Discretion</td>
</tr>
<tr>
<td>Continuous Professional Development</td>
<td>&gt; Of 20 Hours/Year Or Cert. Rqmt.</td>
<td>&gt; Of 20 Hours/Year Or Cert. Rqmt.</td>
<td>&gt; Of 20 Hours/Year Or Cert. Rqmt.</td>
</tr>
</tbody>
</table>
Building the Bridge

Current

SME Focus Group
## Competency Profiles

### Task Analysis

#### Core

<table>
<thead>
<tr>
<th>Task Analysis</th>
<th>Task Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
<tr>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
<td>Use cyber defense tools for continuous monitoring and analysis of system activity to identify malicious activity.</td>
</tr>
</tbody>
</table>
## 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!
For more information on the Inter-Agency Federal Career Path Working Group, visit our page on the OMB Max Portal:

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.