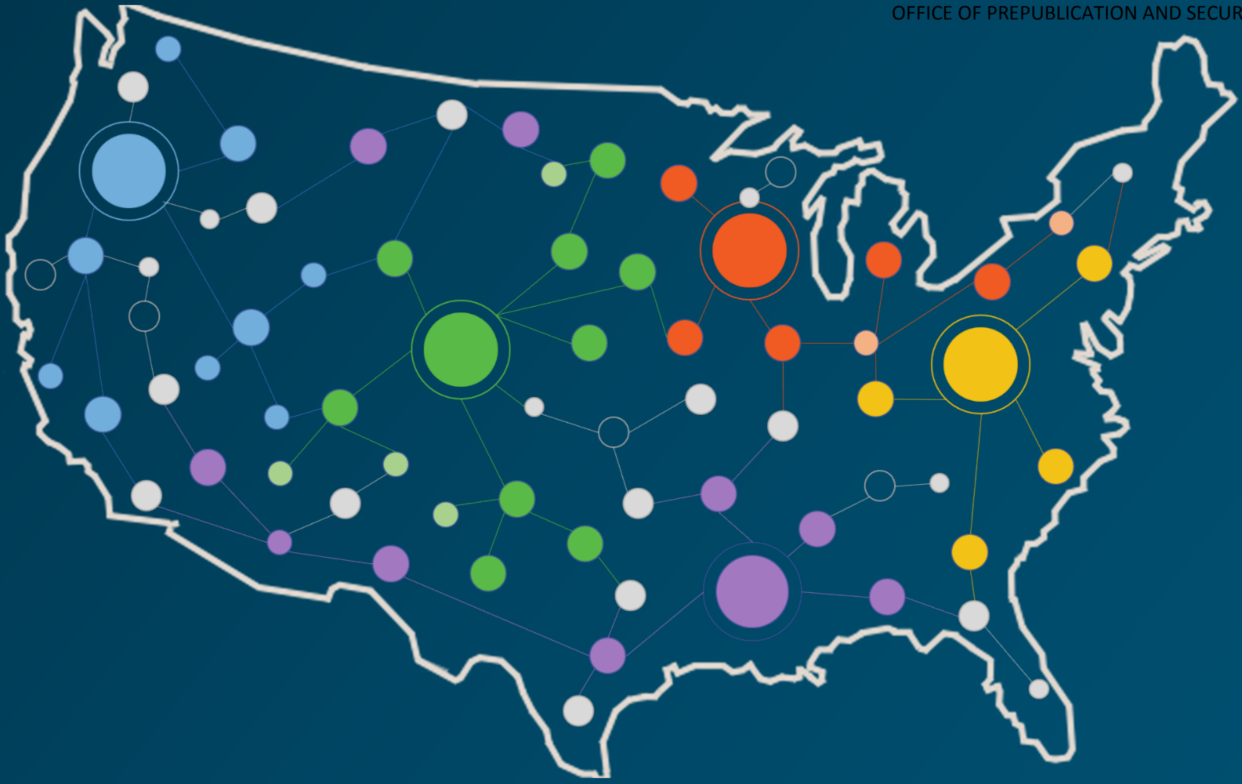
INTERAGENCY FEDERAL CYBER CAREER PATHWAYS INITIATIVE

Collectively Developing Career Resources for the Federal Cyber Workforce

November 2020



Christopher Paris
Cyber Workforce Management
Office of the VA Chief Information Officer

Matthew Isnor
DoD Cyberspace Workforce Development
Office of the DoD Chief Information Officer

Megan Caposell
Workforce Planning and Talent Management
Office of the CISA Chief Human Capital Officer

Contents

Executive Summary

The United States must increase its cyber workforce by 300k, or 62%, in order to meet existing demands. Globally, the world's cyber workforce will need to increase by 145%[1]. This growing cyber talent gap, coupled with the increasing sophistication of cyber attacks, underscores the need for innovative and forward thinking solutions that leverage the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) to build a highly robust, skilled, and resilient Federal cyber workforce. Application of the NICE Framework for the development of cyber career resources directly supports the National Cyber Strategy[2], Executive Order (EO) 23870, *America's Cybersecurity Workforce*[3], and the Federal Cybersecurity Assessment Act (FCWAA)[4] of 2015. Furthermore, because the entire Federal Government is mandated by law to align cyber positions to the NICE Framework, it's imperative that Federal Departments and Agencies (D/As) work collectively to develop resources that can be used across Federal organizations. To that end, the Interagency Federal Cyber Career Pathways Working Group was established.

Established and co-chaired by the Department of Defense (DoD), Department of Homeland Security / Cybersecurity Infrastructure Security Agency (DHS/CISA), and Department of Veterans Affairs (VA), the Interagency Federal Cyber Career Pathway Working Group (Working Group) was formed in July 2019 with Federal endorsement from the Chief Information Officer Council (CIOC), Chief Human Capital Officer Council (CHCOC), and Chief Learning Officer Council (CLOC). The Working Group operates with the ultimate intent of working collectively with Interagency partners to develop baseline cyber career resources aligned with NICE Framework Work Roles. More specifically, the Working Group seeks to merge disparate federal cyber workforce efforts, develop and promote cyber workforce guidance and best practices, and standardize implementation of the NICE Framework by creating Cyber Career Pathways (Pathways) for NICE Framework Work Roles.

Pathways will serve as baseline resources that will enable the Federal Government to develop targeted strategies for recruiting, retaining, and developing the cyber workforce of the future while fostering the Federal Government's brand as a competitive and desirable employer for cyber talent. This report details the establishment of the Working Group, its objectives, intended audiences and applications, and the methodology followed to collectively develop baseline Pathways.

Working Group-developed Pathways are publicly accessible on the DoD Cyber Exchange website: https://public.cyber.mil/cw/pathways.

[1] International Information System Security Certification Consortium (ISC)^2, Cybersecurity Workforce Study 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482, Page 3

[2] President Donald J. Trump, National Cyber Strategy, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[3] Executive Office of the President, Executive Order 13870, https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

[4] 114th Congress, Federal Cybersecurity Workforce Assessment Act (FCWAA), https://www.congress.gov/bill/114th-congress/senate-bill/2007

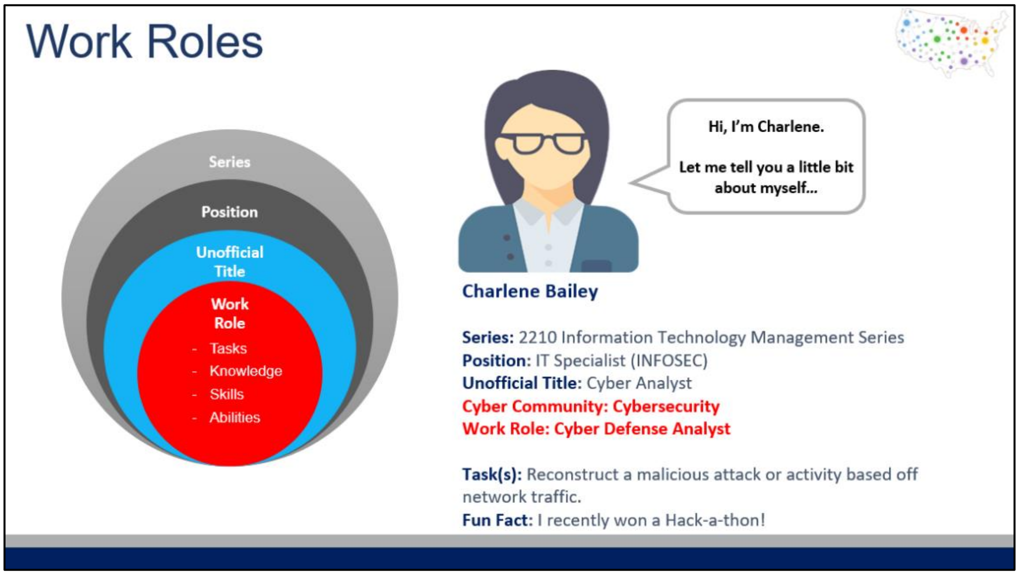
Background – Understanding the Cyber Workforce

NICE Framework

The NICE Framework was developed in partnership with NIST, DHS, DoD, and other Federal D/As. From its inception, it was designed to be a reference resource for the Federal Government as well as industry and academia. The NICE Framework provides a common language that defines 52 different types of cyber work, in the form of Work Roles, as well as the knowledge, skills, abilities, and tasks (KSATs) required to perform those roles. The NICE Framework comprises seven Categories, 33 Specialty Areas, 52 Work Roles, and thousands of KSATs:

- **Category:** Describes similar types of work that share common functions. Each Category contains several Specialty Areas.
- **Specialty Area:** Describes common types of cyber work. Specialty Areas within a Category are typically more similar than Specialty Areas in other Categories. Each Specialty Area contains one or more cyber work roles that typically execute key functions.
- **Work Role:** Describes a related set of responsibilities required to execute key functions within a work role. Work roles consist of a definition, as well as a representative list of tasks and KSAs.
- **Task:** Activities an individual performs on a regular basis to carry out the functions of a job.
- **KSAs:** Attributes required to perform Tasks, often demonstrated through qualifying experience, education, or training.

Work Roles allow organizations to view, understand, and analyze their cyber workforce in a comprehensive yet focused manner. As illustrated by Figure 1, Work Roles provide the Federal Government with workforce insight beyond existing Occupational Series, Parentheticals, and official Position Titles. By aligning the workforce to Work Roles within the NICE Framework, organizations can develop targeted recruitment, training, career development, and retention strategies.



Work Roles

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!

Figure 1. Work Role

Cyber Skill Communities

In an effort to promote broad implementation of the NICE Framework, and to address the full scope of cyber work and workers represented within it, the Working Group developed the concept of skill communities that depict the alignment of similar skills falling within the cyber workforce. As shown in Figure 2, the cyber workforce consists of the following skills communities:

- **IT:** Skills required to 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:** Skills required to 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 cyber capabilities.
- **Cyber Effects:** Skills required to plan, support, and execute cyber capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.
- **Intel (Cyber):** Skills required to collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.
- **Cross-Functional:** Skills required to lead, acquire, and manage cyber initiatives; develop cyber workforce talent; and conduct cyber related legal and law enforcement activities.

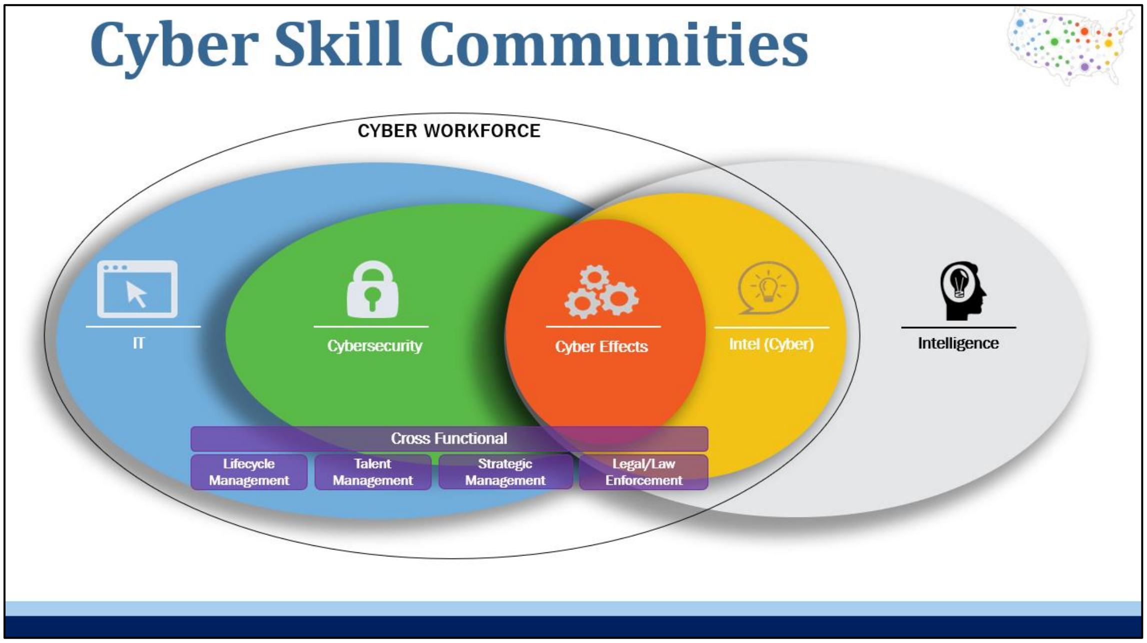
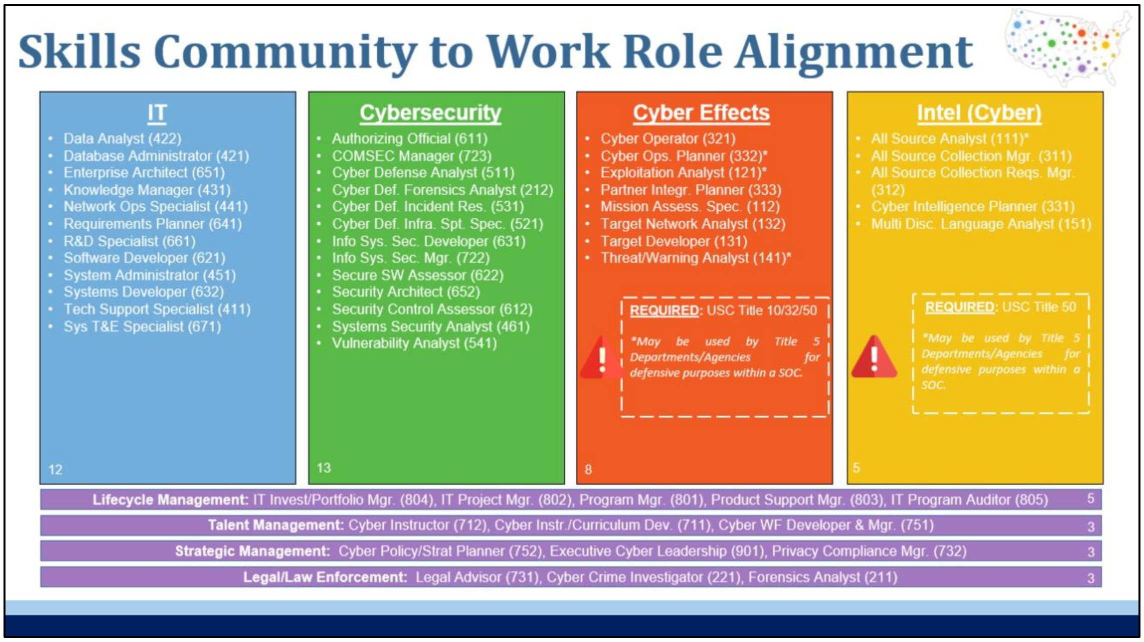


Figure 2. Cyber Workforce / Cyber Skills Communities

This depiction unifies distinct elements of the cyber workforce under a common umbrella. Notably, it presents cybersecurity as a skill community within the larger cyber workforce; which will aid Federal practitioners, as well as industry and academia stakeholders in understanding that multiple communities are represented within the NICE Framework beyond those focused on explicit cybersecurity functions. Finally, to fully support further application of cyber skill communities, the Working Group aligned NICE Framework work roles to each respective community, as shown in Figure 3.



Skills Community to Work Role Alignment

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)
- Sys 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)*

REQUIRED: USC Title 10/32/50

**May be used by Title 5 Departments/Agencies for defensive purposes within a SOC.*

8

Intel (Cyber)

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

REQUIRED: USC Title 50

**May be used by Title 5 Departments/Agencies for defensive purposes within a SOC.*

5

Lifecycle Management: IT Invest/Portfolio Mgr. (804), IT Project Mgr. (802), Program Mgr. (801), Product Support Mgr. (803), IT Program Auditor (805) 5

Talent Management: Cyber Instructor (712), Cyber Instr./Curriculum Dev. (711), Cyber WF Developer & Mgr. (751) 3

Strategic Management: Cyber Policy/Strat Planner (752), Executive Cyber Leadership (901), Privacy Compliance Mgr. (732) 3

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

Figure 3. Work Role Alignment to Cyber Skills Communities

Cyber skills communities, and the alignment of Work Roles to these communities, served a pivotal function in the collective development of Pathways. It allowed the Working Group to depict and clarify the scope and intended audiences Pathways were being created for. The alignment also allowed the Working Group to more strategically identify, solicit, and obtain active participation from cyber practitioners throughout the Federal Government in support of objectives detailed in following sections of the Report.

Interagency Federal Cyber Career Pathways Initiative

Problem / Business Need

America's cyber workforce is a strategic asset that protects the American people, the homeland, and the American way of life. Currently, the nation finds itself in the middle of a cyber workforce crisis. There simply aren't enough qualified cyber professionals to fill current job openings. Right now, there are over 72k vacant cyber jobs in the DC Metro area alone, with over 500k positions vacant domestically[5]. The Federal Government must take drastic steps now to not only build a pipeline of qualified cyber professionals for the future, but also to develop mechanisms for upskilling, reskilling, and enabling the current workforce to fill important cyber positions.

The Executive and Legislative Branches have issued policies and codified requirements, such as the National Cyber Strategy, the President's Management Agenda, and EO 13870[3], *America's Cybersecurity Workforce*, to improve the Federal Government's ability to acquire, build, and retain talent and ultimately develop the tools and capacity for cyber practitioners and talent managers to overcome the current shortage of cyber talent. Nationally, initiatives have been developed that focus on creating innovative approaches to providing opportunities that maximize individuals' cyber knowledge, skills, and abilities. Integral to overcoming these challenges are baseline Federal requirements and career resources that enable cyber professionals to visualize, build, and navigate a successful cyber career pathway within the Federal Government.

Solution

The Federal Cybersecurity Workforce Assessment Act (FCWAA)[6] mandated that all Federal D/As align positions performing IT, cybersecurity, and cyber-related functions to up to three Work Roles from the NICE Framework. While the requirement to map cyber focused positions to Work Roles was clear, what it meant to occupy a position aligned with Work Roles from the NICE Framework was not.

In October 2018, an interagency group of cyber workforce developers, familiar with the NICE Framework and responsible for implementing requirements of FCWAA, met to brainstorm the impact and career development potential of performing Work Roles aligned with the NICE Framework. This group recognized that the Federal Government, by aligning its entire cyber workforce to a common framework, was in a unique position to collectively develop baseline requirements and career resources for cyber positions employing Work Roles from the NICE Framework. The only questions that remained were who, how, and when.

Groundwork for an interagency initiative was laid in October 2018, but it didn't come to fruition until July 2019 when, after receiving Federal endorsement from the CIOC, CHCOC, and CLOC, representatives from DoD, DHS/CISA, and VA launched the Federal Cyber Career Pathway Initiative (Initiative) and established the Interagency Federal Cyber Career Pathways Working Group (Working Group).

Working Group Purpose

The Working Group comprises cyber workforce development representatives from 21 of 24 Chief Financial Officer (CFO) Act D/As. The Working Group operates with the ultimate intent of collectively developing baseline requirements and career resources, specifically Pathways, for Work Roles within the NICE Framework. Additionally, it seeks to merge disparate workforce related initiatives across Government seeking to accomplish similar and related objectives, while directly supporting:

[5] Cyber Seek, Cybersecurity Supply/Demand Heat Map, https://www.cyberseek.org/heatmap.html

[6] Consolidated Appropriations Act of 2016, Federal Cybersecurity Workforce Assessment Act (FCWAA), https://www.congress.gov/bill/114th-congress/senate-bill/2007/text

- Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*[7]*,* by supporting the growth and sustainment of a workforce skilled in cybersecurity and related fields

- EO 13870[3], *America's Cybersecurity Workforce*[3], by increasing adoption and implementation of the NICE Framework

- EO 13932, *Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates*[8], by identifying core Work Role criteria, education, and certification requirements assessing Federal job applicants applying for cyber positions aligned to Work Roles within the NICE Framework

- The President's Management Agenda (PMA) Cross-Agency Priority (CAP) Goal, *Developing a Workforce for the 21st Century*[9]*,* by improving the ability of employees to design career paths in federal service

- The Chief Information Officer Council's (CIOC), *Future of the Federal IT Workforce Update,* by making federal IT career paths more attractive to the workforce of the future.

Scope

Career Pathways

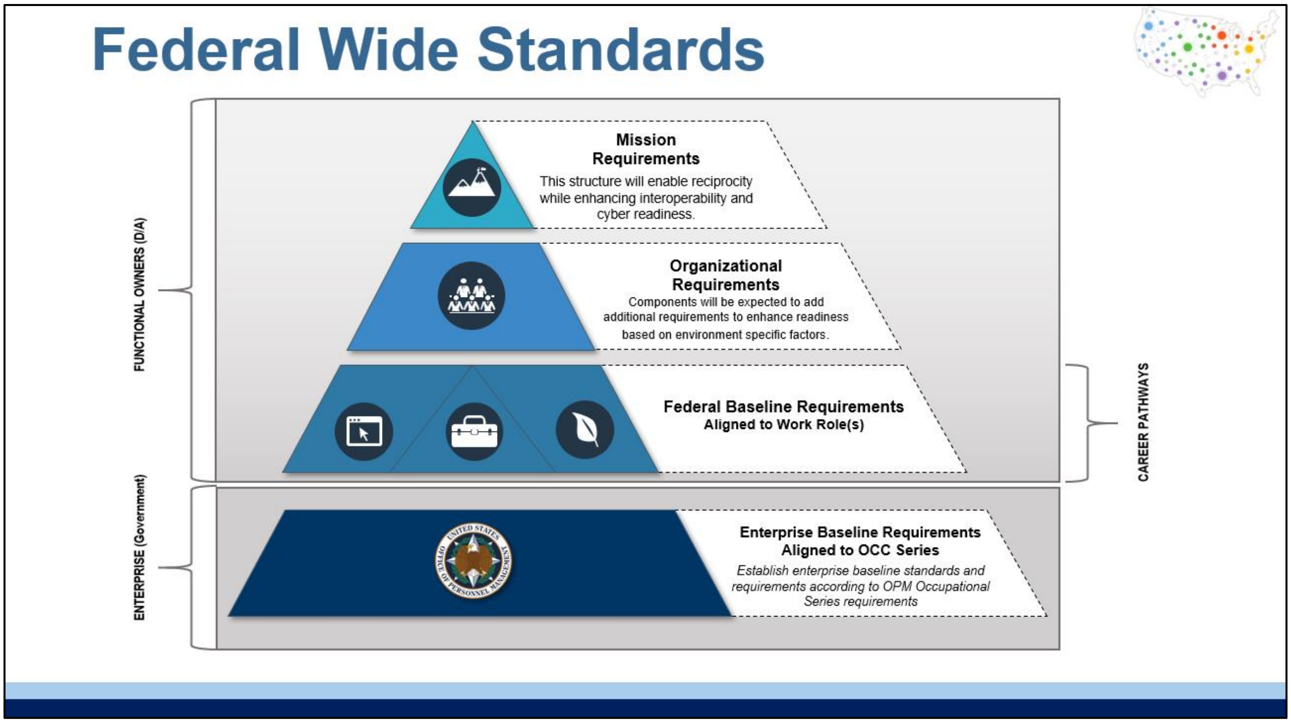
Initiative outputs are completed Pathways for NICE Framework Work Roles most commonly employed by D/As under Title 5 of the United States Code (USC)[10]. 13 Work Roles are frequently, if not entirely, employed by D/As under USC Title 10 (Armed Forces)[10], Title 32 (National Guard) [10], or Title 50 (War and National Defense)[10] and will be the focus of future cyber practitioner Focus Groups. Developed Pathways address foundational attributes about each work role, including occupational series alignment, common Work Role pairings, related functional or position titles, alignment with the General Schedule (GS), career mobility in the form of on and off ramp relationships to complimentary Work Roles, identification of core KSATs and competencies, suggested Work Role-specific education and certifications, and the alignment of individual KSAs to Tasks. The foundational Work Role attributes captured within the Pathways enable the Federal Government to establish baseline requirements, specific to each Work Role, over and above those prescribed by traditional Occupational Series, as depicted in Figure 4 below.

[7] Executive Office of the President, Executive Order 13800, https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[8] Executive Office of the President, Executive Order 13932, https://www.federalregister.gov/documents/2020/07/01/2020-14337/modernizing-and-reforming-the-assessment-and-hiring-of-federal-job-candidates

[9] General Services Administration & the Office of Management and Budget, Developing a Workforce for the 21st Century, https://www.performance.gov/CAP/workforce/

[10] Office of the Law Revision Council, United States Code, https://uscode.house.gov/



Federal Wide Standards

FUNCTIONAL OWNERS (D/A)

Mission Requirements
This structure will enable reciprocity while enhancing interoperability and cyber readiness.

Organizational Requirements
Components will be expected to add additional requirements to enhance readiness based on environment specific factors.

Federal Baseline Requirements
Aligned to Work Role(s)

CAREER PATHWAYS

ENTERPRISE (Government)

Enterprise Baseline Requirements
Aligned to OCC Series
Establish enterprise baseline standards and requirements according to OPM Occupational Series requirements

Figure 4. Federal Wide Work Role Standards

Working Group Effort

The Working Group, comprised of cyber workforce developers and managers from 21 of 24 Chief Financial Officer (CFO) Act D/As and private sector representatives within the American Council for Technology-Industry Advisory Council (ACT-IAC), served as Initiative stewards and cyber workforce ambassadors within Federal D/As. Members had three main responsibilities:

1. Identify D/A cyber practitioner subject matter experts (SMEs) and coordinate their participation in career pathway planning focus groups (focus groups) unique to individual Work Roles.
2. Organize, lead, or assist in Work Role focus groups, assuming the responsibility for coordinating and executing the focus groups, as well as compiling and delivering synthesized feedback in a consolidated document to the Working Group.
3. Verify, validate, and provide input on working group materials including, but not limited to, Charter, developed Pathways, communications, marketing, etc.

Intended Audiences and Applications

This Initiative provides Pathways that can be leveraged by multiple audiences including cyber professionals, their supervisors, human capital professionals, early career and experienced professionals, and academia. These groups will use the Pathways in a number of ways critical to the maintenance and growth of the current and future cyber workforce. The sections that follow identify the intended audiences and outline common applications for each.

Common Applications for Employers

Employers include: supervisors and hiring managers of cyber professionals.

- Establish transparent expectations for direct reports and potential future hires by leveraging Work Role descriptions and KSATs
- Partner with human capital professionals to tailor job announcements with Work Role-specific qualifications to ensure they attract, hire, and retain the most qualified cyber talent needed to maintain and grow their cyber workforce
- Streamline hiring processes by utilizing standardized content and KSATs, thereby enabling consistent and efficient hiring practices across different employers

- Inform employees' learning plans and skills-based assessments so that both employers and employees have a common understanding of development goals
- Participate in effective career conversations with direct reports by utilizing a consistent and structured framework which correlates to improved job satisfaction

Common Applications for Human Capital Professionals

Human capital professionals include: human capital management, talent acquisition, classification, and learning and development.

- Increase knowledge of the cyber workforce in order to recommend development approaches necessary to build a sustainable cyber workforce
- Consistently develop and classify cyber position descriptions by leveraging Work Role language, thereby increasing uniform application across the Federal Government
- Tailor job announcements with Work Role-specific qualifications to ensure they attract and hire the most qualified cyber talent
- Partner with learning and development professionals in identifying skills gaps and build Work Role-specific, customized training to develop the current workforce
- Enable consistent feedback processes based upon standardized Work Role and career growth language derived from the Pathways, ensuring transparency and equity

Common Applications for Early Career Professionals

Early career professionals include: students currently in high school or college, as well as recent cyber graduates.

- Understand the many types of work that makeup the larger cyber workforce and identify Work Roles of particular interest
- Identify specific KSATs as well as unique training and certification requirements for desired Work Roles to prepare for a cyber position within the Federal Government
- Become more familiar with cyber-specific language to facilitate resume development
- Refine and expedite job searches by utilizing the functional titles aligned to desired Work Roles
- Understand career trajectory by identifying natural progression via Work Role on-ramps and off-ramps and how best to transition within the cyber workforce

Common Applications for Experienced Professionals

Experienced professionals include: cyber professionals looking to develop or advance their cyber career, as well as veterans and non-cyber professionals looking to enter the cyber field.

- Understand the many types of work that makeup the larger Cyber Workforce and identify Work Roles of particular interest
- Identify Work Roles that align with professional goals and identify KSATs required to move laterally or advance in their cyber career
- Influence and support the creation of individual development plans (IDPs) by reviewing Work Role qualifications that match their interests, skills, and abilities to achieve a rewarding and challenging career

Common Applications for Academia

Academia includes: educational providers and career counselors, to include educators and instructors from universities, trade schools, and technical schools.

- Develop curricula consistent with the KSATs required of cyber professionals so that students will be able to apply what they learned in the classroom to their future cyber career

- Support students in creating cyber career development plans by reviewing various Work Roles outlined within the Pathways and matching their interests to their own career goals
- Assist current and future members of the cyber workforce in developing and demonstrating the right KSATs to be competitive in the job market by recommending specific courses and other training opportunities aligned to their career journey

Stakeholders

Working Group stakeholders and their respective roles are listed below.

Stakeholders	Interest/Role
Department of Defense (DoD), Department of Homeland Security Cybersecurity Infrastructure Security Agency (DHS CISA), Department of Veterans Affairs (VA)	Tri-Chairs of the Interagency Federal Cyber Career Pathways Initiative. Responsible for obtaining Federal sponsorship for the Initiative; establishing and leading the Working Group; organizing, facilitating, and leading cyber practitioners focus group; and developing and publishing cyber career pathways for Work Roles within the NICE Framework. Deliverables will have a direct impact on existing and anticipated cyber workforce management programs.
Federal Departments and Agencies	Interagency-wide participation will require a significantly less level of effort to accomplish the common goal of developing cyber career pathways. Products will inform D/A cyber workforce program plans as well as improve capacity and capability.
Administration	The Initiative will lend to accomplishing multiple efforts such as those under the National Cyber Strategy, the President's Management Agenda Cross-Agency Priority Goal, EO 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, EO 13870[3] on America's Cybersecurity Workforce, EO 13932 on Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates, the Federal Cybersecurity Workforce Assessment Act, as well as other or subsequent policies and/or directives. This Initiative connects multiple working efforts to ensure a common, structured approach to developing Federal baseline requirements.
Office of Personnel Management	The output will leverage and support the need for aggregate Federal wide cyber coding data, as well as inform aspects of OPM Federal-wide cyber workforce management activities including cyber competency models and the development or refinement of interpretative guidance for cyber positions.
Work Role Practitioners	Federal cyber practitioners have a vested interest in participating in the gathering of information and development of cyber career pathways to ensure consensus and inclusion of diverse perspectives. Developed pathways may inform future expectations of their role and their ability to move and progress in their career.
Federal Chief Information Officer's Council	Initiative directly supports the CIO council priorities through "identifying, hiring, and empowering the best possible people in federal IT," and the CIOC Workforce Committee's Strategic Focus Area dedicated to developing Strategic Career Roadmaps.

Stakeholders	Interest/Role
Federal Chief Human Capital Officer's Council	Cyber Career Pathways will inform and influence human capital management strategies focused on attracting, developing and retaining a high performing, engaged and diverse Federal cyber workforce.
Federal Chief Learning Officer Council	The Framework will serve as a best practice that will inform learning and development opportunities across the Federal Government by identifying baseline education and certifications, core technical competencies, aligning Work Role Tasks to their respective Knowledge, Skills, and Abilities, and developing Learning Objectives that can inform the development of Work Role curricula.

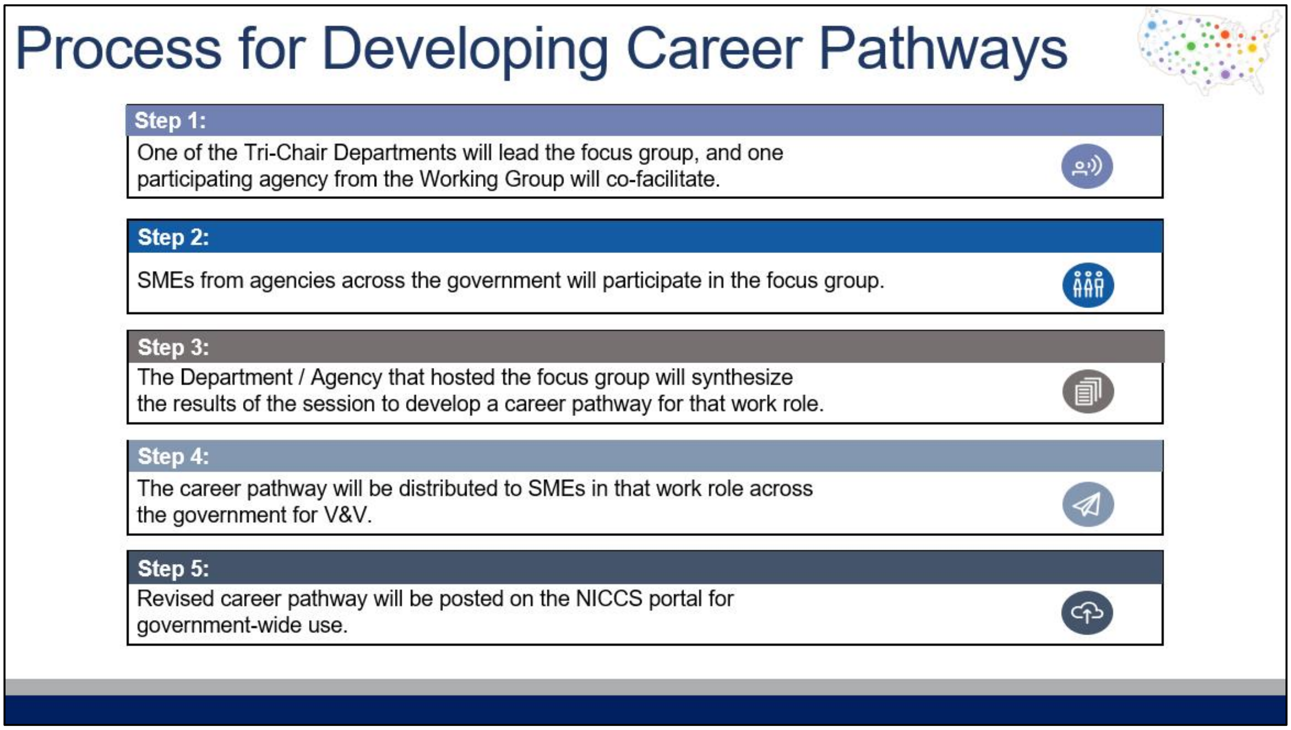
Table 1. Working Group Stakeholders

Pathways Development Process and Methodology

The following section details the process and methodology Working Group representatives followed to organize, lead, develop, verify and validate, and produce Pathways.

Process

Key to developing Pathways for NICE Framework Work Roles was establishing a defined process for collecting, synthesizing, and validating input that could be easily repeated by the Working Group. Equally important was building a process which leveraged cyber practitioner talent across the Federal Government in order to provide the widest range of perspectives. While input from practitioners led to the development of draft Pathways, they did not become final until verification and validation was obtained from the Working Group and their respective cyber workforces. This ensured that developed pathways represented the collective interests of the Interagency and could serve as the Federal Government baseline. Figure 5 outlines the specific steps the Working Group followed to schedule, source, host, develop, validate, and publish each Pathway.



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.

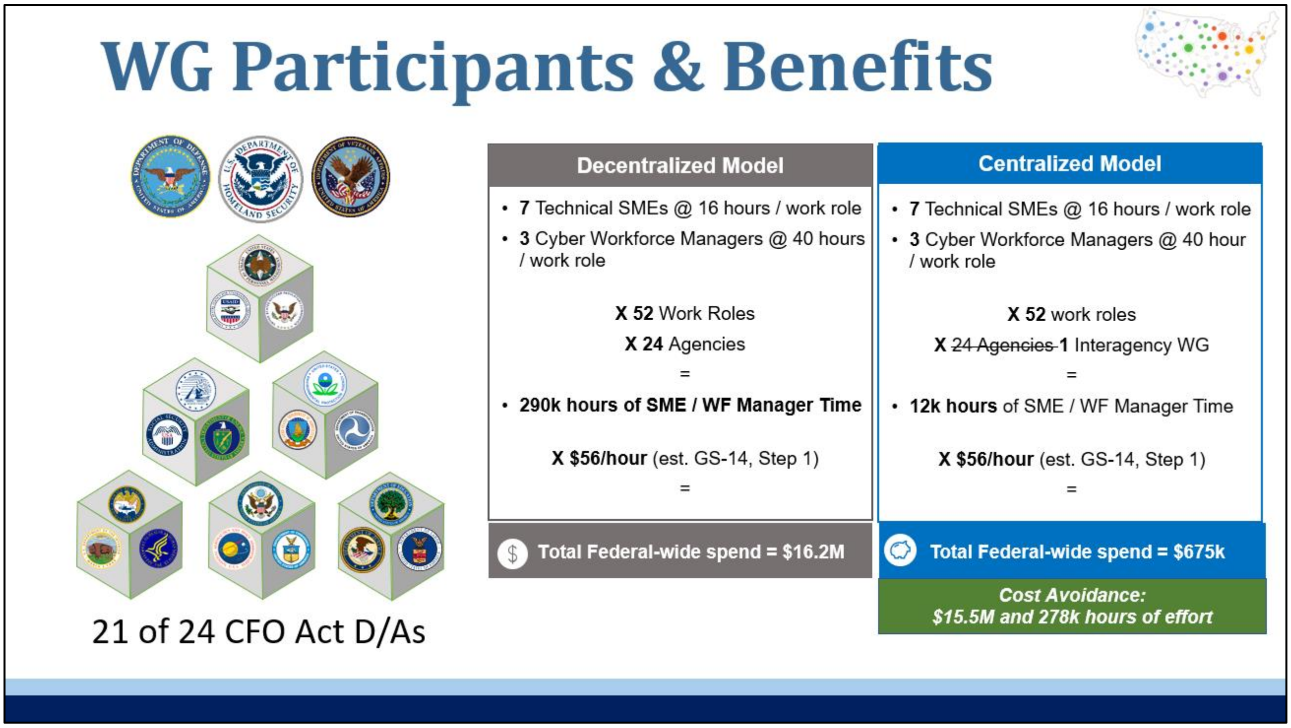
Step 3:
The Department / Agency that hosted the focus group will synthesize the results of the session to develop a career pathway for that work role.

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.

Figure 5. Career Pathways Development Process

Leveraging practitioners across the Federal Government within each focus group was strategic and intentional. By guiding practitioners with varying perspectives and experience through defined and repeatable exercises, the Working Group was able to synthesize practitioner's varied input into a singular Pathway. Achieving Interagency consensus meant the Federal Government was developing products with a cohesive voice while avoiding the duplication of time and resources. Figure 6 highlights the estimated cost avoidance achieved by conducting focus groups and achieving outcomes together instead of independently.



WG Participants & Benefits

21 of 24 CFO Act D/As

Decentralized Model

- **7** Technical SMEs @ 16 hours / work role
- **3** Cyber Workforce Managers @ 40 hours / work role

X 52 Work Roles

X 24 Agencies

=

- **290k hours of SME / WF Manager Time**

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

=

$ **Total Federal-wide spend = $16.2M**

Centralized Model

- **7** Technical SMEs @ 16 hours / work role
- **3** Cyber Workforce Managers @ 40 hour / work role

X 52 work roles

X ~~24 Agencies~~ **1** Interagency WG

=

- **12k hours** of SME / WF Manager Time

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

=

Total Federal-wide spend = $675k

Cost Avoidance:
$15.5M and 278k hours of effort

Figure 6. Estimated Initiative Cost Avoidance through Interagency Collaboration

Methodology

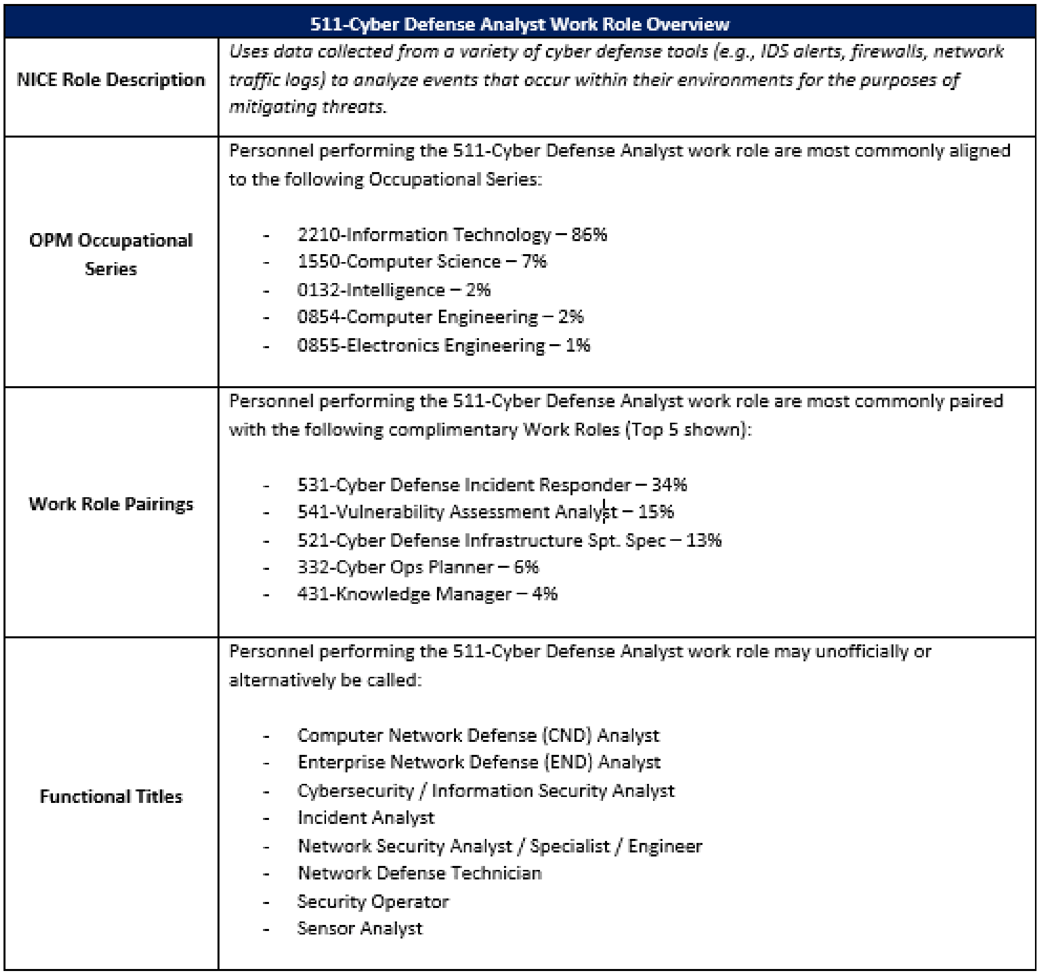
Focus groups were held for each Work Role. Focus group participants consisted of cyber practitioners from across the Federal Government currently occupying positions aligned to, or with prior experience performing, the Work Role being discussed. Leveraging publicly available cyber workforce resources, as well as Working Group developed tools, Working Group representatives led practitioners through structured exercises designed to prompt discussion and elicit insight into the Work Role being discussed. In each session, facilitators provided an overview of the Initiative and Pathways goals and, subsequently, garnered feedback from the group by conducting the following exercises:

1. Work Role Overview
2. Career Progression and Mobility
3. Suggested Qualifications
4. Task Development and KSA Mapping
    a. Behavioral Indicator Development
    b. KSA Mapping

The high-level steps conducted to complete each of these exercises are outlined in the following sections.

Work Role Overview

The Work Role Overview exercise is designed to capture foundational attributes about a Work Role. It provided practitioners an opportunity to weigh in on how the Work Role is described within the NICE Framework and whether that description captures the full intent of the Work Role in a way that's easy to understand. This exercise paved the way for how the Work Role would be understood throughout the Focus Group and, more importantly, how key attributes like related Work Roles, related functional and position titles, and alignment to Occupational Series and GS would be captured, validated, and displayed within completed Pathways documents.

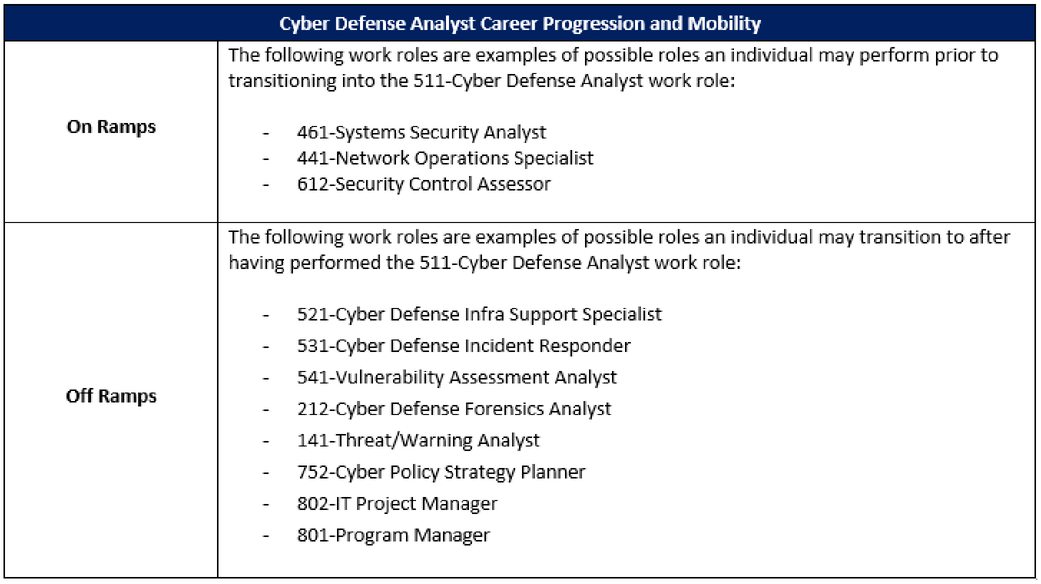


511-Cyber Defense Analyst Work Role Overview	
NICE Role Description	*Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.*
OPM Occupational Series	Personnel performing the 511-Cyber Defense Analyst work role are most commonly aligned to the following Occupational Series: - 2210-Information Technology – 86% - 1550-Computer Science – 7% - 0132-Intelligence – 2% - 0854-Computer Engineering – 2% - 0855-Electronics Engineering – 1%
Work Role Pairings	Personnel performing the 511-Cyber Defense Analyst work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 531-Cyber Defense Incident Responder – 34% - 541-Vulnerability Assessment Analyst – 15% - 521-Cyber Defense Infrastructure Spt. Spec – 13% - 332-Cyber Ops Planner – 6% - 431-Knowledge Manager – 4%
Functional Titles	Personnel performing the 511-Cyber Defense Analyst work role may unofficially or alternatively be called: - Computer Network Defense (CND) Analyst - Enterprise Network Defense (END) Analyst - Cybersecurity / Information Security Analyst - Incident Analyst - Network Security Analyst / Specialist / Engineer - Network Defense Technician - Security Operator - Sensor Analyst

Figure 7. Work Role Overview Example

Career Progression and Mobility

Work Roles naturally share connections with one another based on overlapping KSATs, alignment within the same Skills Community, or due to the nature of their specialization and function within the larger cyber workforce. The intent of the Career Progression and Mobility exercise was for practitioners to identify the natural or logical Work Roles individuals may perform prior to and following the Work Role being discussed, in other words, the on ramps and off ramps. On ramps and off ramp Work Roles can be viewed as potential stepping stones one may use, but is not limited to, when charting a unique cyber career journey.



Cyber Defense Analyst Career Progression and Mobility	
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 511-Cyber Defense Analyst work role: - 461-Systems Security Analyst - 441-Network Operations Specialist - 612-Security Control Assessor
Off Ramps	The following work roles are examples of possible roles an individual may transition to after having performed the 511-Cyber Defense Analyst work role: - 521-Cyber Defense Infra Support Specialist - 531-Cyber Defense Incident Responder - 541-Vulnerability Assessment Analyst - 212-Cyber Defense Forensics Analyst - 141-Threat/Warning Analyst - 752-Cyber Policy Strategy Planner - 802-IT Project Manager - 801-Program Manager

Figure 8. Work Role Career Progression and Mobility Example

Suggested Qualifications

There are unique education, training, and certification requirements for each Work Role. The Suggested Qualifications exercise sought practitioner input regarding the certifications and environment specific requirements that have enabled the practitioner to further their understanding of, or performance within, the Work Role being discussed. The input obtained from Federal practitioners will inform future third party assessments of certification content to core Work Role KSATs. Through strategic partnership with DoD, Pathways will incorporate, via an external link, qualification requirements aligned to the future iteration of DoD's *Cyberspace Management Program, DoD Directive 8140*[11]*.* While required for DoD cyber personnel, Work Role-specific education and certifications will be presented as suggested ways by which individuals can qualify for Federal cyber positions aligned to NICE Framework Work Roles.

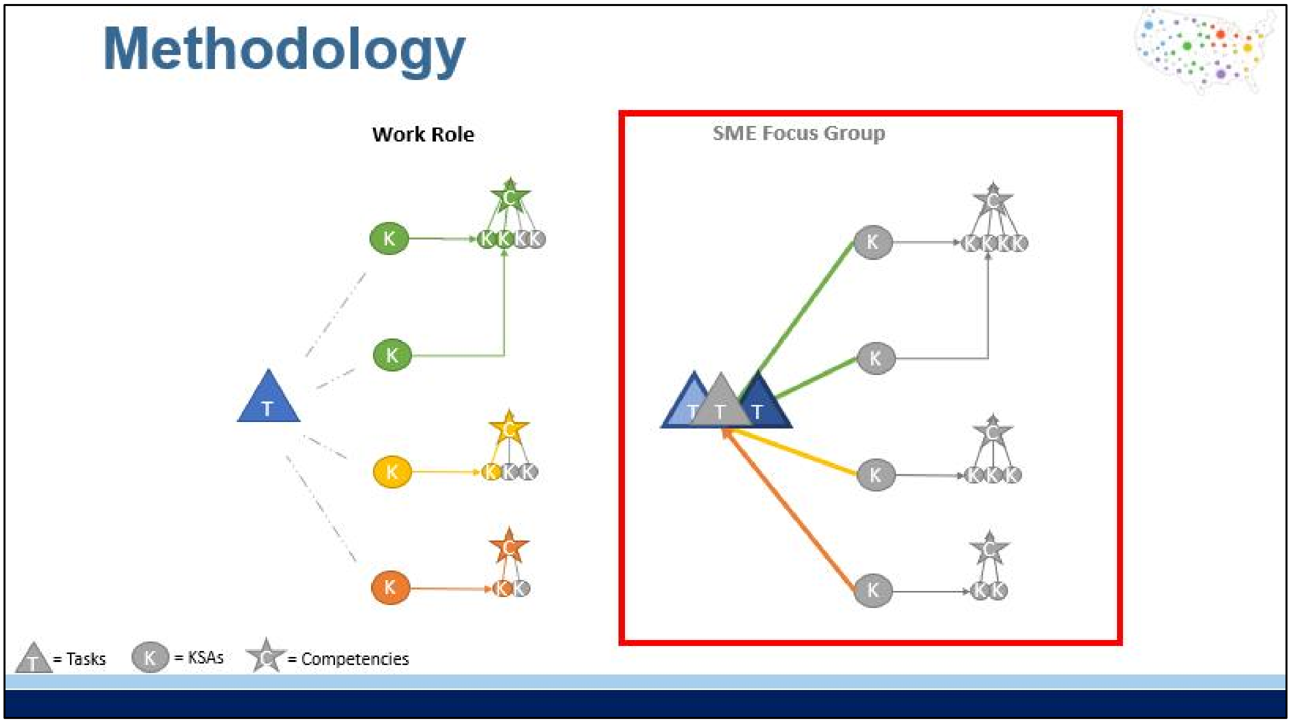
Task Development and KSA Mapping

The NICE Framework associates specific Tasks and KSAs with each Work Role. Also available is a proposed alignment of individual KSAs to larger Competency Areas. However, early into this Initiative the Working Group identified a gap within the NICE Framework, as depicted in. While the NICE Framework makes clear the need for KSAs to perform Work Role Tasks, it does not include a mapping of individual Knowledge, Skill, or Ability statements to the specific Tasks they support. Furthermore, Tasks are written at a singular proficiency level and do not offer example or suggested variations for performance at various proficiency levels.

As depicted in Figure 7 below, the Task Development and KSA Mapping exercise was specifically designed to bridge these identified gaps by:

1. Identifying Core KSATs for the Work Role.
2. Developing and assigning Task permutations, or Behavioral Indicators, derived from Tasks within the Work Role, across entry, intermediate, and advanced Proficiency Levels; and
3. Mapping individual KSAs to the specific core Tasks they most readily support.
    a. Aggregating practitioner's Task-to-KSA mappings enabled the identification of Competency Areas that directly support Work Role core Tasks.

[11] Department of Defense, Cyberspace Workforce Management Program, Directive 8140.01, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf?ver=2019-06-06-120639-863



Methodology

Figure 7. Connecting KSAs to Tasks and Developing Behavioral Indicators

Verification and Validation (V&V)

Once a Pathways document was fully assembled, it was sent out to the Focus Group practitioners for verification and validation (V&V). Once all of the comments from the practitioners were adjudicated, the completed Pathways document was sent to all members of the Working Group for a final V&V. This process ensured that input was solicited and obtained from as subject matter experts and perspectives as possible in order to achieve Interagency consensus.

Outcome

The release of the NICE Framework and Work Roles paved the way for the government, industry, academia, and the public to engage in a conversation, using a single language, to collectively understand cyber and the types of roles and work that professionals within this domain perform. Pathways are a continuation of that dialogue, with a focus on the tangible application of that collective understanding. Through the efforts of this Initiative and Working Group, the Federal Government will have access to a standardized set of Pathways that can be utilized by various audiences and, from a human capital standpoint, support all stages of the employee lifecycle as depicted in Figure 8. Pathways leverage years of criticality analyses, focus groups with hundreds of federal cyber practitioners, and aggregate Federal Government cyber coding data to expand the collective understanding of cyber Work Roles and in turn, support the growth of the current and future cyber workforce. Additionally, Pathways provide the foundation from which new career resources and tools can be developed to further promote the collective understanding of Cyber and application of Work Roles.

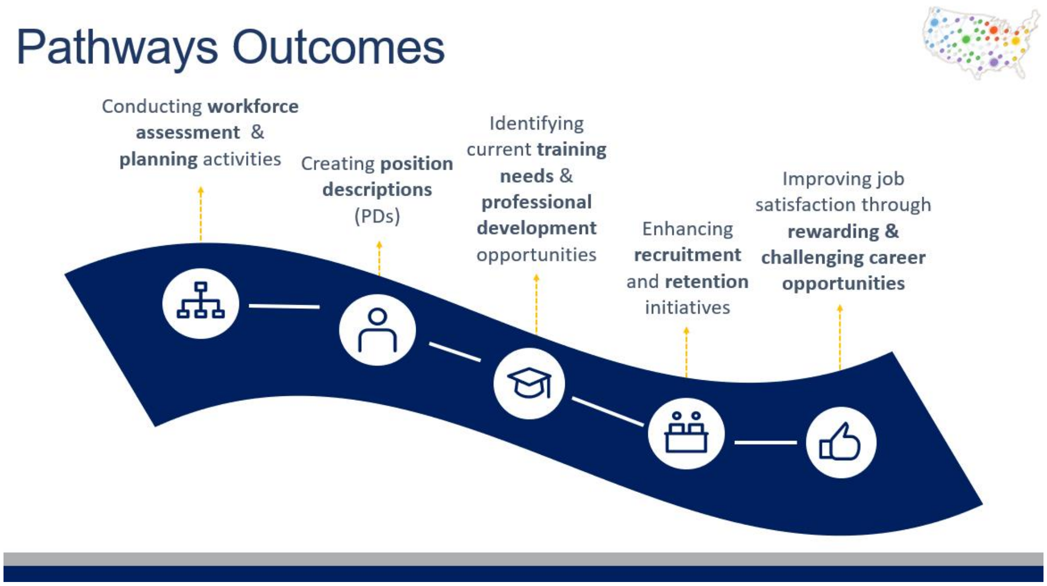

Pathways Outcomes
Conducting workforce assessment & planning activities
Creating position descriptions (PDs)
Identifying current training needs & professional development opportunities
Enhancing recruitment and retention initiatives
Improving job satisfaction through rewarding & challenging career opportunities

Figure 9. Pathways Outcomes

From the outset of this Initiative, the Working Group envisioned leveraging the input gained from cyber practitioners to inform the development of an interactive and engaging tool that not only presents a refreshed way of navigating the NICE Framework, but also provides actionable data to meet the needs of students and recent graduates, professionals, managers, and human capital specialists working within or interested in joining the cyber workforce. Through a strategic partnership with DHS/CISA's Cybersecurity Defense Education and Training (CDET) team, the Working Group was able to bring that vision to life with the release of the Cyber Career Pathways Tool[12], available on the National Initiative for Cybersecurity Careers and Studies (NICCS). This tool aids individuals with identifying, building, and navigating a potential career in Cyber by increasing understanding of the knowledge, skills, and abilities needed to begin, transition, or advance a cyber career. Additionally, this tool and the Pathways that underpin it, enable D/As to develop targeted cyber workforce strategies and capabilities that support cyber professionals, their supervisors, and human capital professionals.

The Working Group, Pathways, and their byproducts serve as a testament to the outcomes that can be achieved through collaboration and shared vision. While Pathways are not intended to serve as the 100% solution for any one D/A, they do represent a collective baseline, or foundation. Together, the Federal Government can build upon this shared foundation as it seeks to develop the cyber workforce it needs, both now and in the future.

[12] National Initiative for Cybersecurity Careers and Studies, Cyber Career Pathways Tool, https://niccs.us-cert.gov/workforce-development/cyber-career-pathways

Appendix A: Accessing Completed Federal Cyber Career Pathways

To date, the Working Group has developed Pathways for work roles listed in Table 2. Pathways are publicly available on the DoD Cyber Exchange website at: https://public.cyber.mil/cw/pathways.

Work Role	OPM Code	Cyber Community
Authorizing Official/Designating Representative	**611**	Cybersecurity
Security Control Assessor	**612**	Cybersecurity
Secure Software Assessor	**622**	Cybersecurity
Security Architect	**652**	Cybersecurity
Information Systems Security Developer	**631**	Cybersecurity
Systems Security Analyst	**461**	Cybersecurity
Information Systems Security Manager	**722**	Cybersecurity
Communications Security (COMSEC) Manager	**723**	Cybersecurity
Cyber Defense Analyst	**511**	Cybersecurity
Cyber Defense Infrastructure Support Specialist	**521**	Cybersecurity
Cyber Defense Incident Responder	**531**	Cybersecurity
Vulnerability Assessment Analyst	**541**	Cybersecurity
Cyber Defense Forensics Analyst	**212**	Cybersecurity
Software Developer	**621**	IT
Enterprise Architect	**651**	IT
Research & Development Specialist	**661**	IT
Systems Requirements Planner	**641**	IT
System Testing and Evaluation Specialist	**671**	IT
Systems Developer	**632**	IT
Database Administrator	**421**	IT
Data Analyst	**422**	IT
Knowledge Manager	**431**	IT
Technical Support Specialist	**411**	IT
Network Operations Specialist	**441**	IT
System Administrator	**451**	IT
Cyber Legal Advisor	**731**	Legal/Law Enforcement
Cyber Crime Investigator	**221**	Legal/Law Enforcement
Law Enforcement /Counterintelligence Forensics Analyst	**211**	Legal/Law Enforcement
Program Manager	**801**	Lifecycle Management
IT Project Manager	**802**	Lifecycle Management
Product Support Manager	**803**	Lifecycle Management
IT Investment/Portfolio Manager	**804**	Lifecycle Management
IT Program Auditor	**805**	Lifecycle Management
Privacy Officer/Privacy Compliance Manager	**732**	Strategic Management
Cyber Policy and Strategy Planner	**752**	Strategic Management
Executive Cyber Leadership	**901**	Strategic Management
Cyber Instructional Curriculum Developer	**711**	Talent Management
Cyber Instructor	**712**	Talent Management
Cyber Workforce Developer and Manager	**751**	Talent Management

Table 2. Completed Work Roles