

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

The background of the slide is a photograph of the United States Capitol building in Washington, D.C. The building is a large, white, neoclassical structure with a prominent central dome. The sky is blue with scattered white clouds. The text is overlaid on the top half of the image.

Welcome

June 23, 2020

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



Rodney Petersen

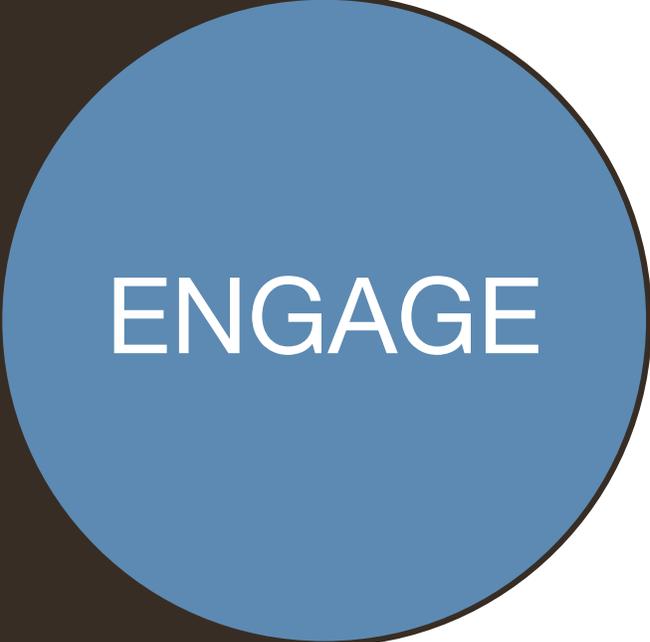
Director

National Initiative for Cybersecurity Education



Mission of NICE

To energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.



ENGAGE

- NICE Interagency Coordinating Council
- NICE Working Group and Subgroups
 - Apprenticeships
 - Collegiate
 - Competitions
 - K12
 - Training and Certifications
 - Workforce Management



EVENTS

NICE Webinar Series

nist.gov/nice/webinars

NICE Conference and Expo

November 16-18, 2020 | Atlanta, Georgia

NICEconference.org

NICE K12 Cybersecurity Education Conference

December 7-8, 2020 | St. Louis, Missouri

K12cybersecurityconference.org



fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Register Today for the FISSEA Summer Series 2020

July 20, 2020, 1:00-2:30 pm

“CyberRap, Music, Dance, Gamification, and Fun in Cybersecurity Training”

Featuring: Preparing for National Cyber Security Awareness Month
presented by the National Cyber Security Alliance

August 24, 2020, 1:00-2:30 pm

*“Adaptive Learning: Utilizing AI and Social Collaboration
for User-Centric Training Results”*

Featuring: Presentation of the FISSEA Security Awareness and
Training Contest Winners

September 21, 2020, 1:00-2:30 pm

Topic to be announced

Visit: <https://csrc.nist.gov/Projects/fissea/2020-summer-series>

Welcome from Veronica Villalobos, OPM

- Federal Cybersecurity Workforce Community
 - Committed to building, maintaining a robust cybersecurity workforce
 - Driven by collaboration, passion, creativity
 - Sustained by member involvement in work groups that produce ideas, solutions, resources
 - Highest-level policy groups
 - NICE work groups
 - Grass-roots, issue-focused groups
 - Cyber PD/JOA Interagency Team
 - Cyber Career Pathways Interagency Workgroup
 - Email us for information on how to participate: CyberHRStrategy@opm.gov



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Opening Remarks

Walter G. Copan

*Under Secretary of Commerce for Standards and Technology
and NIST Director*

Chief Human Capital Officers Council (CHCOC)

Dr. John York

Senior Advisor for Policy & the CHCO Council

June 23, 2020



ABOUT THE CHCO COUNCIL

- The Chief Human Capital Officers Council serves the nation by advising and collaborating with the U.S. Office of Personnel Management and other stakeholders to create human capital management strategies that attract, develop and retain a high performing, engaged and diverse federal workforce.
- The Chief Human Capital Officers Act of 2002, enacted as part of the Homeland Security Act of 2002 (Pub. L. No. 107-296) on November 25, 2002, required the heads of 24 Executive Departments and agencies to appoint or designate Chief Human Capital Officers (CHCOs).
- Each CHCO serves as his or her agency's chief policy advisor on all human resources management issues and is charged with selecting, developing, training, and managing a high-quality, productive workforce.





Chief Information Officers Council (CIO Council) Workforce Committee

June 23, 2020



Workforce Committee

- The **Workforce Committee** operates under the authority of the **Chief Information Officers Council (CIOOC)**.
- The purpose is to work in partnership with the Human Resources (HR) community to develop, implement, and communicate strategies to recruit and manage a fully trained and qualified IT workforce to meet and future mission requirements.



Current Initiatives

- Women in Federal IT & Cyber Events
 - Series of virtual engagements throughout the summer 2020 (www.cio.gov)
- The Future of the IT Workforce Report
 - Public version is available at www.cio.gov
- The Cyber Orientation
 - Fall 2020



For Information

- For initiatives, news and volunteer opportunities visit www.cio.gov
- **Questions:** feedback@cio.gov
- Join our CIO Community listserv by sending email to feedback@cio.gov

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

The background of the slide is a photograph of the United States Capitol building in Washington, D.C. The building is white with a prominent central dome and is set against a bright blue sky with scattered white clouds. The image is slightly faded to allow the text to be clearly visible.

Opening Remarks

Michael J. Rigas

Acting Director, Office of Personnel Management

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Updates to the NICE Framework

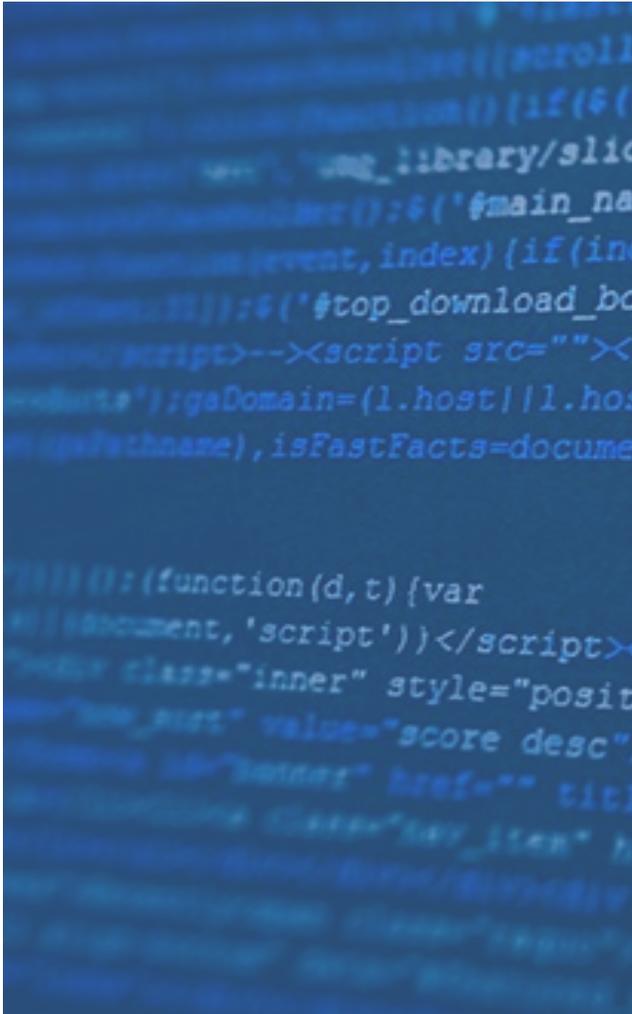
*Bill Newhouse, Matt Isnor, Lisa Dorr, Kenneth
Vrooman, Pam Frugoli*

Matthew Isnor

Senior Program Lead
Cyber Workforce Development
Department of Defense, OCIO



DoD Cyberspace Workforce Framework (DCWF)



Trends & Key Challenges



Inconsistent Lexicon

While strides have been made, the language used to discuss cyber work and skill requirements is inconsistent. This hinders the Nation's ability to assess capabilities, identify skill gaps, and prepare the pipeline of future cyber talent.



Disjointed Professional Development

There is a lack of clearly defined roles and career paths for cyber work. Efforts to establish accreditation standards for cyber curricula and certifications have been inconsistent.



Lack of Cybersecurity Professionals

A report by the *Partnership for Public Service* state, "There is a nationwide shortage of highly qualified cybersecurity experts, and the government has fallen behind in the race for this talent."



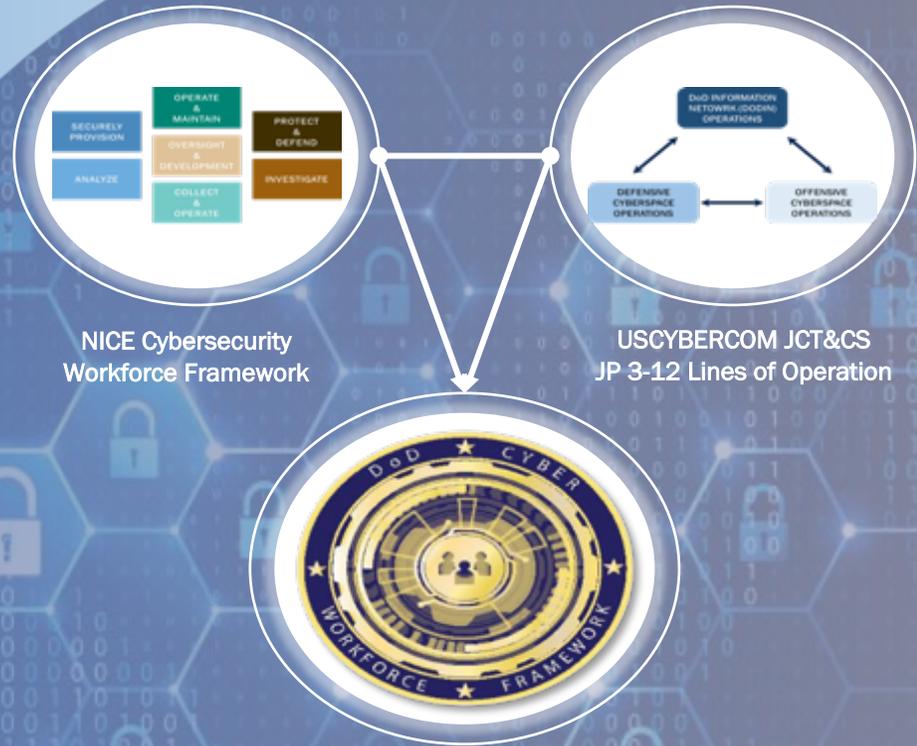
Cybersecurity Viewed as Separate Function

A report by the *Partnership for Public Service* state, "There is a nationwide shortage of highly qualified cybersecurity experts, and the government has fallen behind in the race for this talent."

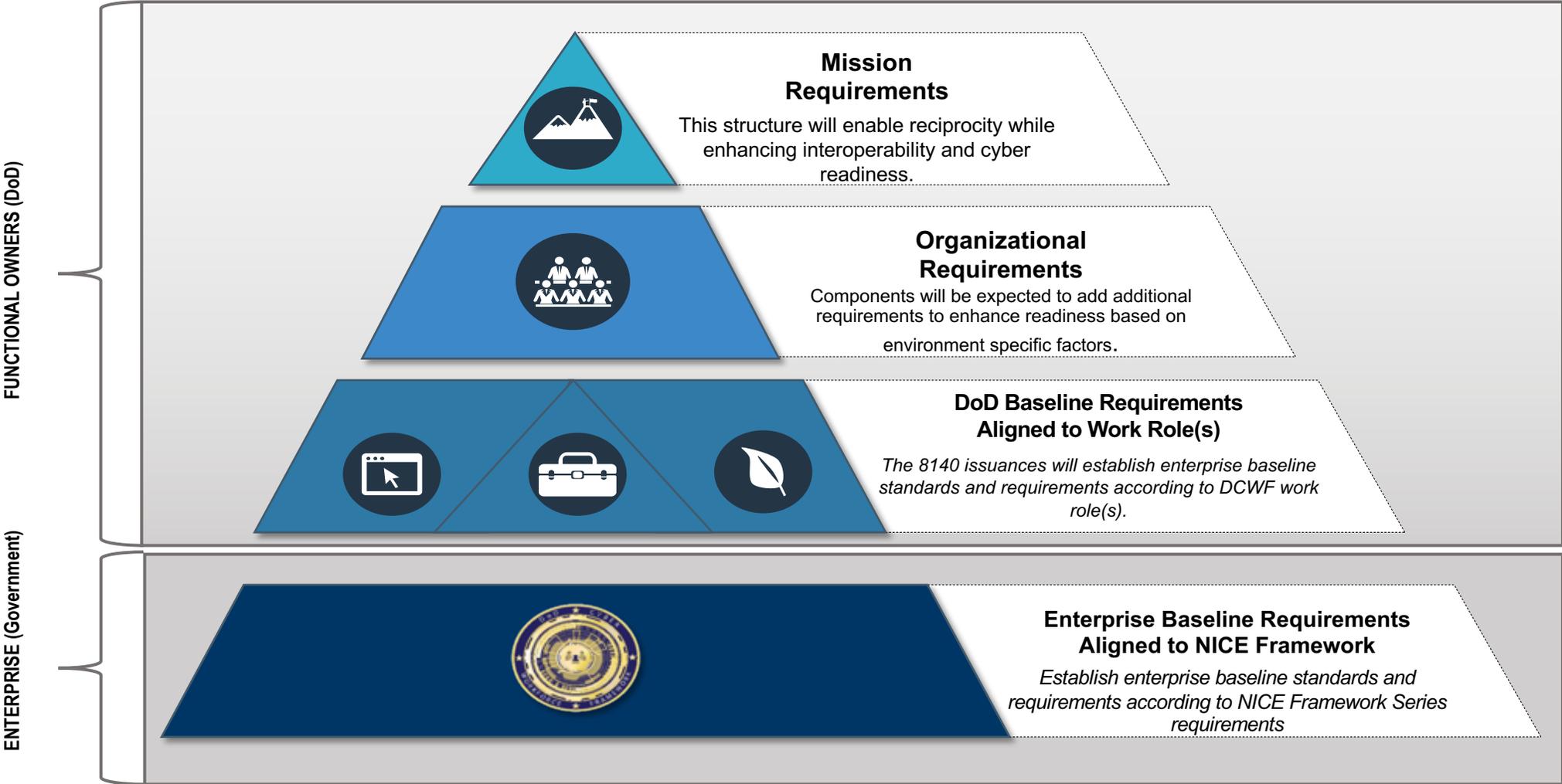


DoD Cyberspace Workforce Framework (DCWF)

- Establishes an authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator
- Develops qualification requirements for cyber work roles outlined in DoD Manual 8140.XX
- Facilitates uniform identification, tracking, and reporting required by the Federal Cybersecurity Workforce Assessment Act (FCWAA)
- The DCWF has been adapted at the national level in NIST Special Publication 800-181
- Used to develop an international framework under the NATO Multinational Cyber Defense Training & Education Project.



DoD Cyberspace Workforce Framework (DCWF)



Lisa Dorr, Senior Talent Manager



**Department of Homeland Security Office
of the Chief Human Capital Officer**

- Cybersecurity and Intelligence Talent Experience (CITE) Division
- Cybersecurity Talent Management System (CTMS) Innovations Team
- Senior Talent Manager for Strategic Analysis & Change Management and Talent Engagement & Development



DHS Cybersecurity Talent Management System

Background

Congress granted the Secretary broad authority to establish an alternative personnel system to recruit and retain cybersecurity talent

- Passed as part of the December 2014 Border Patrol Agent Pay Reform Act
- Broad authority with some restrictions and requirements, including producing regulation
- Similar language to authorities for personnel systems in Department of Defense and Intelligence Community

Challenge

Simply eliminating a step in the hiring process or adding a pay grade will not make DHS competitive, especially given the global shortage for cybersecurity talent

- Department's cybersecurity human capital challenges are about more than just pay
- The world of work—especially cybersecurity work—continues to evolve
- Conventional civil service approaches, including position-based hiring and pay, are showing their age

Solution

DHS is preparing to launch the CTMS and Cybersecurity Service (DHS-CS) to better manage cybersecurity talent in the 21st century

- Modernize talent management to align to and keep pace with cybersecurity work
- Take a comprehensive, mission-focused approach to recruit and retain talent
- Understand and customize leading private and public sector practices for DHS

Methodology

Sourced input from key DHS cybersecurity and human capital stakeholders

+

Reviewed all major federal personnel transformations since the 1970s

+

Benchmarked leading private sector practices, including those for hiring assessment and compensation

+

Engaged with human capital experts from the Office of Personnel Management and the Intelligence Community



DHS Cybersecurity Talent Management System

Workforce Trends

- 1 Government work is increasingly knowledge work, requiring complex problem-solving and unpredictable application of skills
- 2 Jobs are becoming increasingly non-standard and complex
- 3 Employee expectations no longer always map to the 30-year federal career
- 4 Highly-competitive labor markets exist in which the Federal Government is only one employer

Practices to Revisit

- 1 Position classification from the first half of the 20th century cannot describe cybersecurity work or talent
- 2 Self-rating and brief interviews cannot measure cybersecurity expertise
- 3 Rigid, tenure-based approaches to pay and career progression are not competitive



Ken Vrooman, Senior Advisor



Cybersecurity and Infrastructure Security Agency

- Cyber Defense Education and Training sub-division
- Acting Branch Chief for the Curriculum, Evaluation and Support Branch



CYBERSECURITY DEFENSE EDUCATION & TRAINING (CDET)



Cybersecurity Defense Education & Training

- As the Nation's Risk Advisor, CISA leads the effort to ensure there is an appropriate staffing of cybersecurity professionals to address the increasing demand of protecting the government, critical infrastructures, SLTT, and public/private partners.
- To accomplish this, CISA is standing up the Cyber Defense Education & Training (CDET) Subdivision to consolidate and expand the agency's ability to address this workforce shortage crisis.

CDET Mission

Educating the Nation to Address Cybersecurity Challenges

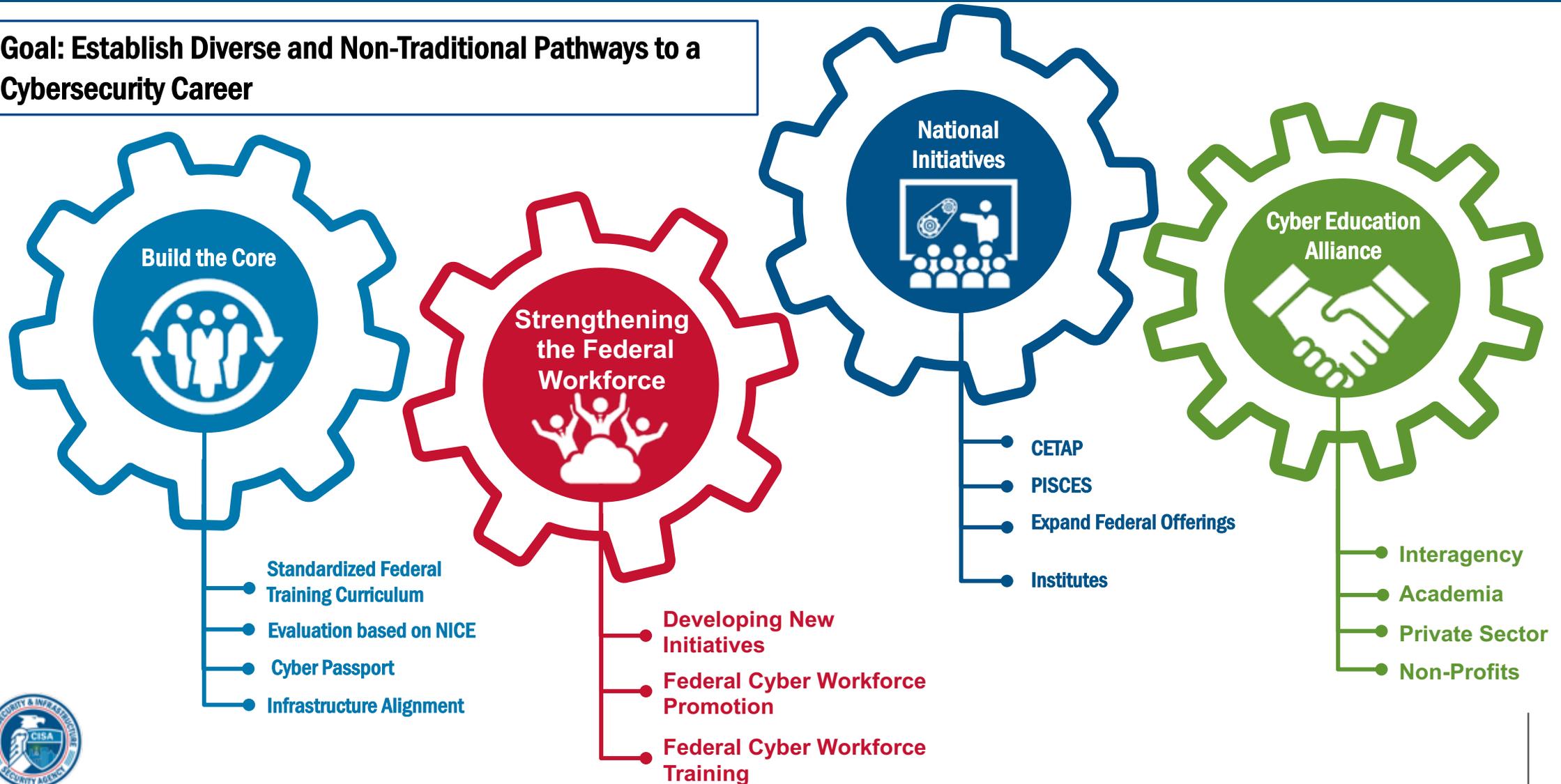
CDET Vision

Sustain an Adaptive Cybersecurity Workforce as a National Asset

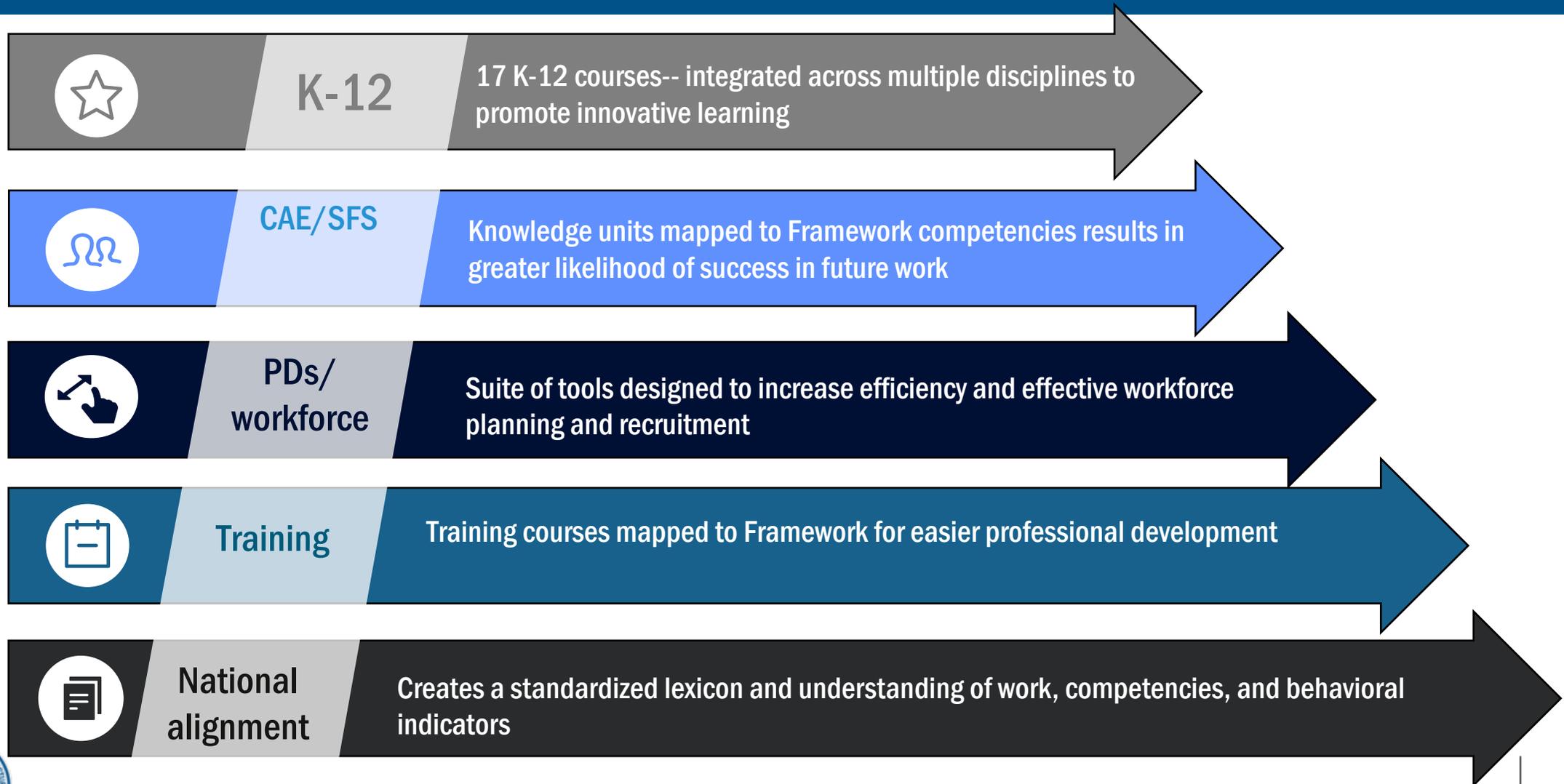


Building the Pipeline

- **Goal: Establish Diverse and Non-Traditional Pathways to a Cybersecurity Career**



NICE Framework is the Core





For more information:
www.cisa.gov

Questions?
Email: education@cisa.dhs.gov

Pam Frugoli

Senior Workforce Analyst
Employment and Training Administration
U.S. Department of Labor



Employment and Training Administration Department of Labor

- Help to disseminate the valuable information about cybersecurity careers to a wider audience
 - ETA-sponsored public career information websites receive an average of 7 million visits per month
- Help promote cybersecurity as a training and career option to customers of the public workforce system
 - ETA grants to states and other partners
 - 2,400 local American Job Centers



O*NET OnLine and MyNextMove

O*NET OnLine

Occupation Quick Search:

Help Find Occupations Advanced Search Crosswalks Share O*NET Sites

Build your future with O*NET OnLine.

Welcome to your tool for career exploration and job analysis!

O*NET OnLine has detailed descriptions of the world of work for use by job seekers, workforce development and HR professionals, students, researchers, and more!

[What is O*NET?](#)

What's New?

Updated BLS information included in O*NET websites

[Learn More](#)

Get O*NET news by [email](#) or [RSS](#).

I want to be a...

Start the career you've dreamed about, or find one you never imagined.

[Find It Now at My Next Move](#)

ATTN: VETERANS

Put your military skills and experience to work in civilian life. Learn how at:

MY NEXT MOVE FOR VETERANS

[Get Started](#)

Hot Technologies are frequently included in employer job postings.

Occupation Search Keyword or O*NET-SOC Code:

Find Occupations Browse groups of similar occupations to explore careers. Choose from industry, field of work, science area, and more.

Advanced Search Focus on occupations that use a specific tool or software. Explore occupations that need your skills.

Crosswalks Connect to a wealth of O*NET data. Enter a code or title from another classification to find the related O*NET-SOC occupation.

Bright Outlook Browse by O*NET Data: Military

MY NEXT MOVE

What do you want to do for a living?

"I want to be a ..."

Search careers with key words.

Describe your dream career in a few words:

Examples: doctor, build houses

[Search](#)

"I'll know it when I see it."

Browse careers by industry.

There are over 900 career options for you to look at. Find yours in one of these industries:

Administration & Support Services

[Browse](#)

"I'm not really sure."

Tell us what you like to do.

Answer questions about the type of work you might enjoy. We'll suggest careers that match your interests and training.

[Start](#)

Still not sure? Check out careers in these groups:

[Bright Outlook](#) [Interests](#) [Job Prep](#)

Are you a veteran looking for work?
[My Next Move for Veterans](#) helps you find a civilian career similar to your military job.

¿Hable español?
[Mi Próximo Paso](#) incluye tareas, aptitudes, información sobre salarios y más de 900 carreras diferentes.

FIND THE APPRENTICESHIP THAT'S RIGHT FOR YOU [APPRENTICESHIP.GOV](#)

Help Explore Careers O*NET Sites

Was this page helpful? [Job Seeker Help](#) [Contact Us](#)

Share: [Facebook](#) [Twitter](#) [LinkedIn](#) [Email](#)

Link to Us [Cite this Page](#)

Follow us: [Facebook](#) [Twitter](#) [LinkedIn](#) [Email](#)

[About this Site](#) [Privacy](#) [Disclaimer](#)

Site updated May 19, 2020

My Next Move is sponsored by the U.S. Department of Labor, Employment & Training Administration, and developed by the National Center for O*NET Development.



O*NET Profile for Information Security Analysts



Help Find Occupations Advanced Search Crosswalks Share O*NET Sites

Summary Report for: 15-1122.00 - Information Security Analysts

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

Sample of reported job titles: Data Security Administrator, Information Security Officer, Information Security Specialist, Information Systems Security Analyst, Information Systems Security Officer, Information Technology Security Analyst (IT Security Analyst), Information Technology Specialist, Network Security Analyst, Security Analyst, Systems Analyst

View report: Summary Details Custom

Tasks | Technical Skills | Tools Used | Knowledge | Skills | Abilities | Work Activities | Detailed Work Activities | Work Context | Job Zone | Education | Credentials | Interests | Work Styles | Work Values | Related Occupations | Work Activities Employment | Job Outlook | Additional Information

Tasks

5 of 12 displayed

- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures.
- Modify computer security files to incorporate new software, correct errors, or change individual access status.

back to top

Technology Skills

5 of 51 displayed Show 5 tools used

- Development environment software — Apache Ant, Go, Microsoft Visual Studio, National Instruments LabVIEW
- Network monitoring software — IBM QRadar SIEM, Nagios, Symantec Blue Coat Data Loss Prevention, Wireshark
- Operating system software — Linux, Microsoft Windows Server, Shell script, UNIX
- Transaction security and virus protection software — HP Webinspect, McAfee, Portswigger BurP Suite, Symantec

Occupation Quick Search:

Wages & Employment Trends

Median wages (2019) \$47.95 hourly, \$99,730 annual

State wages

Local wages ZIP Code:

Employment (2018) 112,300 employees

Projected growth (2018-2028) Much faster than average (11% or higher)

Projected job openings (2018-2028) 12,800

State trends

Top industries (2018) [Professional, Scientific, and Technical Services](#)
[Finance and Insurance](#)

Source: Bureau of Labor Statistics [2019 wage data](#) and [2018-2028 employment projections](#). "Projected growth" represents the estimated change in total employment over the projections period (2018-2028). "Projected job openings" represent openings due to growth and replacement.

[back to top](#)

Job Openings on the Web

[back to top](#)

Sources of Additional Information

All 10 displayed

Disclaimer: Sources are listed to provide additional information on related jobs, specialties, and/or industries. Links to non-DOL Internet sites are provided for your convenience and do not constitute an endorsement.

- [\(ISC\)2](#)
- [CompTIA](#)
- [CompTIA Association of IT Professionals](#)
- [High Technology Crime Investigation Association](#)
- [Information Systems Security Association](#)
- [InfraGard](#)
- [ISACA](#)
- [National Initiative for Cybersecurity Education](#)
- [Occupational Outlook Handbook: Information security analysts](#)



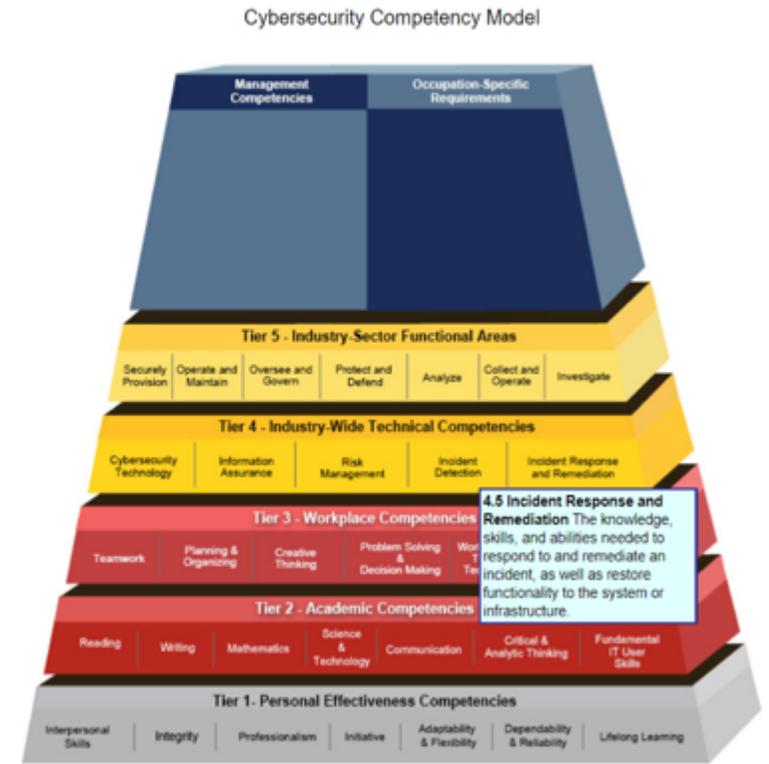
Competency Model Clearinghouse

The screenshot shows the homepage of the Competency Model Clearinghouse. At the top, there is a navigation bar with links for 'Get Started', 'Industry Models', 'Models in Action', 'Build a Model Tool', and 'Find Resources'. Below this is a large banner for 'View an Industry Model' featuring a pyramid diagram with three levels: 'OCCUPATION RELATED' (top), 'INDUSTRY RELATED' (middle), and 'FOUNDATIONAL' (bottom). The banner lists several industry models: Geospatial Technology, Advanced Manufacturing, Fundamentals of Health Care, Mechatronics, Renewable Energy, and others. Below the banner are four buttons: 'Get Started', 'Industry Models', 'Models in Action', and 'Build a Model Tool'. At the bottom, there are three columns of content: 'Latest Industry Models' (listing Advanced Manufacturing, Cybersecurity, Commercial and Industrial Construction, Heavy Highway Civil Construction, and Commercial Technology), 'Do It Yourself' (listing Build your own Model, View Build a Model Tool demo, Register Here, and General Instructions to Build a Model), and 'What's New' (listing Advanced Manufacturing Competency Model Updated, Cybersecurity Competency Model Updated, Added new video to the CMC video series, and New Case Summary - Developing Competency-Based Approaches).

- [Industry Association Links](#)
- [NICE Free and Low Cost Online Cybersecurity Learning Content](#) **New**
- [Cybersecurity Workforce Demand](#)
- [Cybersecurity Workforce Development Toolkit](#) **New**
- [NICCS Training Catalog](#)
- [NICCS - Call for Training Providers](#)
- [Building the Cyber-Savvy Workforce - Webinar](#)
- [Cybersecurity Certifications](#)
- [Cybersecurity Education](#)
- [Certification Finder](#)

- How To**
- [Download the industry model and worksheets in several formats](#)
 - [Instructions to view the model graphic](#)

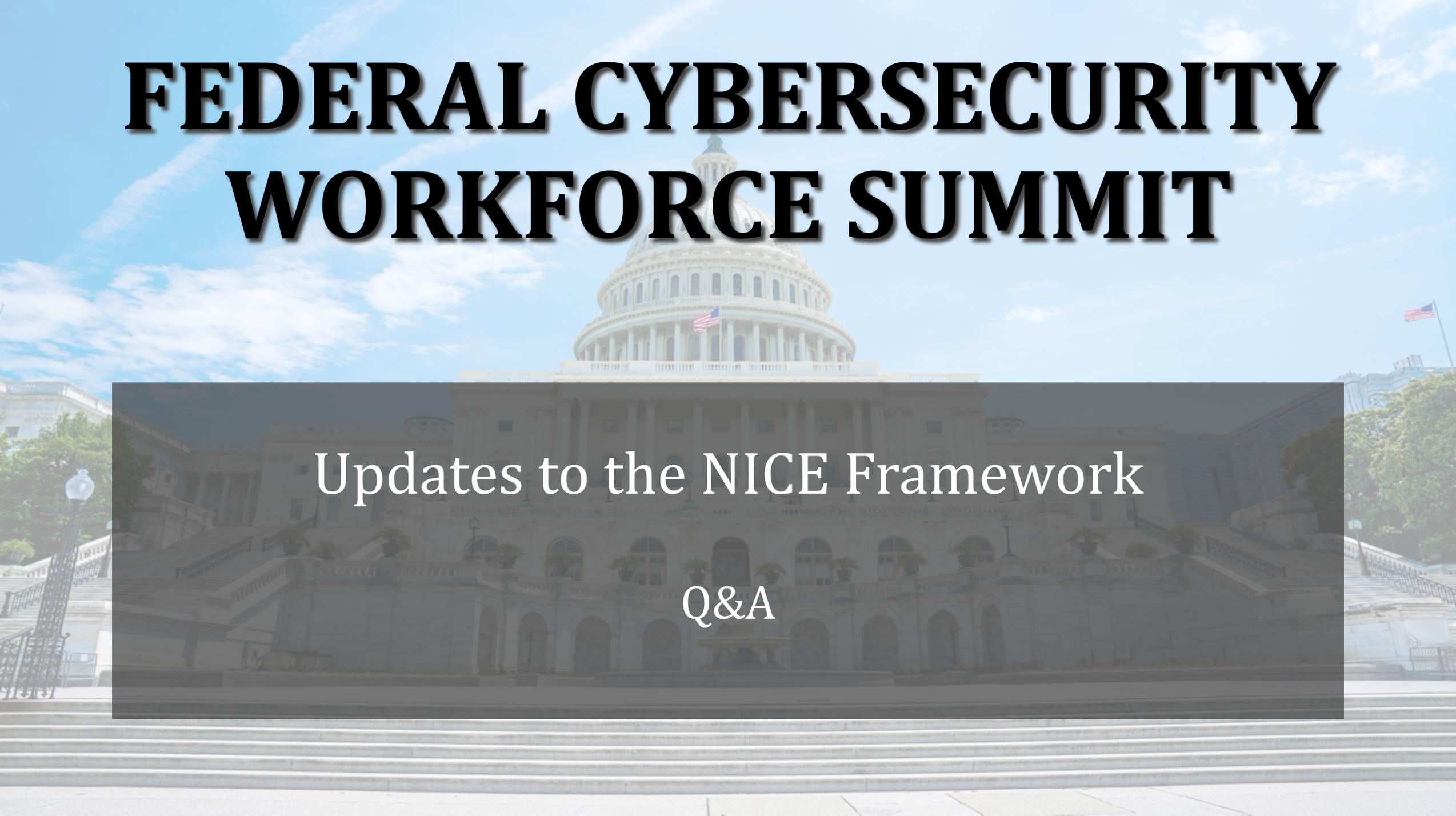
- General Information**
- [The "Building Blocks"](#)
 - [Frequently Asked Questions](#)



<https://www.careeronestop.org/competencymodel/>



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

The background of the slide is a photograph of the United States Capitol building in Washington, D.C. The building is a large, white, neoclassical structure with a prominent central dome. The sky is blue with scattered white clouds. The image is slightly faded to allow the text to be clearly visible.

Updates to the NICE Framework

Q&A

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

The background of the slide is a photograph of the United States Capitol building in Washington, D.C. The building is a large, white, neoclassical structure with a prominent central dome. The sky is blue with scattered white clouds. The text is overlaid on the top half of the image.

Intermission

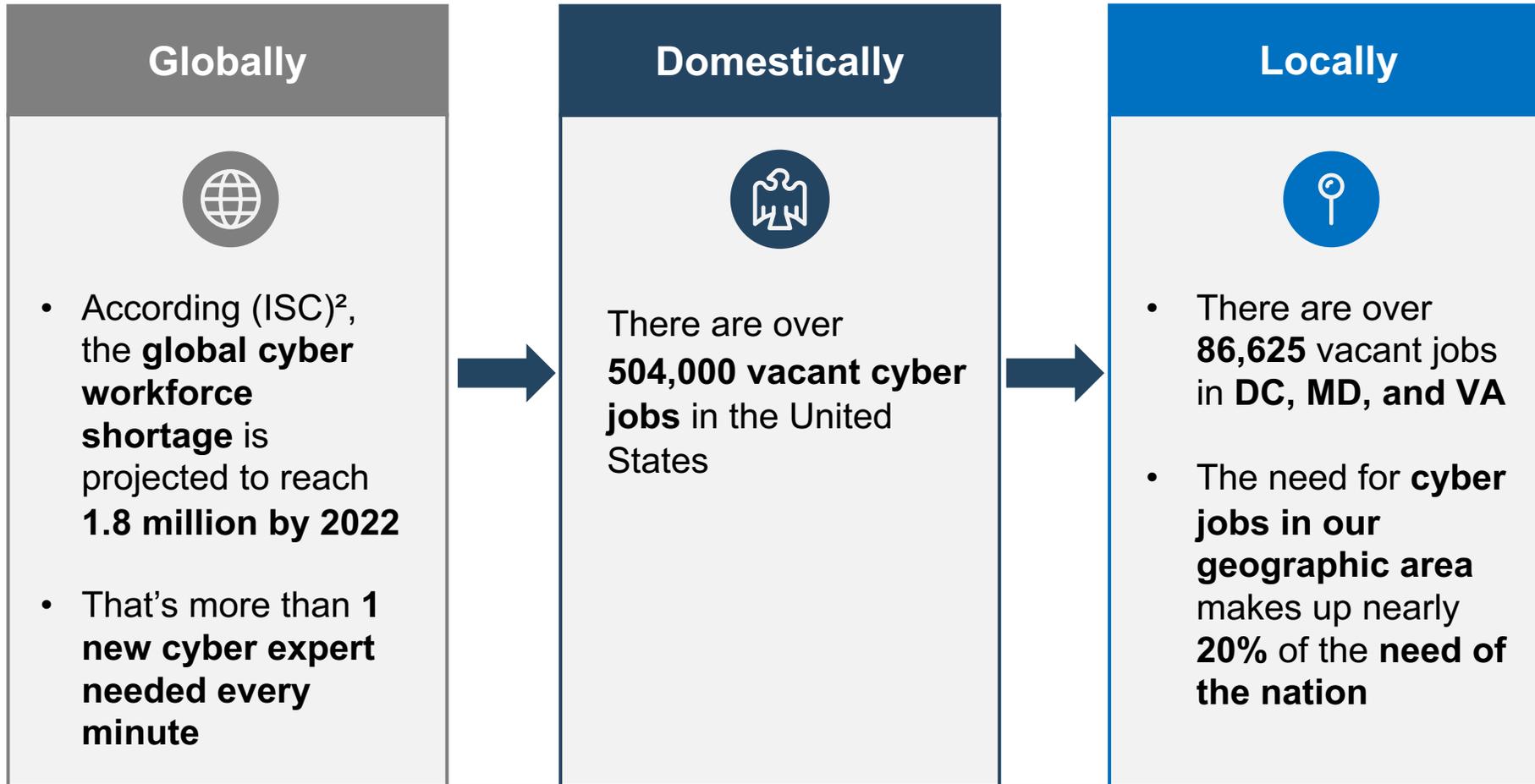
FEDERAL CYBERSECURITY WORKFORCE SUMMIT



Cybersecurity Career Pathways for
Federal Employees

Megan Caposell, Matt Isnor, Christopher Paris

The Challenge



Cyber has the Spotlight

National Cyber Strategy

To improve recruitment and retention of highly qualified cybersecurity professionals to the Federal Government, the Administration will continue to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce.

Federal Cybersecurity Workforce Assessment Act

The Act furthers the work the U.S. Office of Personnel Management (OPM) and agencies have begun to identify the Federal cybersecurity workforce. It also positions us to improve our workforce planning capabilities for this critical workforce and promotes collaboration in implementation among agencies.

EO on America's Cybersecurity Workforce

The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers—especially when those talents and capabilities can advance our national and economic security.

President's Management Agenda

Developing a Workforce for the 21st Century: Improve the ability of employees to design career paths in federal service and for agencies to clarify career paths that would be most helpful to fulfill workforce planning needs.



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.
- An **interactive cyber career pathway tool** available to the public.



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 & Benefits

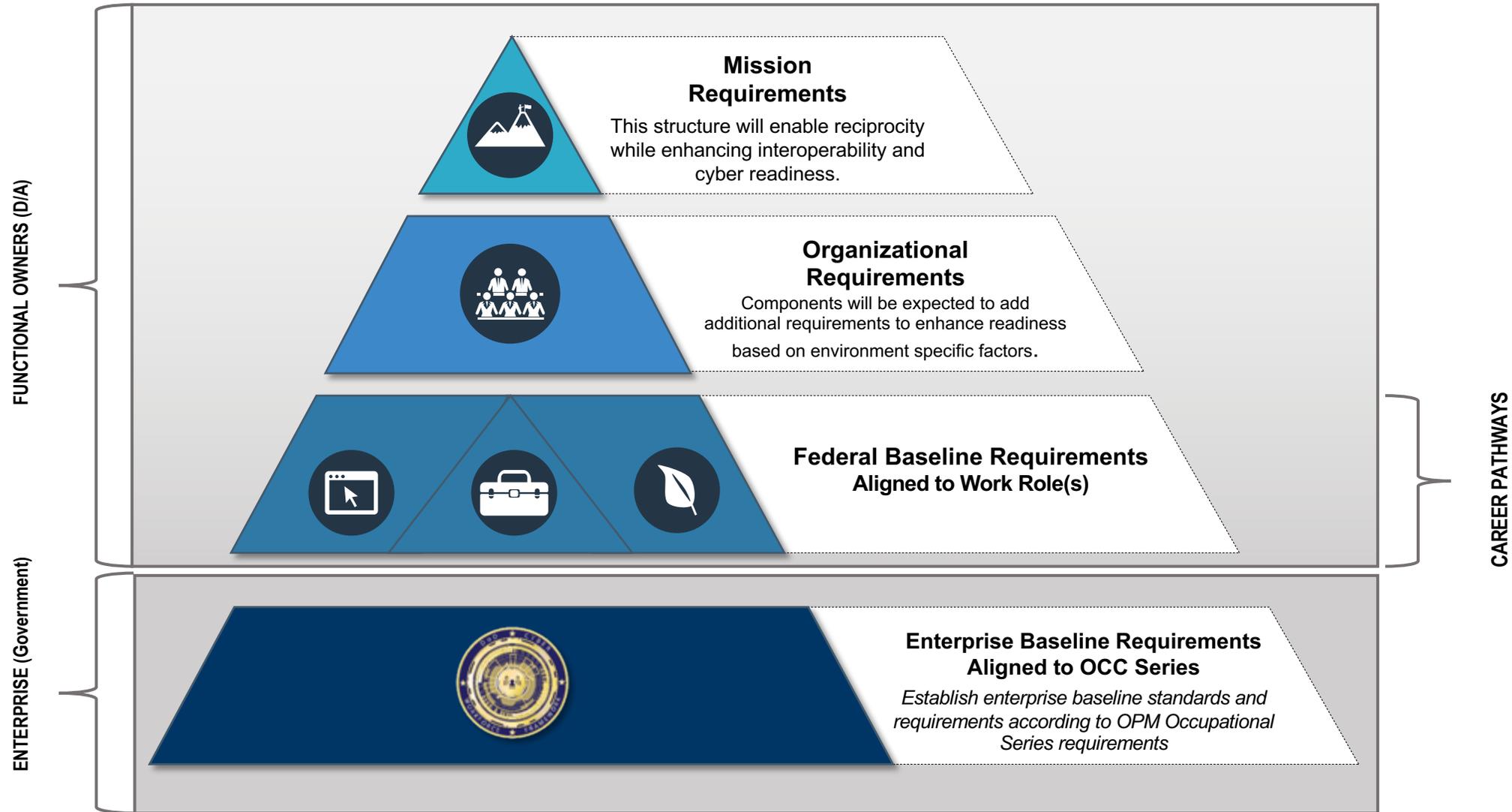


21 of 24 CFO Act D/As

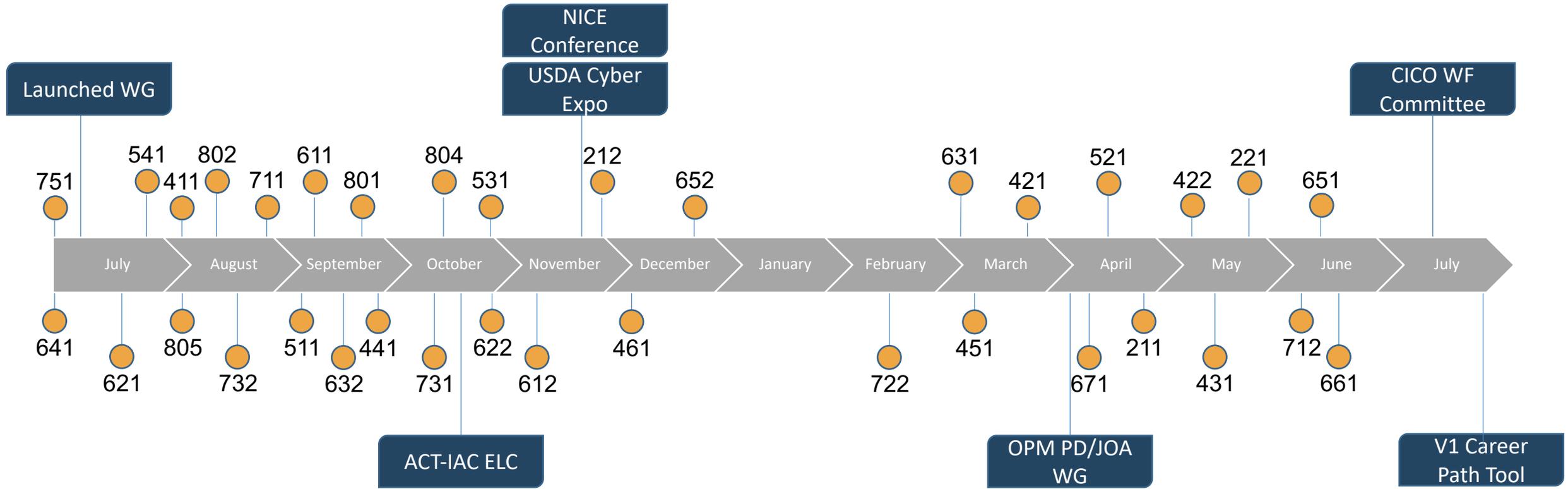
Decentralized Model
<ul style="list-style-type: none"> • 9 Technical SMEs @ 16 hours / work role • 3 Cyber Workforce Managers @ 148 hours / work role
<p>X 52 Work Roles</p> <p>X 24 Agencies</p> <p>=</p>
<ul style="list-style-type: none"> • 689k hours of SME / WF Manager Time
<p>X \$56/hour (est. GS-14, Step 1)</p> <p>=</p>
<p>\$ Total Federal-wide spend = \$38.7M</p>

Centralized Model
<ul style="list-style-type: none"> • 2 Technical SMEs @ 16 hours / work role <li style="text-align: center;">X 52 Work Roles
<ul style="list-style-type: none"> • 3 Cyber Workforce Managers @ 136 hours <li style="text-align: center;">X 2 work roles
<p>=</p>
<ul style="list-style-type: none"> • 60k hours of SME / WF Manager Time
<p>X \$56/hour (est. GS-14, Step 1)</p> <p>=</p>
<p>\$ Total Federal-wide spend = \$3.3M,</p>
<p>Cost Avoidance: \$35M and 629k hours of effort</p>

Federal Wide Standards



What We've Accomplished



Career Pathways Tool

Career Pathways

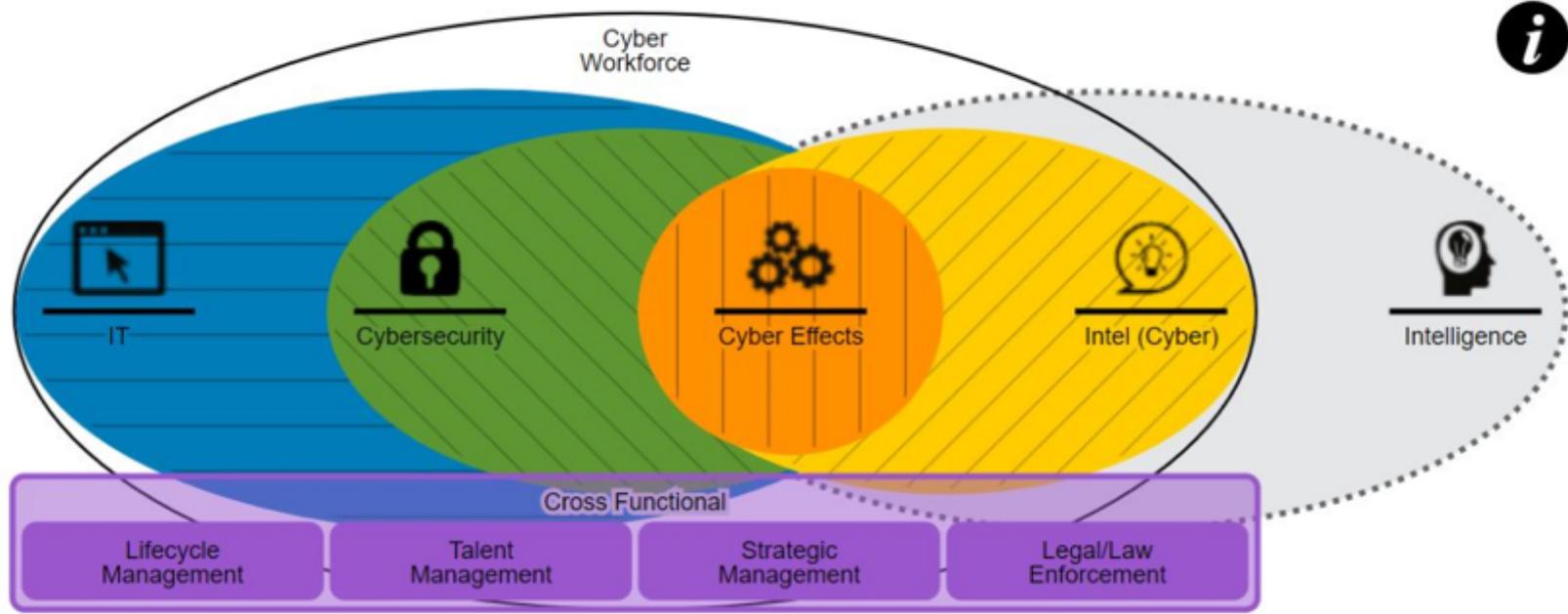
Welcome to the Career Pathways tool!

This tool will help you plan out steps for your cybersecurity career.

To start, select a work role below, or enter keywords in the search bar on the right.

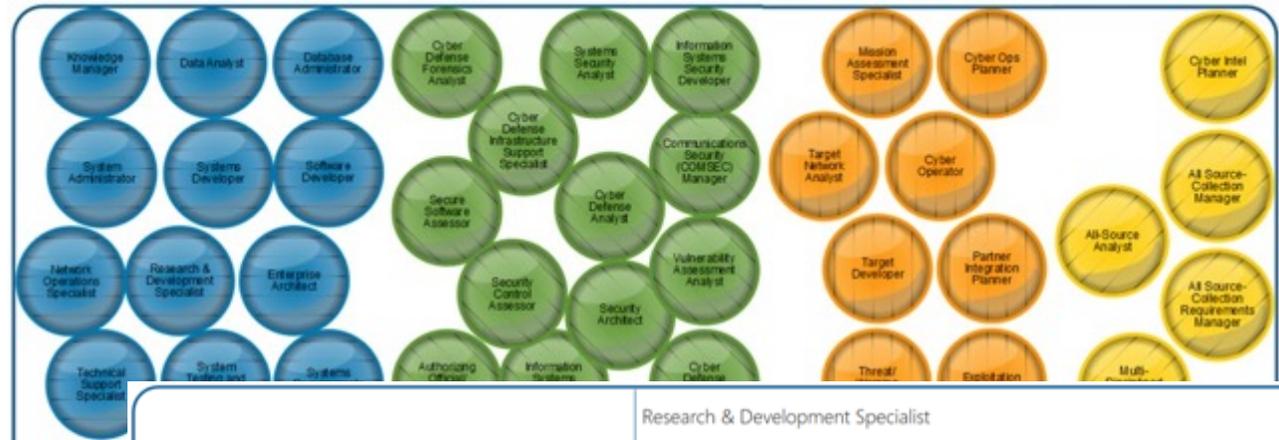
All Core Relationships

Begin typing to search work role names.



Key Features

- Cyber Skill Communities and their alignment to work roles (v1)
- Relational views between work roles and the ability to compare roles based on overlapping Knowledge, Skills, Abilities, and Tasks (KSAT) (v1)
- Core KSAT (v1)
- Alignment to Federal Occupational Series (*future sprint*)
- Related functional and position titles (*future sprint*)
- On/Off Ramps, as well as Pairings to other work roles (*future sprint*)
- Suggested Training and Certifications (*future sprint*)
- Core Competencies (*future sprint*)
- Core Task Behavioral Indicators at Entry, Intermediate, and Advanced proficiency levels (*future sprint*)



Research & Development Specialist

Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Category: Securely Provision
Specialty Area: Technology R&D
Community: IT

Tasks	Knowledge	Skills	Abilities	Capability Indicators
T0064	Review and validate data mining and data warehousing programs, processes, and requirements.			
T0249	Research current technology to understand capabilities of required system or network.			

Identify cyber capabilities strategies for custom hardware and software development based on mission.

Research & Development Specialist

Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Category: Securely Provision
Specialty Area: Technology R&D
Community: IT

Security Control Assessor

Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Category: Securely Provision
Specialty Area: Risk Management
Community: Cybersecurity

Percentage Match	Tasks	Knowledge	Skills	Abilities	Capability Indicators
7.65% Shared Subject Areas	0.00% Shared Tasks	15.57% Shared Knowledge	1.47% Shared Skills	8.33% Shared Abilities	



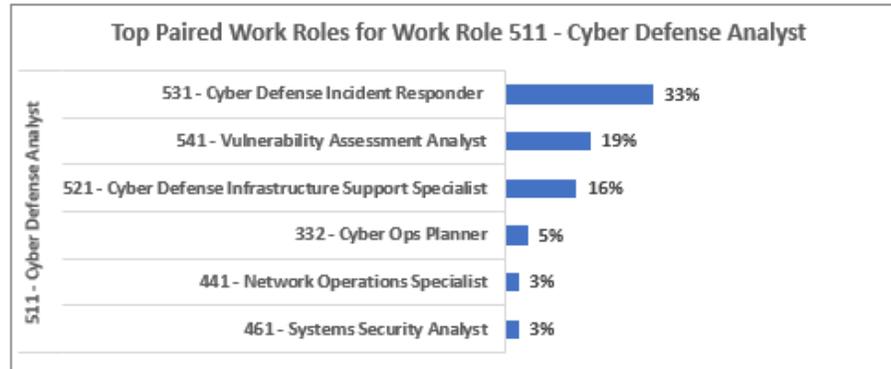
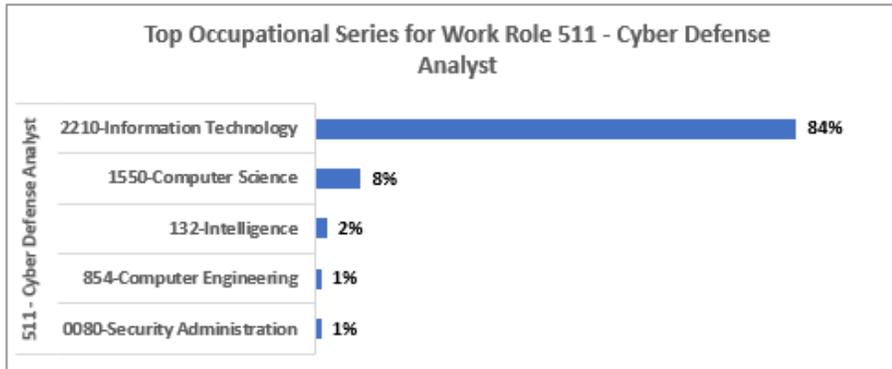
Additional Resources

Federal Government Wide Mapping of NICE Cybersecurity Work Roles

OPM Data as of 2019

Select Work Role ☰ 🔍

111 - All-Source Analyst	211 - Law Enforcement /CounterIntelligen...	212 - Cyber Defense Forensics Analyst	221 - Cyber Crime Investigator
332 - Cyber Ops Planner	411 - Technical Support Specialist	421 - Database Administrator	422 - Data Analyst
422 - Data Analyst	431 - Knowledge Manager	441 - Network Operations Specialist	451 - System Administrator
461 - Systems Security Analyst	511 - Cyber Defense Analyst	521 - Cyber Defense Infrastructure Suppo...	531 - Cyber Defense Incident Responder
541 - Vulnerability Assessment Analyst	611 - Authorizing Official/Designating Re...	612 - Security Control Assessor	621 - Software Developer
622 - Secure Software Assessor	631 - Information Systems Security Devel...	632 - Systems Developer	641 - Systems Requirements Planner
652 - Security Architect	671 - System Testing and Evaluation Spe...	711 - Cyber Instructional Curriculum Deve...	712 - Cyber Instructor
722 - Information Systems Security Mana...	731 - Cyber Legal Advisor	732 - Privacy Officer/Privacy Compliance ...	751 - Cyber Workforce Developer and Ma...
801 - Program Manager	802 - IT Project Manager	804 - IT Investment/Portfolio Manager	805 - IT Program Auditor
901 - Executive Cyber Leadership			



Who Can Use the Tool?



EMPLOYERS

- Conducting workforce assessment & planning activities
- Consistent PD Development / Classification
- Tailored JOAs w/ Role-Specific Requirements
- Identifying training needs / aligning training budget to role-specific training and certifications
- Learning Objectives, Curricula, Aptitude/Performance-based assessments aligned to work roles



PROFESSIONALS

- Clear understanding of the Cyber Workforce, Skill Communities, Work Roles
- Ability to identify, analyze, compare cyber roles of interest
- Upskill / Reskill using role-specific training and certifications
- Individual development plans to achieve desired career path
- Rewarding and challenging career



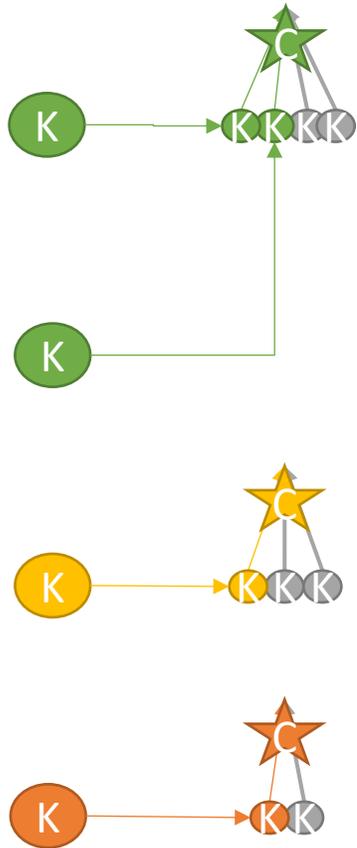
STUDENTS / RECENT GRADS

- Identify cyber roles of interest
- Understand relationship and progressions between work roles and communities
- Identify and pursue training and certifications that may increase preparedness for a cyber career within the Federal government

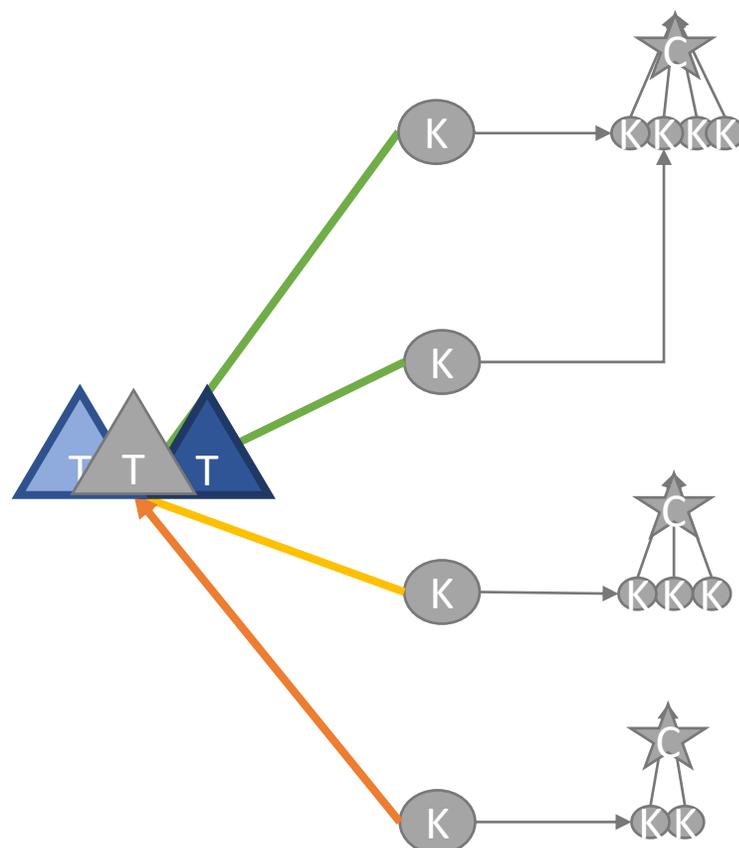


What's Next?

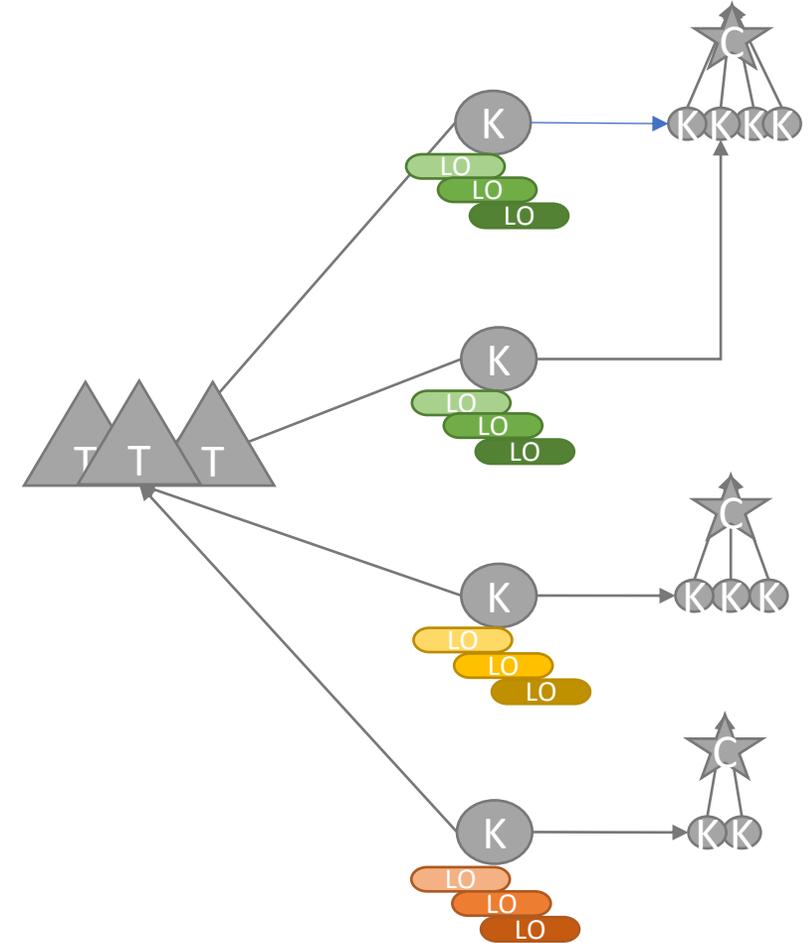
Work Role



Phase 1 – Link KSAs to Tasks



Phase 2 – Learning Objectives



Phase 2 Initiatives

- Community and Work Role Learning Objectives
- Behavior-based Interview Questions
- Criteria and Requirements for Aptitude / Performance-based Assessments
- Criteria and Requirements for Federal Credentialing Body

What additional cyber workforce related challenges would you want the interagency Working Group to address?



Join the Working Group

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>



 Christopher.Paris@va.gov



 Megan.Caposell@hq.dhs.gov



 Matthew.M.Isnor.civ@mail.mil



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Cybersecurity Career Pathways for
Federal Employees

Q&A



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION

PRESIDENT'S CUP CYBERSECURITY COMPETITION

To Identify, Recognize, and Reward the Best Cyber Talent in Federal
Service



Overview



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- President's Cup 2019 Wrap-Up
- President's Cup 2019 Challenge Release
- President's Cup 2020
 - President's Cup 2020 Improvements
 - President's Cup 2020 Format
 - Teams
 - Individuals
 - President's Cup 2020 Dates
 - President's Cup 2020 Final Round



President's Cup 2019 Wrap-Up

- Two Tracks – Teams and Individuals
- Two Qualifying Rounds per Track
 - “Game-show” style
 - Held remotely over 10 days with 8 hour time limit
- Challenges from across NICE Cybersecurity Workforce Framework
- Final round consisted of 3D virtual “Escape Room”

Teams Round 1 Gameboard

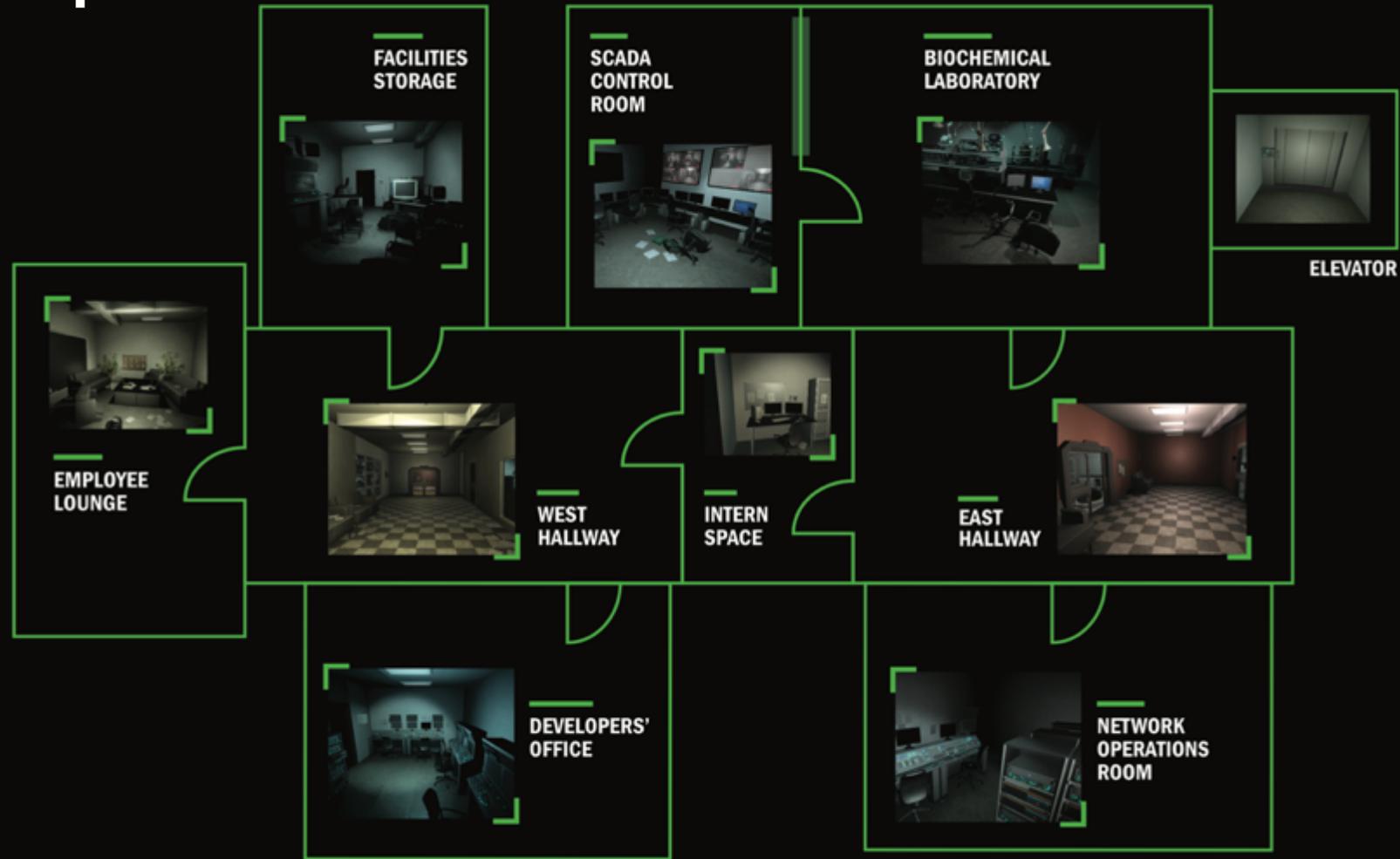
ANALYZE AND INVESTIGATE	COLLECT AND OPERATE	OPERATE AND MAINTAIN	PROTECT AND DEFEND	SECURELY PROVISION
250	250	250	250	250
500	500	500	500	500
1000	1000	1000	1000	1000



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION



Escape Room Map



PRESIDENT'S CUP
CYBERSECURITY COMPETITION

PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup 2019 Wrap-Up (Cont'd)

- Over 1000 registrants across over 200 teams and individuals
- Over 6,000 combined hours across 3 rounds of the competition
- Over 3300 Challenges Attempted, with close to 1800 Challenges Solved Successfully
- Winners celebrated at EEOB with awards ceremony hosted by VPOTUS



PCCC 2019 Livestream:

https://www.youtube.com/watch?v=V7Qb_xrja27I



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup 2019 Challenges

- President's Cup Cyber Competition 2019 Challenges to be released to the community by end of June
 - 48 of 72 Challenges to be released on github.com/cisagov as “open-source” resources
 - All 72 challenges to be released on a cloud-hosted President's Cup gameboard for .gov/.mil to participate
 - “Gameboard” application to be released on github.com/cmu-sei for cyber community to use in future cyber competitions
 - Stay tuned for more info at cisa.gov/presidentscup !



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup Cybersecurity Competition 2020



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup 2020 Improvements



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- **New Challenge Formats**
 - Multi-part and multi-stage challenges
 - Samples of each new format available during registration
- **New Challenge Focus**
 - Work-role based to encourage specialization
 - Two separate individual tracks
- Longer registration window
- More information provided to competitors up-front on challenge board



President's Cup 2020

The competition will be organized around NICE Cybersecurity Workforce Framework Work Roles, with the Solo competition broken down into two tracks:

- Solo Competition

- Track A

- Cyber Defense Forensic Analyst
 - Cyber Defense Incident Responder

- Track B

- Vulnerability Assessment Analyst
 - Exploitation Analyst

- Team Competition

- Cyber Defense Incident Responder
 - Cyber Defense Forensics Analyst
 - Cyber Defense Infrastructure Support Specialist
 - Cyber Defense Analyst
 - Exploitation Analyst
 - Vulnerability Assessment Analyst
 - Software Developer
 - Network Operations Specialist

Participants can compete in any or all three categories
(Solo Tracks A and B, Teams)



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup 2020 Dates

- Qualifiers
 - Must succeed in first qualifier round to participate in second round
 - Teams – best team from each Department, plus top 20% based on score
 - Individuals – Top 100
- Final Round
 - Hosted live in Arlington, VA
 - Top 5 Teams and Top 10 Individuals in Tracks A/B

2020 **COMPETITION TIMELINE**

	 TEAMS COMPETITION	 INDIVIDUAL COMPETITION
REGISTRATION	July 27 - August 14	July 27 - August 28
QUALIFICATION ROUND 1	August 10 - 19	August 24 - September 2 (Both Tracks)
QUALIFICATION ROUND 2	September 8 - 15	September 21 - 28 (Both Tracks)
FINALS	December 8 - 10	-----

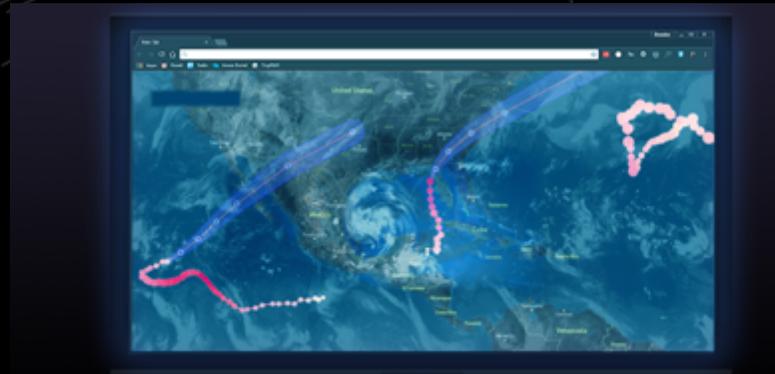
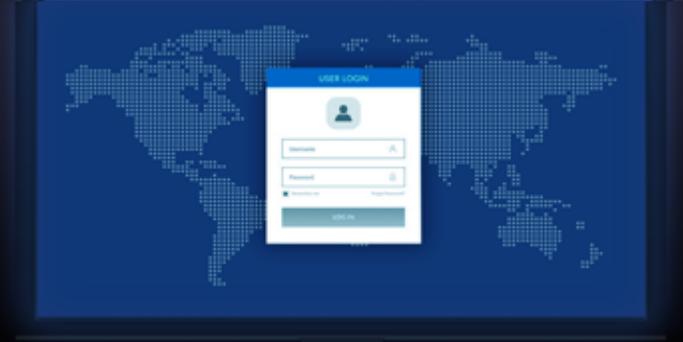


PRESIDENT'S CUP
CYBERSECURITY COMPETITION



President's Cup 2020 Final Round

- Live-stream
- Featuring a new “twist” on the Escape Room format
- More details to come...
- Register at presidentscup.cisa.gov on July 27th!



★ ★ ★ ★ ★ ★ ★ ★ ★ ★
PRESIDENT'S CUP
CYBERSECURITY COMPETITION





PRESIDENT'S CUP

CYBERSECURITY COMPETITION

FOR MORE INFORMATION: [CISA.GOV](https://www.cisa.gov)





FEDERAL CYBERSECURITY WORKFORCE SUMMIT

President's Cup Cybersecurity Competition

Q&A

Wrap Up

- Your feedback is important. Please watch for an email with a survey link.
- Today's Summit will be followed by a 4-part webinar series:
 - **Pay Flexibilities - July 21, 2020**
 - **Hiring Flexibilities - August 11, 2020**
 - **Candidate Assessment - September 15, 2020**
 - **Interpretive Guidance for Cybersecurity Positions - October 1, 2020**
- Webinar registration link: <https://www.eventbrite.com/e/federal-cybersecurity-workforce-webinar-series-registration-109857843768>

