FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Welcome and Overview

Marian Merritt

Deputy Director
National Initiative for Cybersecurity Education
National Institute of Standards and Technology, U.S. Department of Commerce

2022 Federal Cybersecurity Workforce Summit

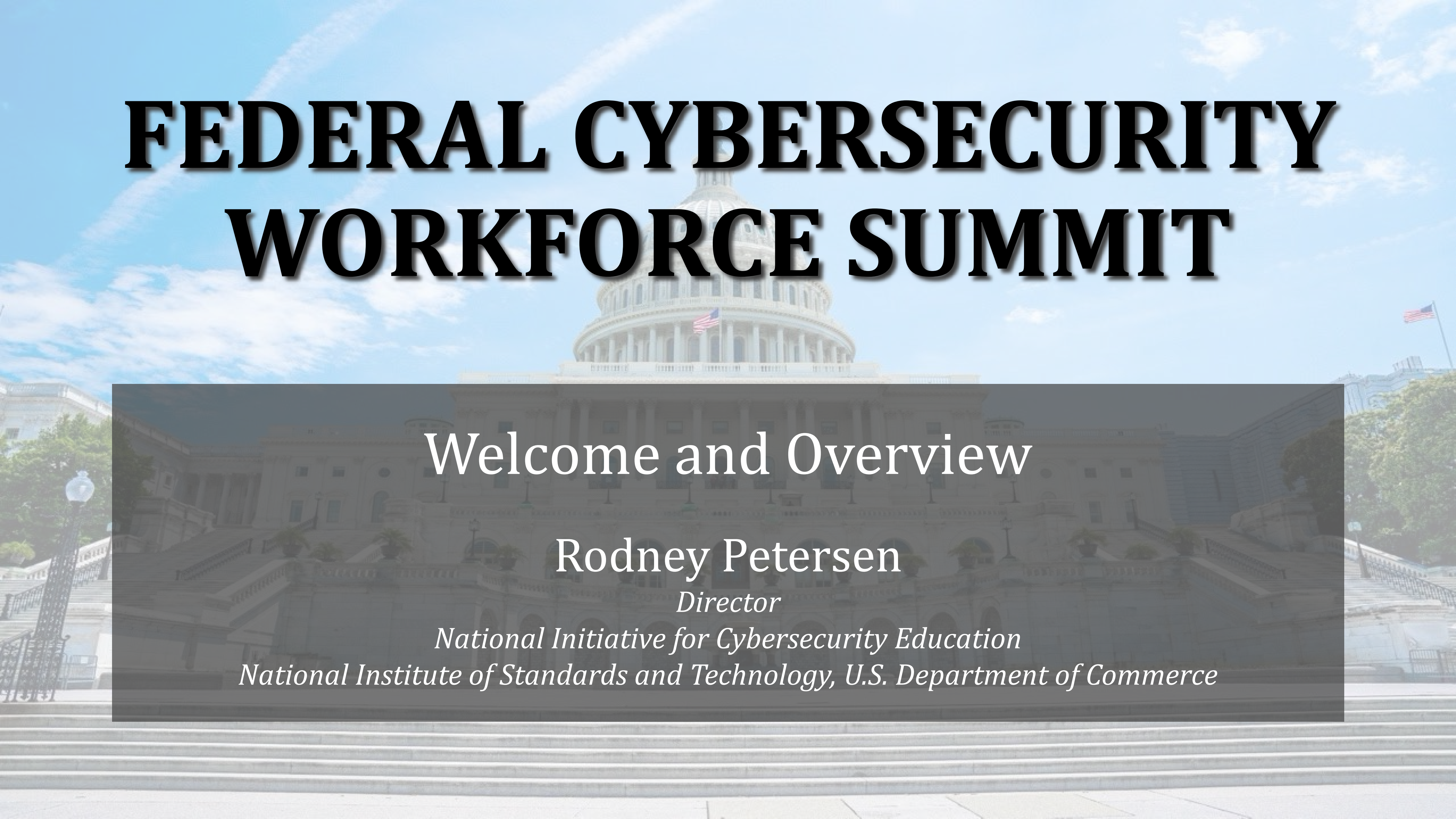
Purpose: To provide strategic directions and programmatic updates for stakeholders in the federal government who support the recruitment, hiring, development, and retention of the workforce necessary to reduce cybersecurity risks in federal environments.

Objectives:

- To provide strategic and program updates from key departments and agencies that influence cybersecurity workforce legislation, policy, guidance, and standards
- To highlight key projects and initiatives that support the growth and sustainment of the Federal cybersecurity workforce
- To create a sense of community among individuals in Federal departments and agencies with similar responsibilities for building a superior cybersecurity workforce

Event Reminders:

- This event will be recorded
- Presentation slides and recording will be available after event
- Q&A will occur after intermission



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Welcome and Overview

Rodney Petersen
Director
National Initiative for Cybersecurity Education
National Institute of Standards and Technology, U.S. Department of Commerce

NICE Strategic Plan and Implementation Plan

To energize, promote, and coordinate a **robust community** working together to advance an **integrated ecosystem** of cybersecurity **education, training, and workforce development**

Career Discovery

Promote the Discovery of Cybersecurity Careers and Multiple Pathways

Learning Process

Transform Learning to Build and Sustain a Diverse and Skilled Workforce

Talent Management

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

NICE Framework

Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)

Research

Drive Research on Effective Practices for Cybersecurity Workforce Development

NICE Events & Community Engagement

🖥 www.nist.gov/nice

✉ nice@nist.gov

@NISTcyber

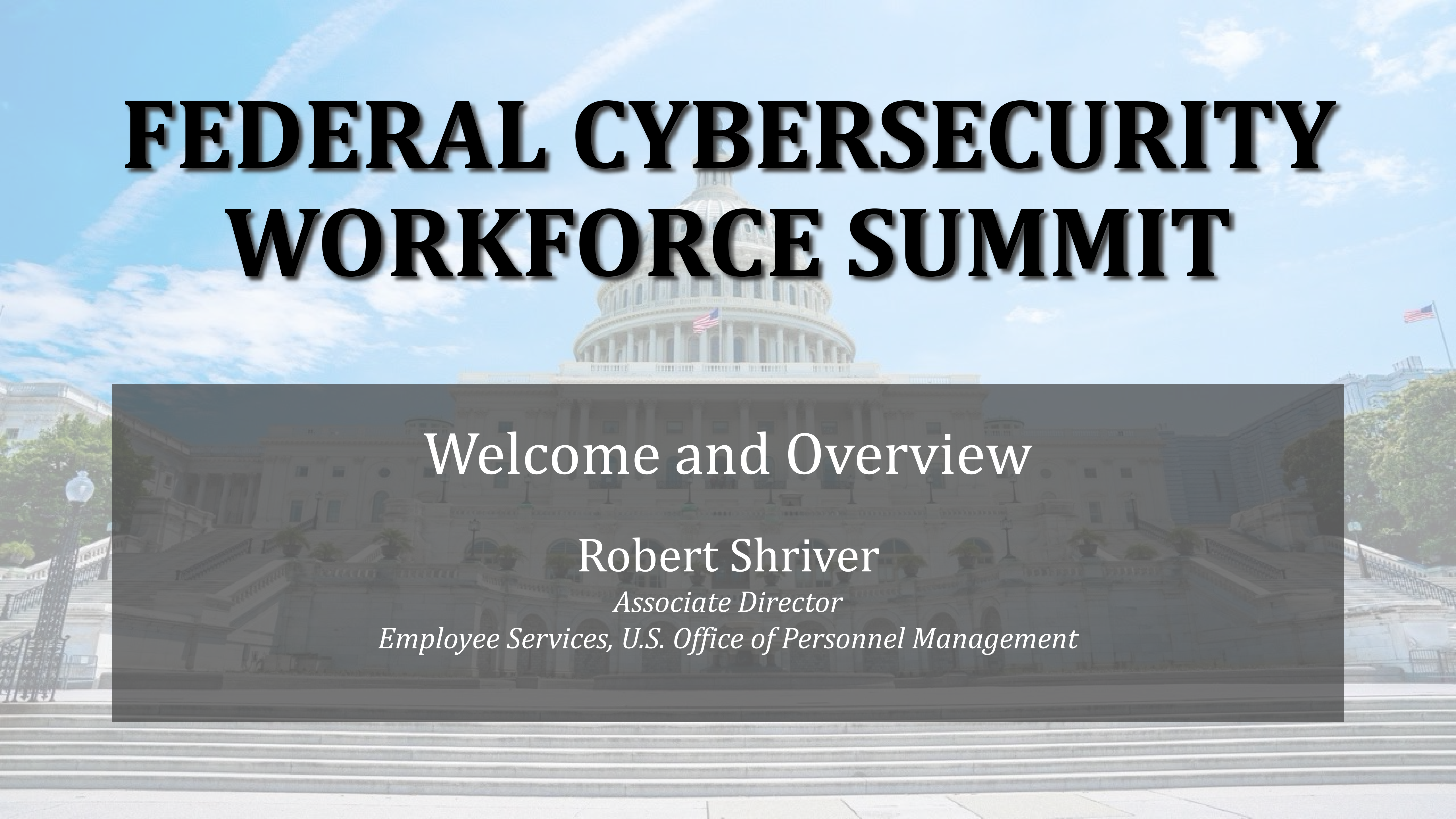
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Learn More with NICE Events

- NICE Webinars (monthly)
- Annual NICE Conference & Expo (Jun 6-8 - Atlanta, GA)
- Cybersecurity Career Awareness Week (Oct 17-22)
- NICE K12 Cybersecurity Education Conference (Dec 5-7 - St. Louis, MO)
- Federal Cybersecurity Workforce Summit and Webinar Series (annually)
- Federal Information Security Educators (FISSEA) (May 17)

Get Involved with the NICE Community

- NICE Community Coordinating Council
  - Working Groups: Promote Career Discovery, Transform Learning Process, and Modernize Talent Management,
  - Communities of Interest: Apprenticeships in Cybersecurity, Cybersecurity Skills Competitions, K12 Cybersecurity Education
  - NICE Framework Users Group
- NICE Interagency Coordinating Council
- NICE Stakeholder Engagement
  - Sectors: Academia, Industry, Government, and International
  - Audiences: Employers, Education and Training Providers, and Learners



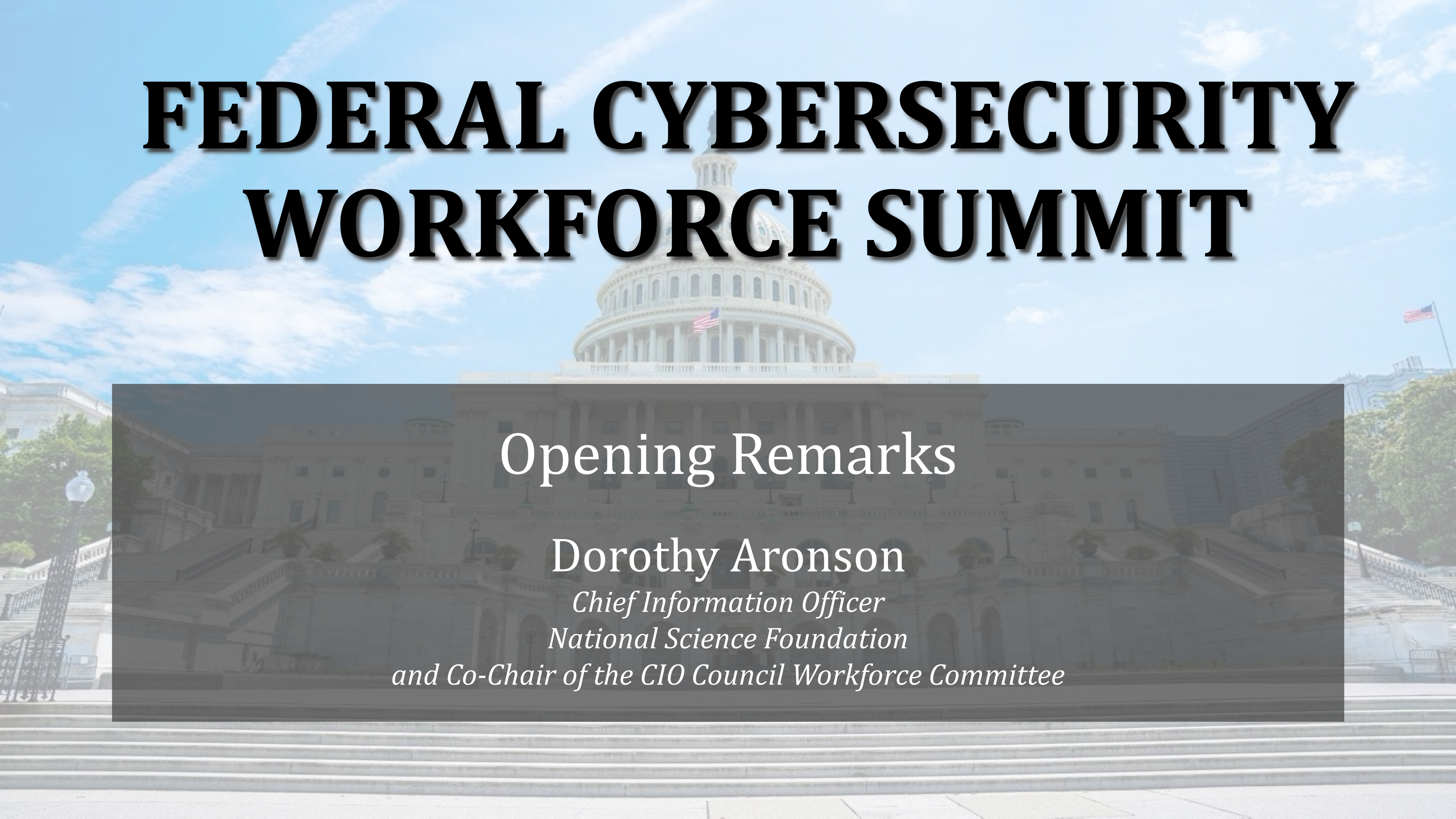
FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Welcome and Overview

Robert Shriver

Associate Director

Employee Services, U.S. Office of Personnel Management



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Opening Remarks

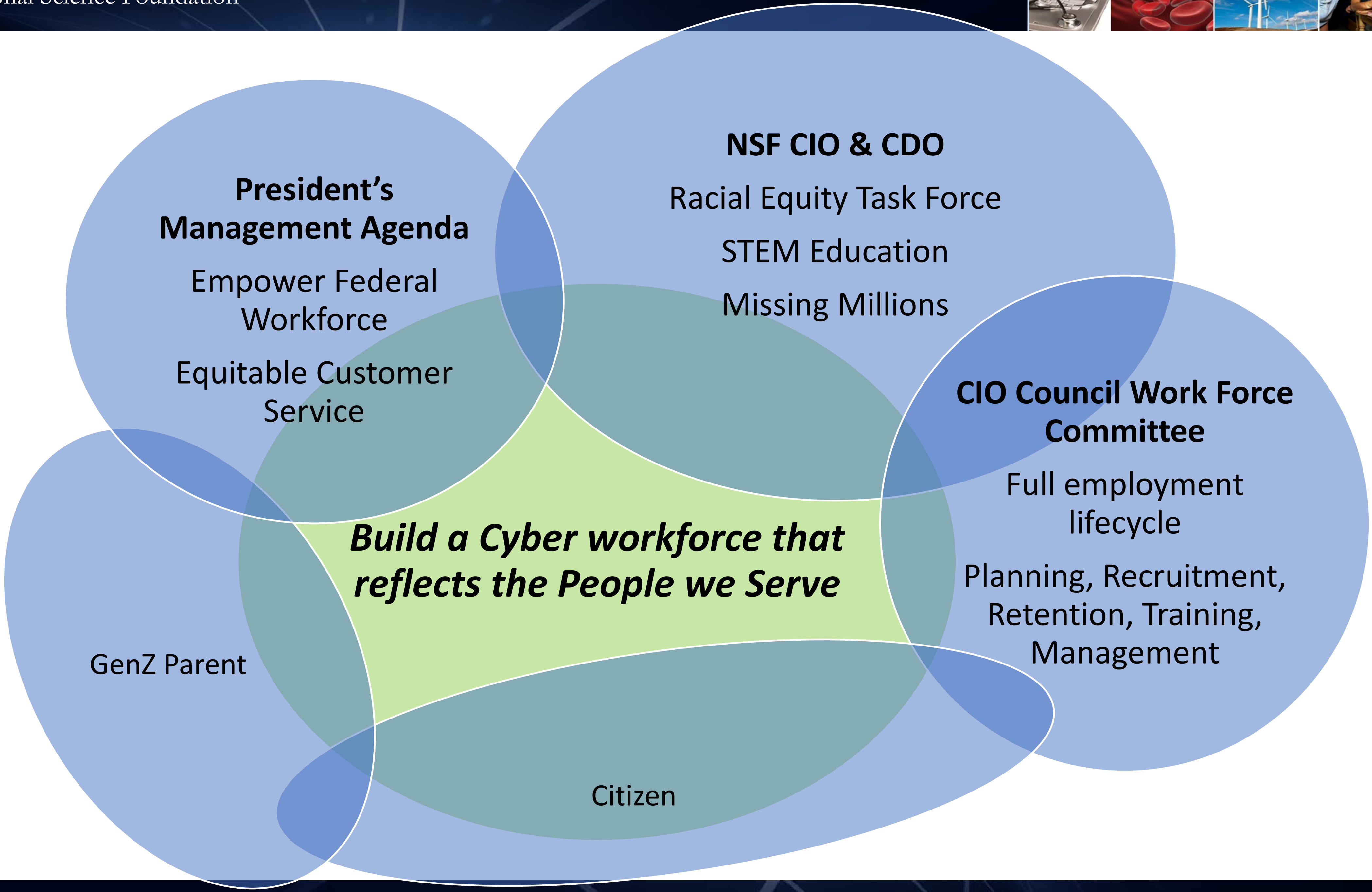
Dorothy Aronson

Chief Information Officer
National Science Foundation
and Co-Chair of the CIO Council Workforce Committee

HBCU RECRUITMENT INITIATIVE

ASSESSMENT

April 2022



President's Management Agenda

Empower Federal Workforce

Equitable Customer Service

NSF CIO & CDO

Racial Equity Task Force

STEM Education

Missing Millions

CIO Council Work Force Committee

Full employment lifecycle

Planning, Recruitment, Retention, Training, Management

Build a Cyber workforce that reflects the People we Serve

GenZ Parent

Citizen

HBCU RECRUITMENT INITIATIVE

PURPOSE

The Federal CIO Council's Workforce Committee seeks to improve the recruitment and hiring of top talent from Historically Black Colleges and Universities (HBCU).

- Focused recruiting at HBCUs can increase diversity, inclusion, and innovation in the workplace.

GOAL & OBJECTIVES

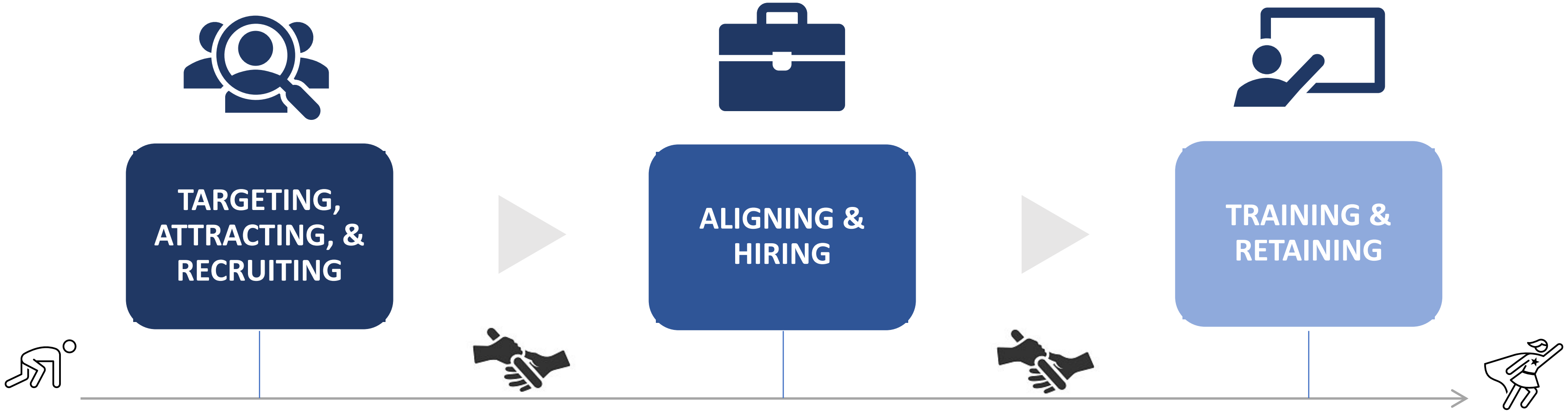
Improve the federal government's engagement and recruitment of IT talent from HBCUs.

- Engage with HBCUs and support the federal government to better connect with, market to, and recruit minority students and graduates.
- Promote and model a diverse and inclusive workforce through federal agencies’ employee outreach.
- Develop a communications tool kit that can be leveraged across the government for HBCU recruitment.

WORKING TOGETHER & PAVING A WAY FOR SUCCESS

Interviews with members from the Workforce Committee led the team to identify challenges within three stages of the hiring process, and offer recommendations based on group discussions, to help expand federal agencies' efforts to attract and retain high-potential diverse talent

From recruiting to hiring and retaining, there are resources, points of entry, and hand-offs that take place along the way.



TARGETING, ATTRACTING, & RECRUITING

ALIGNING & HIRING

TRAINING & RETAINING

Networking and Career Channels:

- Cyber Careers.gov
- Grace Hopper Celebration

Intake:

- Digital Corps
- Pathways Program

Development:

- Cyber NextGen
- Open Opportunities

OVERARCHING THEMES - SNAPSHOT

FEDERAL AGENCIES' RECRUITMENT EFFORTS GO BEYOND HBCUS

- Many agencies' recruitment efforts expand beyond HBCUs and include underrepresented schools such as Minority-Serving Institutes (MSI), Hispanic-Serving Institutes (HSI), and Tribal Serving Institutions (TSI)
- Many agencies recruiting programs in these areas are nascent or have yet to be developed

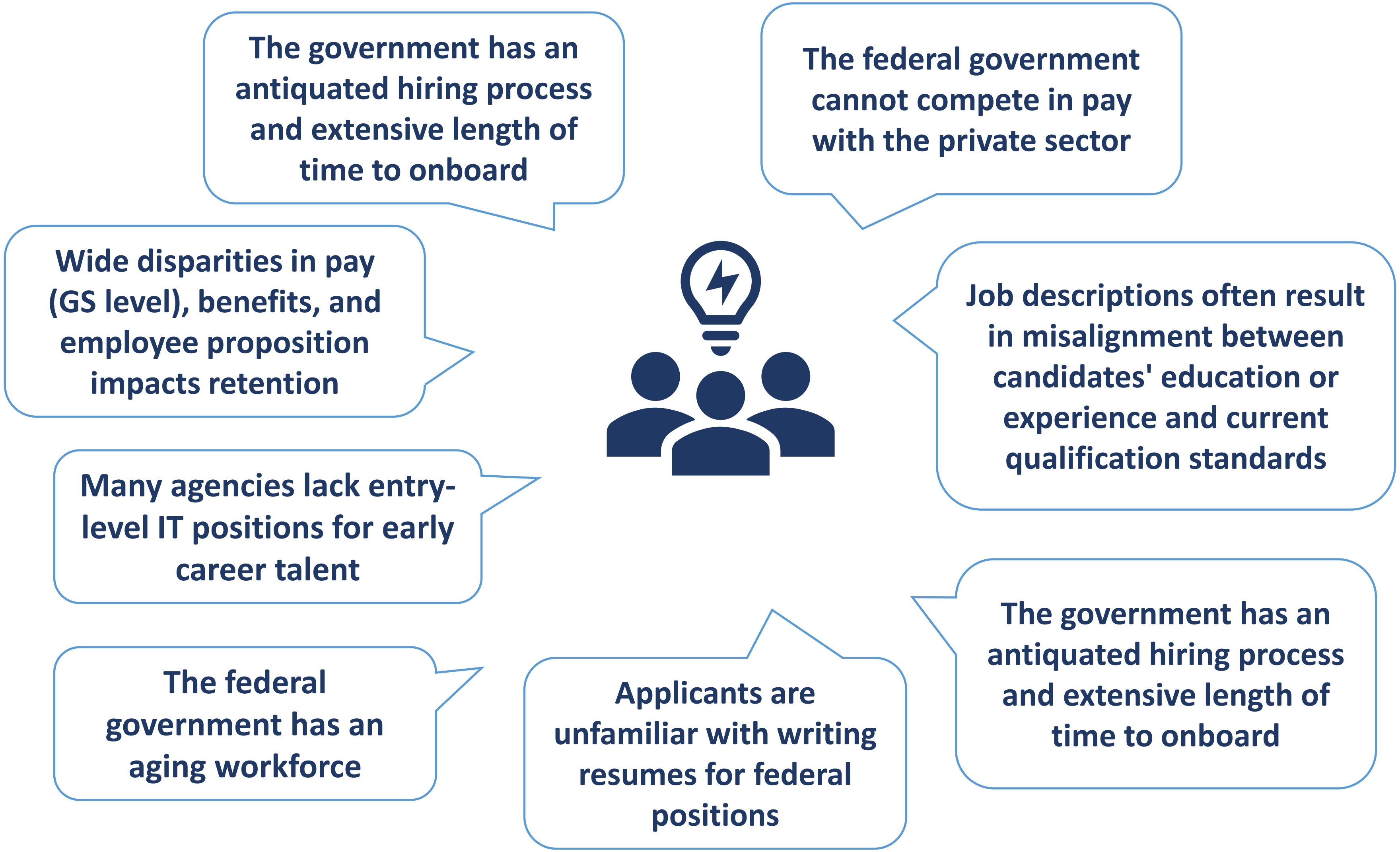
IMPROVING FEDERAL AGENCIES' PERSONA IS IMPORTANT

- Students may not perceive the federal government as being diverse or having cutting-edge IT initiatives
- Federal agencies must deliver messages via various communication tactics during outreach to humanize their image, and
- Demonstrate what working in different IT positions across the government is like FROM individuals who look like applicants

GEN ZS JOIN THE WORKFORCE, BUT EXPECTATIONS DIFFER

- The talent pool of recent graduates have different views and expectations of work (i.e., where they want to work and schedule, how they want to be managed, how long they expect to stay at one job before advancing to the next level). The pitch for stability and long-term placement is not perceived as a benefit.

CHALLENGES



The government has an antiquated hiring process and extensive length of time to onboard

The federal government cannot compete in pay with the private sector

Wide disparities in pay (GS level), benefits, and employee proposition impacts retention

Job descriptions often result in misalignment between candidates' education or experience and current qualification standards

Many agencies lack entry-level IT positions for early career talent

The federal government has an aging workforce

Applicants are unfamiliar with writing resumes for federal positions

The government has an antiquated hiring process and extensive length of time to onboard

OUR JOURNEY

PURPOSE

Meet with recruiting, diversity, equity, and inclusion experts to gain insight into existing programs and efforts, background information, best practices, and lessons learned to plan, develop, and strengthen the impact of this initiative

ASSESS & DEVELOP

- Gather and analyze feedback and data from discussions to understand current landscape; determine appropriate direction
- Define goals and objectives
- Identify engagement opportunities, develop messaging and create communication strategy for HBCU recruiting

IMPLEMENT

Lay a foundation and carry out the activities and communicate key messages as outlined in the communications plan; adjust timelines or activities as needed

feedback@cio.gov

MAINTAIN

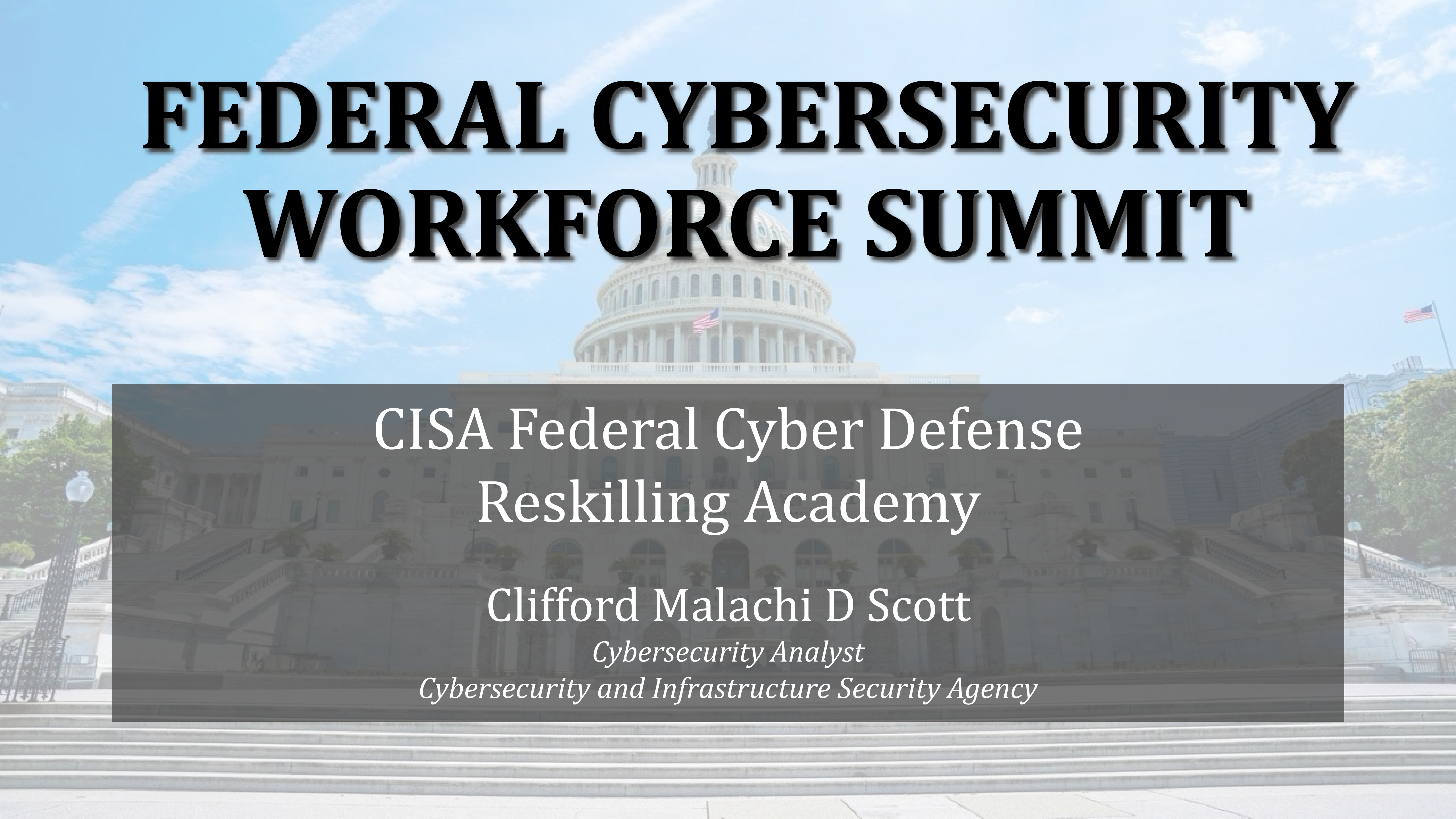
- Provide strategy and communications that agencies can leverage to recruit from HBCUs
- Create multiple continuities for HBCUs to access federal government career resources
- Promote Pathways program/internships
- Routinely participate in career fairs/events and leverage existing student networks

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Federal Cybersecurity Workforce Priorities and Policy Initiatives

Chris Inglis

National Cyber Director
Executive Office of the President



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

CISA Federal Cyber Defense Reskilling Academy

Clifford Malachi D Scott

Cybersecurity Analyst

Cybersecurity and Infrastructure Security Agency

FEDERAL CYBER DEFENSE SKILLING ACADEMY (FCDSA)

C. Malachi D. Scott

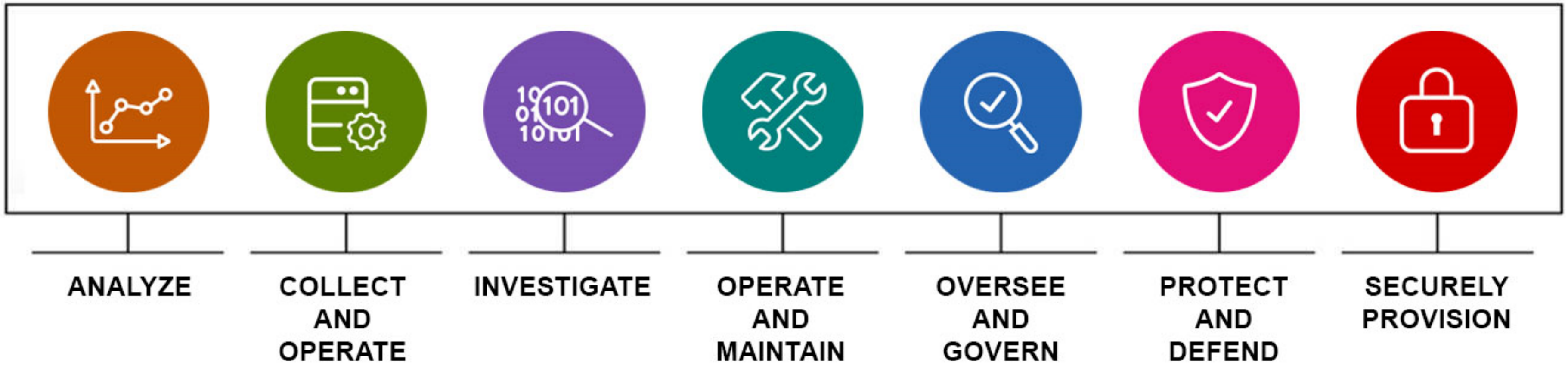
Cyber Defense Education & Training (CDET)

Cybersecurity Workforce Trends

- **Workforce skill gap projection:** According to (ISC)², the global cybersecurity workforce shortage is projected to reach 3.5 million by 2025
- **Workforce job vacancies:** According to CyberSeek, there are 465,000 open U.S. cybersecurity positions waiting to be filled as of April 2022.
- **Recruiting:** 54% of all open cybersecurity positions take an average of three months to fill according to an ISACA study
- **Diversity:** In the U.S. women make up only 24% of the cybersecurity workforce according to a 2022 study conducted by (ISC)²
- **Salary:** According to the Bureau of Labor Statistics, as of May 2020, the median salary for a cyber defense analyst is 103,950.

NICE Cybersecurity Workforce Framework

- Describes cybersecurity work
- Supports strategic workforce development
- Includes 7 Categories, 30+ Specialty Areas, 50+ Work Roles



ANALYZE

COLLECT AND OPERATE

INVESTIGATE

OPERATE AND MAINTAIN

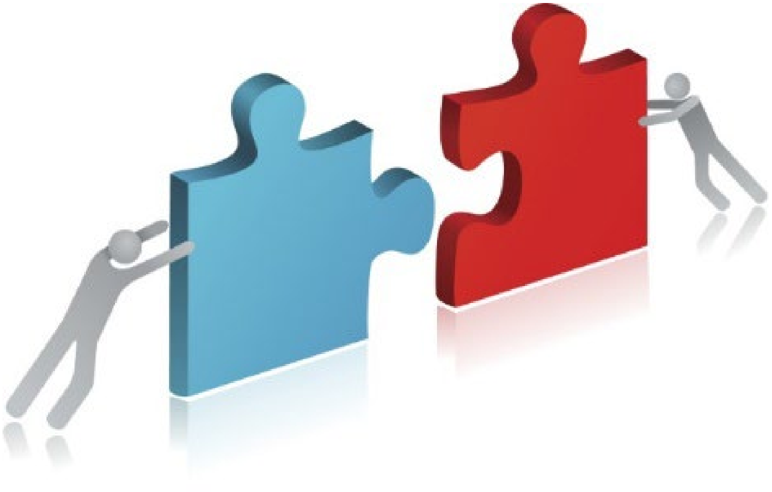
OVERSEE AND GOVERN

PROTECT AND DEFEND

SECURELY PROVISION

Directive

- To support the President's Management Agenda, Cross Agency Priority (CAP) sub-goal to build a modern IT and cybersecurity workforce, collaborate in overseeing and facilitating execution of skills training with the purpose of skills assessments, training curriculum, and programs that align with the National Initiative for Cybersecurity Education (NICE) Workforce Framework.



Purpose

- The FCDSA will training Federal Employees to be Entry Level Cyber Defense Analyst (CDA) per the Workforce Framework. We will train to students to use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.

Applying

- Who may apply
  - DHS Federal Civilian Employees
  - Any job series
  - GS-5s through GS-11s or equivalent
  - Exceptions can be made for GS-12 through GS-15 once lower grades are exhausted

- Aptitude and attitude assessment
  - **Does not assess students' knowledge of cyber security**
  - 45-60 minutes
  - Identifies optimal career matches
  - 12 work style preferences
    - Job satisfaction
    - Task-relevant
    - 7 career families

Full-Time Cohort

- 100% remote
- 12 weeks (Full-Time Cohort)
- Two 1-week breaks
- 8 AM – 5 PM ET
- Monday – Friday excluding Federal Holidays
- No prescheduled Annual Leave outside of the breaks

- Supervisor approval required
- While not a detail, Home Agency agrees that this is the student's full-time duty
- Laptop with webcam
- Must be on webcam during class hours
- Have access to Teams and Skillable

Key Training

Individual courses are matched to the NICE Framework

- Fundamental of Linux
- Windows Familiarization
- CompTIA
- Basic Networking and Protocol Analysis
- Introduction of Python
- Python for Security Analysis
- Concepts of Intelligence Based Computer Network Defense
- Correlating Attacks, Advanced DATA Analysis
- Identifying Common Hacker Techniques, Methods, and Vector
- Incident Detection Response and Handling

Student Comprehension

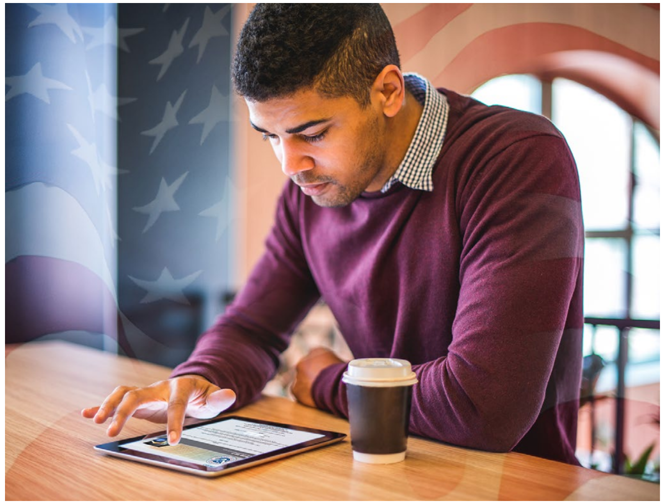
How do we ensure students are learning and retaining?

- Weekly Quizzes
- Automatic grading for instant feedback
- Labs (245hrs out the 501hrs)
- One-on-one instruction, if needed
- Learning Management System
  - Allows multiple tries at Labs for more practice and building of knowledge
- CyberScore Assessment
  - Taken at start of course and end of course.

Testing Knowledge

Students will be given the CyberScore Assessment at the start of the course and at the end.

- CyberScore Assessment Labs test on:
  - Protocol Analysis
  - Intrusion Detection
  - Incident Handling Methodology
  - Network Defense Analysis (Vulnerability)
  - Network Attack Analysis (Pen Testing)
- Each topic has a 45-minute Lab portion.



Certification

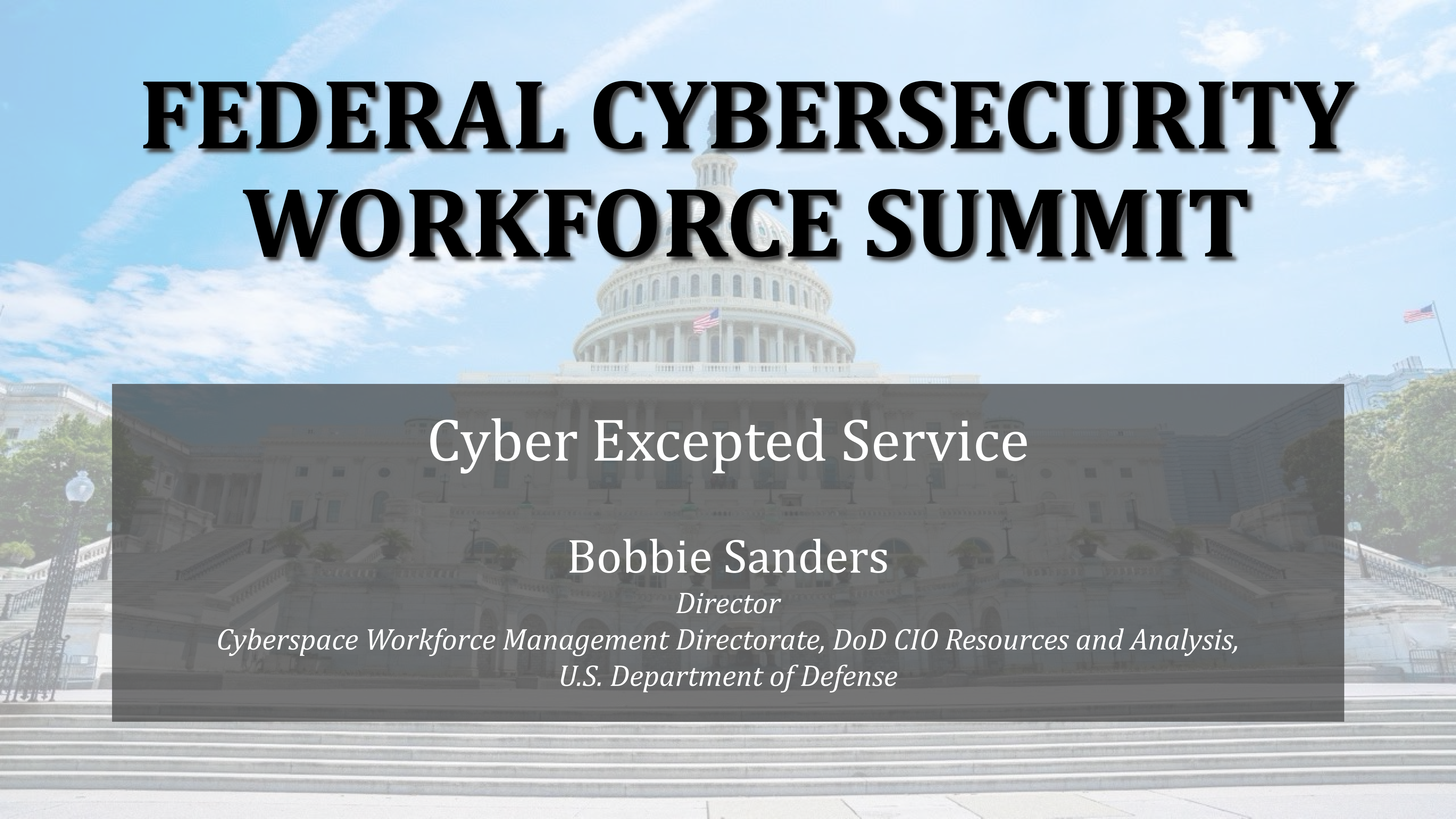
Students receive a voucher to take CompTIA’s Security+ Exam at the end of their Cohort.

- This will test six knowledge domain areas:
  - Threats, Attacks, and Vulnerabilities
  - Technology and Tools
  - Architecture and Design
  - Identity and Access Management
  - Risk Management
  - Cryptography

*Testing is setup to be remote although students can choose to take the test onsite at a Pearson Vue Testing Center.

Questions?

Education@cisa.dhs.gov



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Cyber Excepted Service

Bobbie Sanders

Director

Cyberspace Workforce Management Directorate, DoD CIO Resources and Analysis,
U.S. Department of Defense

INTERMISSION

Program will resume at 2:45 p.m. EDT

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Panel Discussion:

A Workforce Skilled in Cybersecurity for Operational Technology

Karen Wetzel
Manager of the NICE Framework
National Initiative for Cybersecurity Education, National Institute of Standards and Technology, U.S. Department of Commerce

Keith Stouffer
Project Manager
Cybersecurity for Operational Technology, National Institute of Standards and Technology, U.S. Department of Commerce

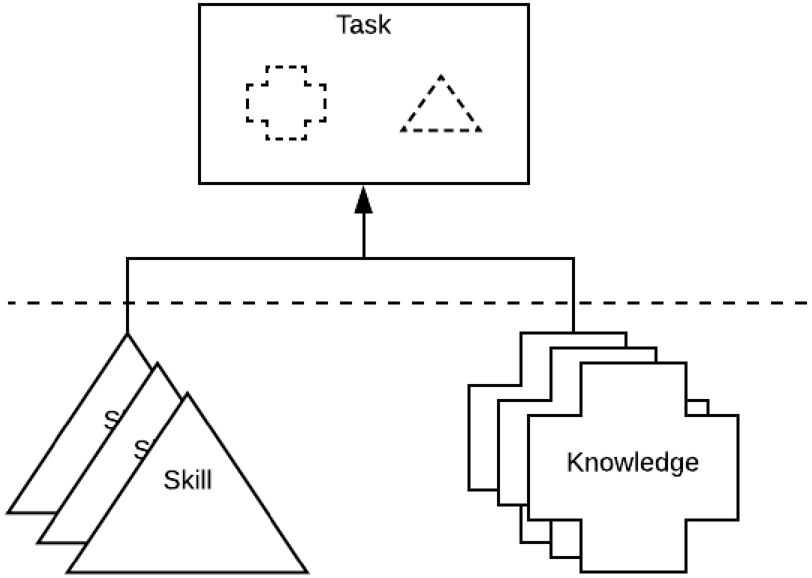
Maureen Roskoski
Senior Professional and Corporate Sustainability Officer
Facility Engineering Associates, PC

Workforce Framework for Cybersecurity (NICE Framework)

- ✓ Establishes a common, consistent lexicon to clearly share information about cybersecurity work
- ✓ Provides direct information about what a workforce needs to know
- ✓ Enables the establishment of regular processes

Building Blocks Approach

TKS Statements: NICE Framework Building Blocks



Using the NICE Framework: Building Block Applications

TEAMS

- Defined by Competencies or Work Roles

COMPETENCIES

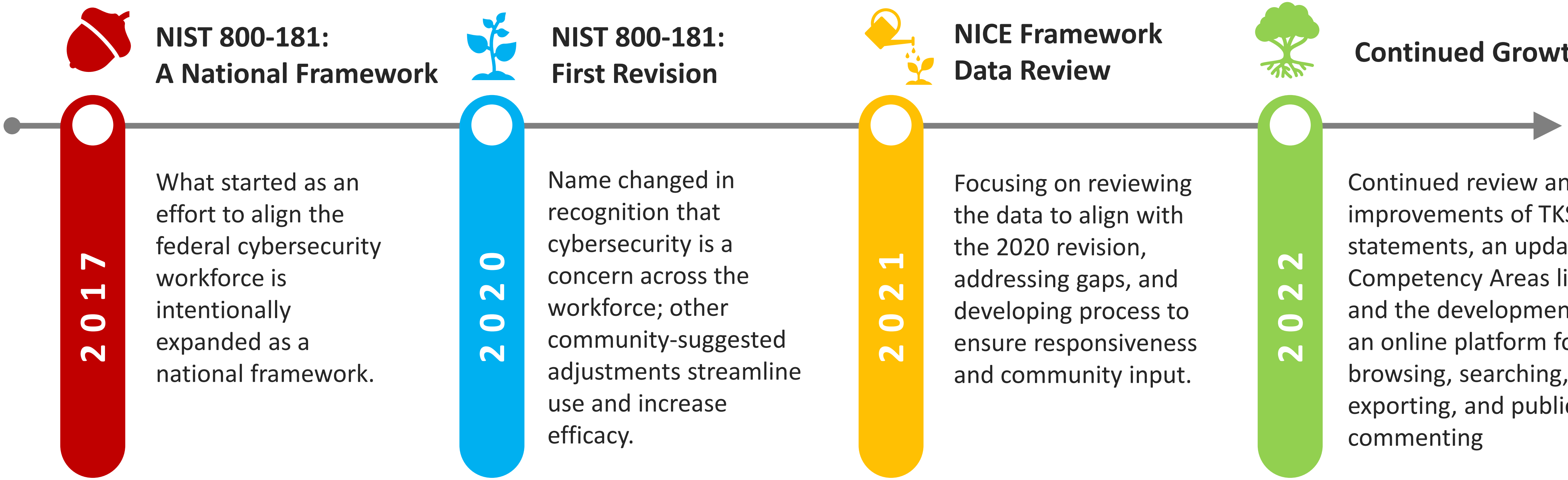
- Groupings of TKS
- Means of assessing a learner

WORK ROLES

- Groupings of Tasks
- Work someone is responsible for

Visit the NICE Framework Resource Center: nist.gov/nice/framework

NICE Framework Evolution



2017

NIST 800-181: A National Framework

What started as an effort to align the federal cybersecurity workforce is intentionally expanded as a national framework.

2020

NIST 800-181: First Revision

Name changed in recognition that cybersecurity is a concern across the workforce; other community-suggested adjustments streamline use and increase efficacy.

2021

NICE Framework Data Review

Focusing on reviewing the data to align with the 2020 revision, addressing gaps, and developing process to ensure responsiveness and community input.

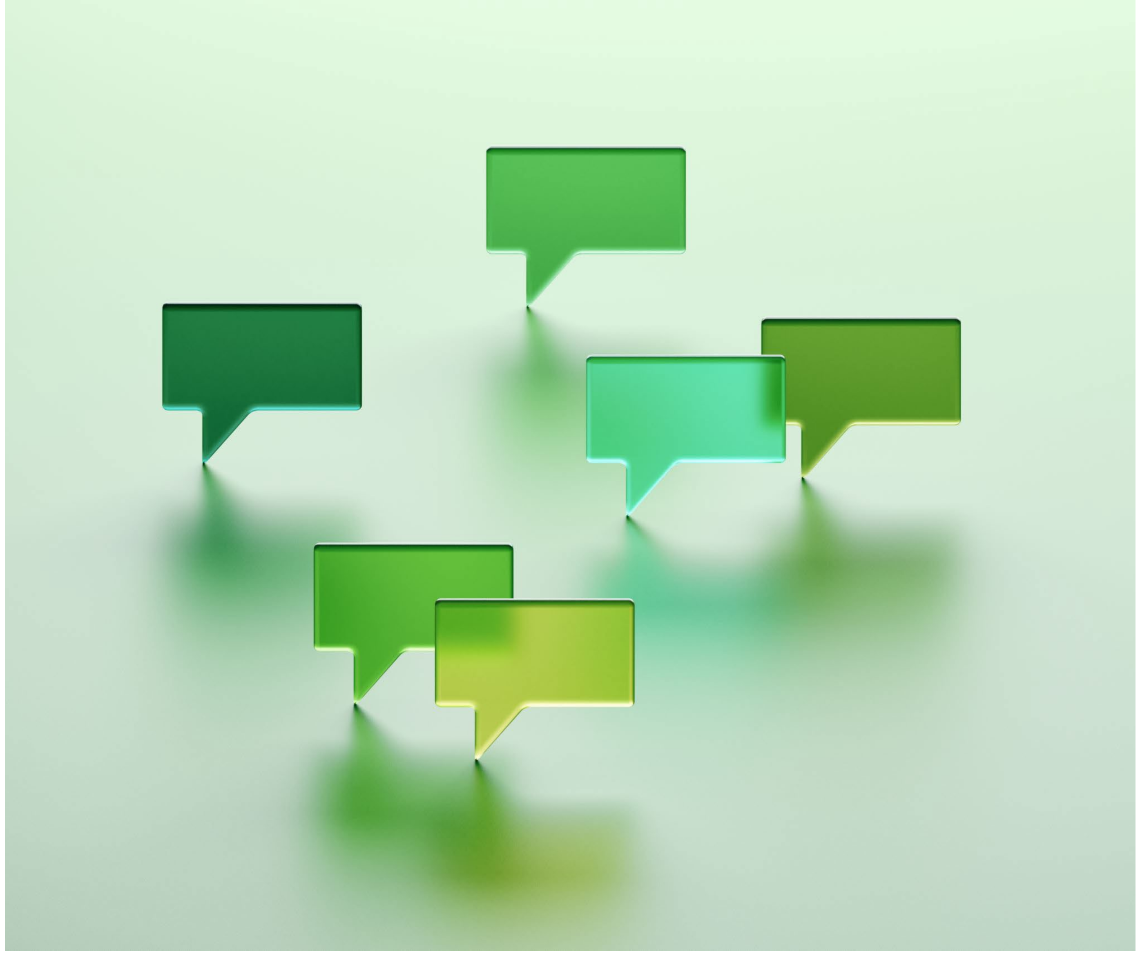
2022

Continued Growth

Continued review and improvements of TKS statements, an updated Competency Areas list, and the development of an online platform for browsing, searching, exporting, and public commenting

Call for Comments: Knowledge and Skill Statements

https://www.nist.gov/news-events/news/2022/04/updated-nice-framework-knowledge-and-skill-statements-public-comment



Adjustments address:

- Alignment with TKS Authoring Guide principles
- Unnecessary redundancies or duplicates
- Inconsistent and unclear language

Comment deadline:

11:59pm ET on June 3, 2022

Send comments to:

NICEFramework@nist.gov

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Lightning Rounds

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

Data Scientist Occupation

April Davis

Director

Classification & Assessment Policy, Talent Acquisition & Workforce Shaping, Employee Services,
U.S. Office Of Personnel Management

FEDERAL CYBERSECURITY WORKFORCE SUMMIT

United States Digital Corps Program

Caitlin Gandhi

Program Lead

U.S. Digital Corps, U.S. General Services Administration

Program Overview

Federal Cybersecurity Workforce Summit

April 26, 2022

UNITED STATES
DIGITAL CORPS

US Digital Corps Overview

The U.S. Digital Corps was **launched in August 2021 by the Biden-Harris administration** and is operated by GSA’s Technology Transformation Services (TTS).

It is a two-year fellowship for early-career technologists to work in government with a path to career positions—with the goal of building a deep, sustainable tech talent pipeline for federal agencies.

UNITED STATES
DIGITAL
CORPS

CROSS-GOVERNMENT SUPPORT

The U.S. Digital Corps is aligned with key Administration priorities and championed by senior agency leaders:

"The Digital Corps offers technologists just starting out in their career the opportunity to make government work better for the American people." – **GSA Administrator Robin Carnahan**.

"The U.S. Digital Corps is a forward-looking solution that will meet the Biden Administration's goals of advancing federal IT and cybersecurity." – **Clare Martorana, Federal Chief Information Officer**

"OPM is excited to support the U.S. Digital Corps as one facet of the Biden-Harris Administration's commitment to rebuilding, reenergizing, and diversifying the federal workforce." – **Kiran Ahuja, OPM Director.**

BROAD IMPACT

ADMINISTRATION PRIORITIES

- President’s Management Agenda
- American Rescue Plan {COVID-19, economic recovery, racial equity, technology modernization}
- Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce
- Executive Order on Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats
- National Security Memorandum on Revitalizing America’s Foreign Policy and National Security Workforce, Institutions, and Partnerships

ADVANCING EQUITY

REVITALIZING THE FEDERAL WORKFORCE

ACCELERATING DIGITAL SERVICES

ATTRACTING CYBER & AI TALENT

PROGRAM OVERVIEW

New **two-year fellowship for junior technologists in the fields of software engineering, cybersecurity, design, product management, and data science & analytics**

- Focus on highly skilled, early-career, diverse talent
- Fellows work on high-impact technology projects at host agencies
- Opportunity for career conversion & permanent placement at host agency
- U.S. Digital Corps program leads centralized recruitment and selection in collaboration with host agencies.
- 40+ fellows expected to begin work at 10+ agencies in June 2022
- At scale, **hundreds or thousands of Fellows per year** hired directly at host agencies.

FELLOW EXPERIENCE

The Digital Corps will be many Fellows' first experience in the federal government, if not the workforce entirely. During the two year program, dedicated, centralized program staff at GSA will support Fellows through:

ORIENTATION

LEARNING & DEVELOPMENT

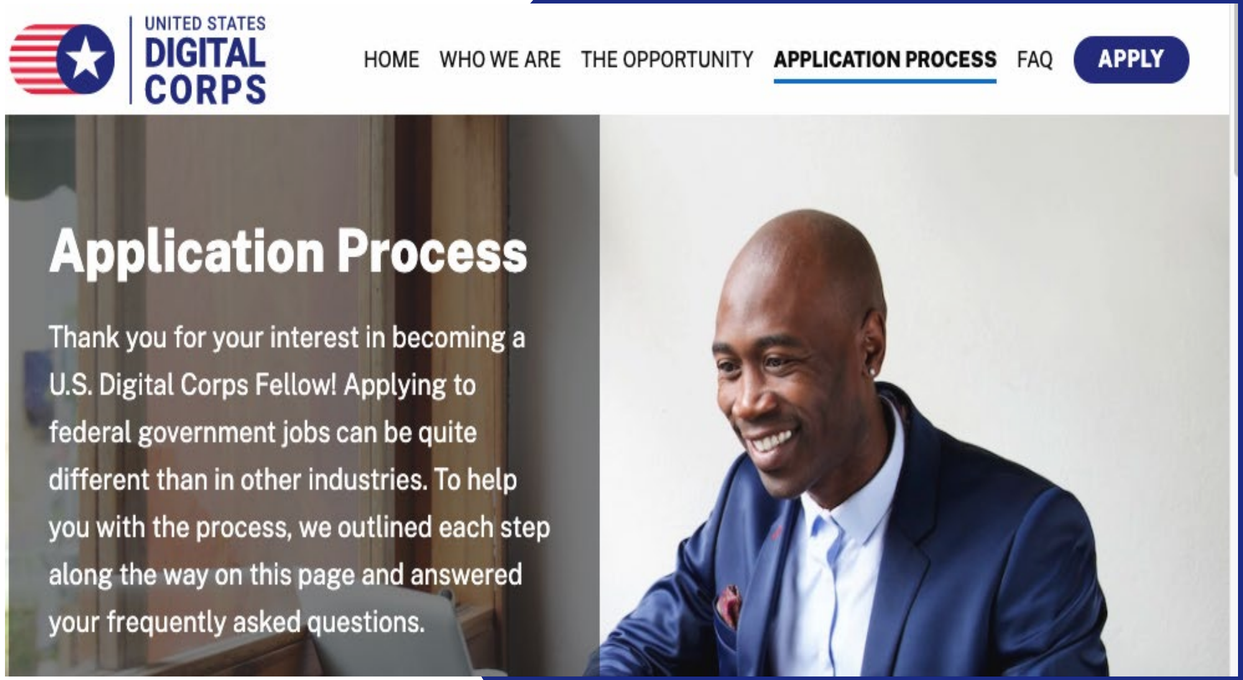
MENTORSHIP

COHORT COMMUNITY

INAUGURAL COHORT

Applications were open from November 8-15:

- 2210 positions @ GS-9 (career ladder to GS-12)
- Remote-first placements
- $82,000+ minimum compensation in Washington D.C. *with recruitment incentive*
- Pathways Recent Graduates authority offers permanent career conversion
- Using SME-QA for qualification



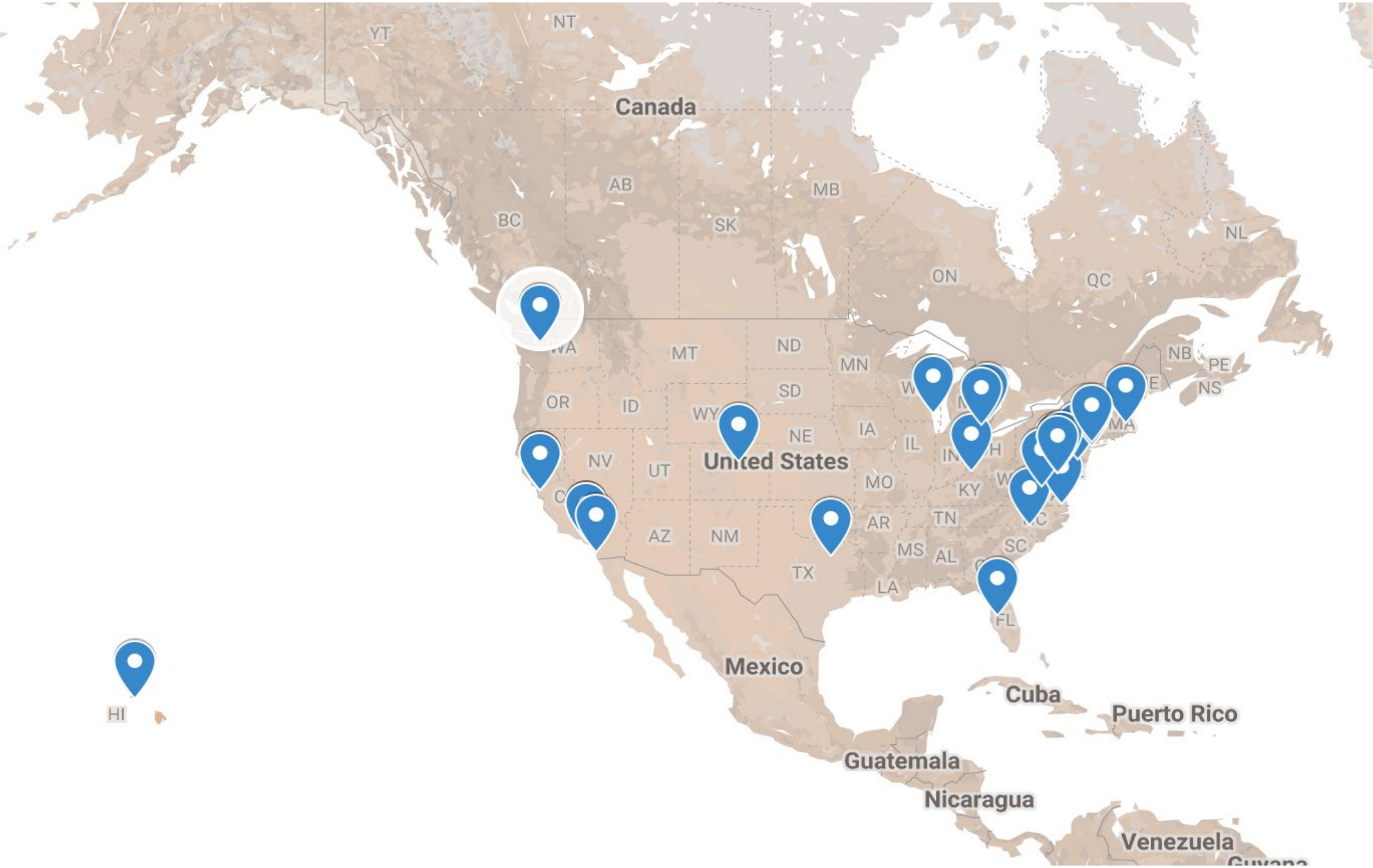
Application Process

Thank you for your interest in becoming a U.S. Digital Corps Fellow! Applying to federal government jobs can be quite different than in other industries. To help you with the process, we outlined each step along the way on this page and answered your frequently asked questions.

⇒ 1,085 applicants in only 7 days

⇒ diverse & representative applicant pool

ONBOARDING CANDIDATES



Informal snapshot:

- 39* issued offers as of 4/15
- 18 states and territories
- 64% will work remotely (*75% of those who had an option chose remote*)
- Approx. 50/50 undergrad vs. grad experience

* and counting…

AGENCY PARTNERSHIP

- ➔ **Requests for 160+ Fellows** from 70 submissions across federal government
- ➔ Prioritized based on:
  - ◆ **Potential for impact**
  - ◆ **Mature technical teams**
  - ◆ **Commitment to Fellow learning & growth**
- ➔ Placing at 13+ agencies in June 2022
- ➔ Aiming for 80+ Fellows / placements in June 2023

Partners shared publicly to-date

2022 Fellows will have impact in …

- **Climate**
- **Customer experience**
- **Cybersecurity**
- **Economic recovery**
- **Equity**
- **Healthcare**
- **Immigration**
- **Open innovation**
- **… and so much more**

LEARNINGS

TALENT

- Interest is high, particularly among people from diverse backgrounds
- Talent is incredibly strong - capable of qualifying at GS-9+

HIRING

- Mechanisms are slow and negatively affect candidate experience, but can be mitigated against - with dedicated effort
- Current policies limit matriculation of our core target talent pool

AGENCY CONDITIONS

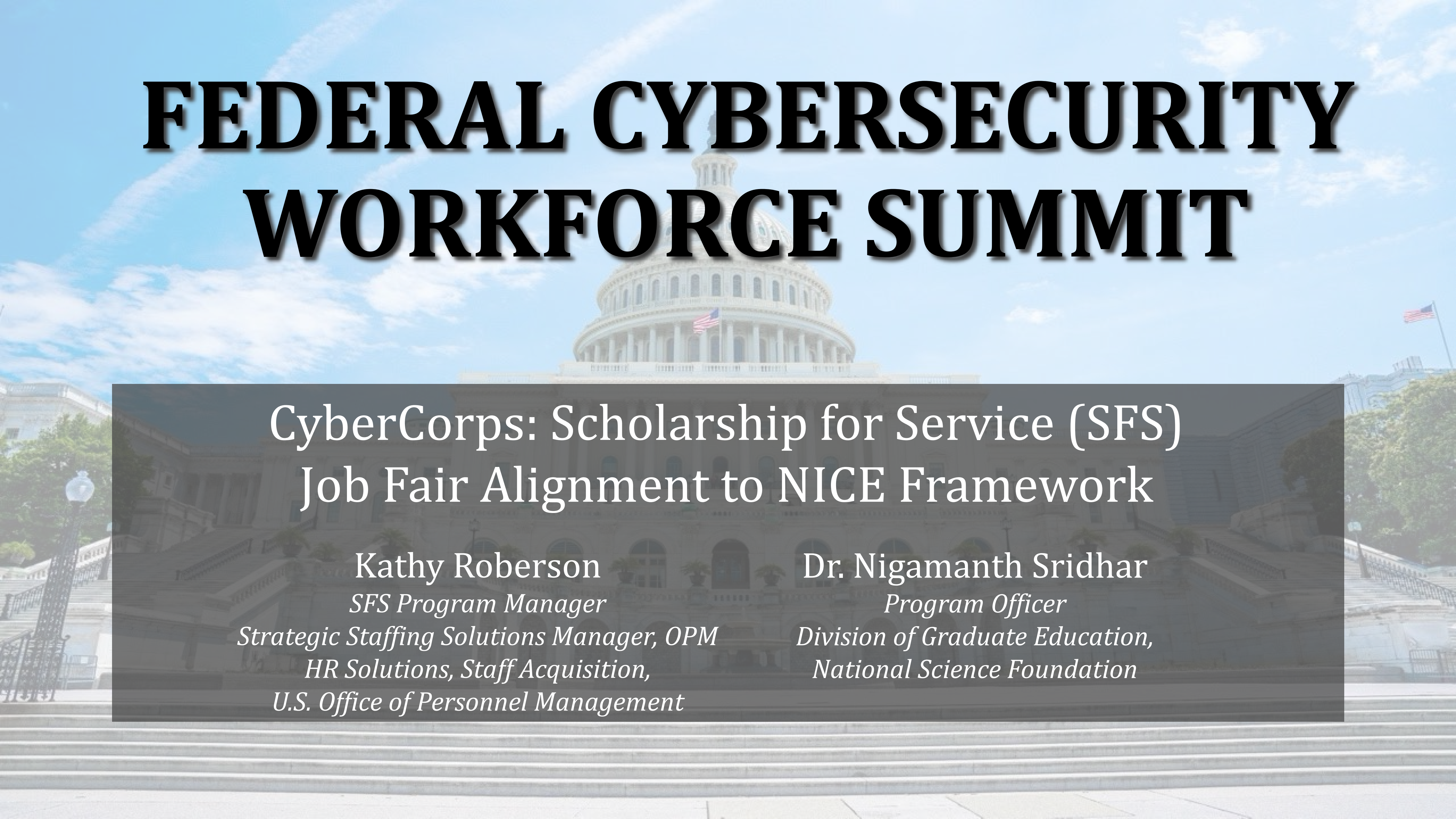
- Agency demand for early GS-level support is incredibly high
- Centralizing core hiring functions alleviates agency burden
- Program participation is limited to well resourced agencies

UNITED STATES
DIGITAL
CORPS

Visit: digitalcorps.gsa.gov

Email: usdigitalcorps@gsa.gov

Follow: @USDigitalCorps



FEDERAL CYBERSECURITY WORKFORCE SUMMIT

CyberCorps: Scholarship for Service (SFS) Job Fair Alignment to NICE Framework

Kathy Roberson
SFS Program Manager
Strategic Staffing Solutions Manager, OPM
HR Solutions, Staff Acquisition,
U.S. Office of Personnel Management

Dr. Nigamanth Sridhar
Program Officer
Division of Graduate Education,
National Science Foundation

CyberCorps® Scholarship For Service (SFS)

The CyberCorps (R): Scholarship For Service (SFS) is managed by National Science Foundation, in collaboration with the U.S. Office of Personnel Management, the Department of Homeland Security and, in accordance with the Cybersecurity Enhancement Act of 2014 (Public Law No: 113-274), as amended by the National Defense Authorization Act. These initiatives reflect the critical need for Information Technology (IT) professionals, industrial control system security professionals, and security managers in Federal, State, local and tribal governments.

CyberCorps®: SFS Mission and Structure

- Seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society.

- Provides funds to colleges and universities to award scholarships to students.

CyberCorps®:SFS Scholarship

Scholarship

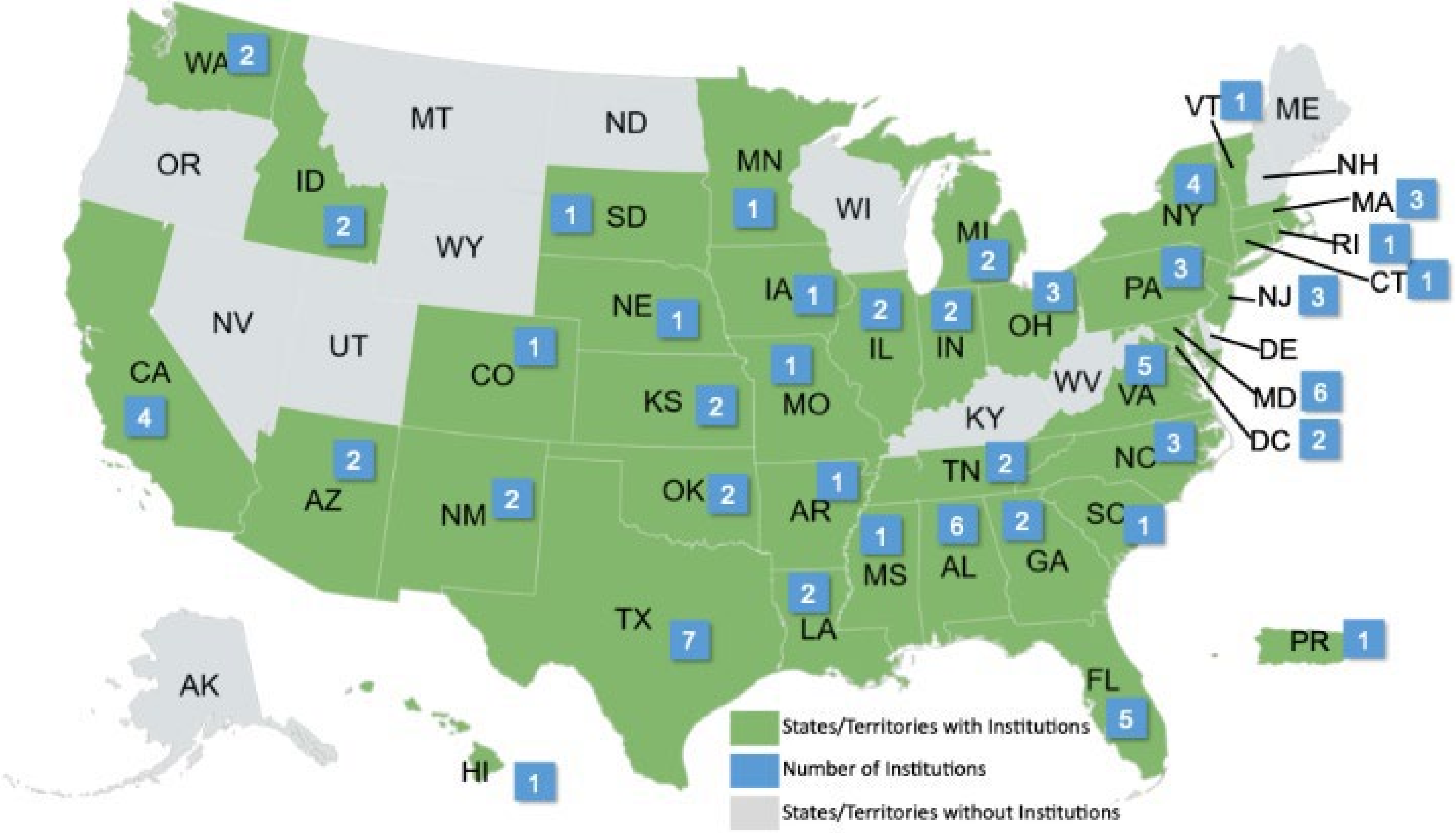
- Funding: tuition, fees, and stipends ($25K/$34K per year)
- Length: 1-3 years
- Obligation: Summer internship, post-graduation service requirement

Eligibility

- Citizen or lawful permanent resident of the United States
- Full-time student within three years of graduation with a bachelor’s or master’s degree in a coherent formal program focused on cyber security; or a research-based doctoral student
- A community college student at an SFS Community College Cyber Pilot (C3P) awardee institution pursing an associates degree or specialized certification in the field of cybersecurity; AND already have a bachelor's degree or are a veteran of the Armed Forces.
- Eligible for government employment (must be able to acquire security clearance)
- Awardee institutions set additional selection criteria

CyberCorps®: By the Numbers

- Over 4,700 scholarships awarded since 2001
- 92% placement rate in more than 140 federal/state/local tribal agencies and FFRDC/national labs
- 99 participating universities
  - 39 states, DC, and Puerto Rico (see list at https://www.sfs.opm.gov/contactsPI.aspx)
  - 19 Minority Serving Institutions
  - 28 community colleges that participate as a partner with a CyberCorps® university
- Over 750 currently in school
- Over 350 will graduate in 2022
- Surveys show that over 64% of graduates stay with the government beyond their obligation


WA 2
MT
ND
VT 1
ME
OR
ID 2
MN 1
NH
MA 3
SD 1
WI
NY 4
WY
MI 2
RI 1
IA 1
CT 1
NE 1
IL 2
IN 2
OH 3
PA 3
NJ 3
NV
UT
CO 1
DE
CA 4
KS 2
MO 1
WV
VA 5
MD 6
KY
DC 2
AZ 2
NM 2
OK 2
AR 1
TN 2
NC 3
MS 1
AL 6
GA 2
SC 1
TX 7
LA 2
PR 1
AK
FL 5
HI 1
🟩 States/Territories with Institutions
🟦 Number of Institutions
⬜ States/Territories without Institutions

Education Level and Fields of Study

- Most Common degree is a Master’s (53%), followed by a Bachelor’s (39%), Ph.D (4%), and Associate’s (4%)
- 74% graduate with a GPA of 3.6 or higher
- Over 60 different areas of study

Common Areas of Study

Computer Science

Computer Engineering

Computer Forensics

Computer & Network Security

Computer Information Systems

Cybersecurity

Information Assurance

Information Security

Uncommon Areas of Study

Accounting

Business Administration

Law/JD

Forensics

Political Science

Computer Criminology

Telecommunications

Wireless Software Engineering

Occupations

Any position related to cybersecurity at an approved organization.

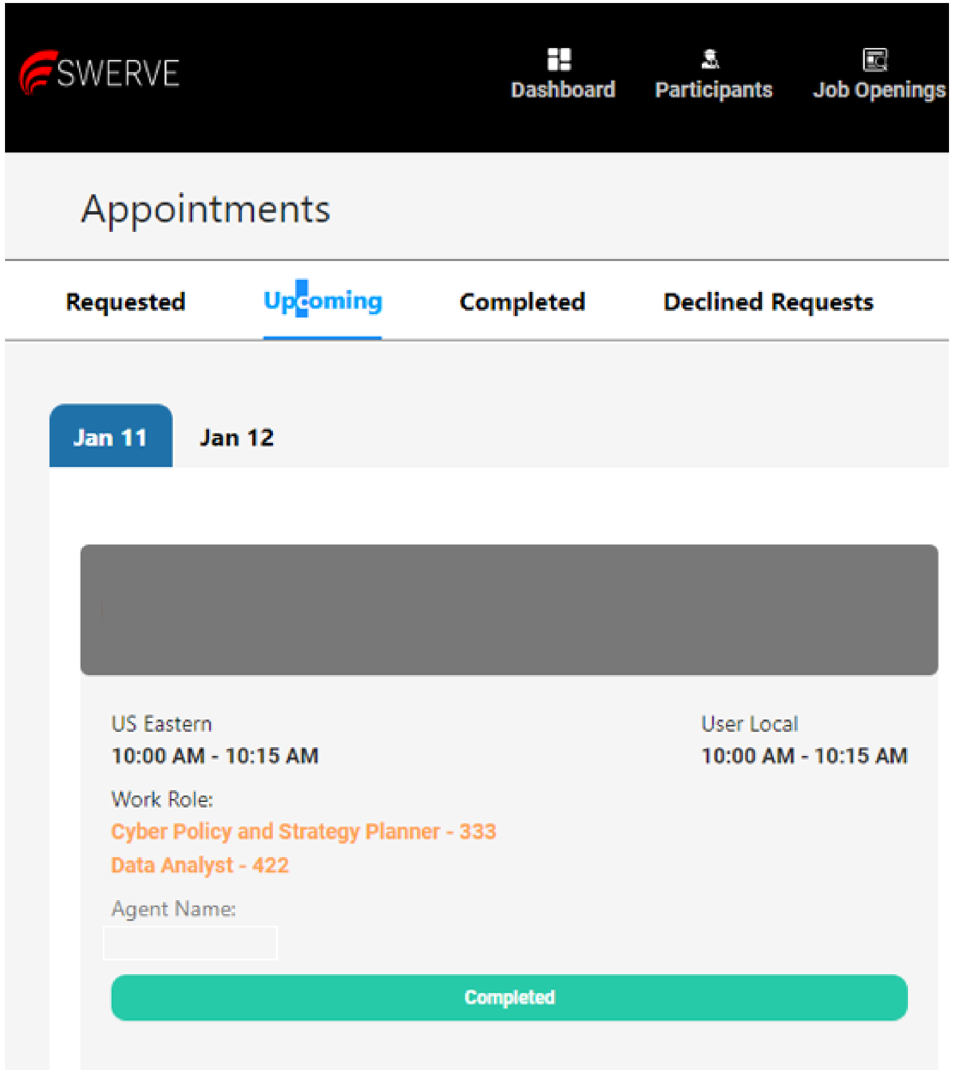
- Accountant (Cyber)
- Attorney (Cyber)
- Analyst
- Computer Scientist
- Computer Science-Cryptography
- Engineer
- Forensics
- Information Security Analyst
- Information Assurance
- Information Technology
- Information Security Officer
- Policy
- Network Security Analysts
- Research and Development
- Security Operations Analyst
- Software Vulnerability Analyst
- Systems Security Designer
- Technology Security Designer
- Telecommunications
- Threat Analyst
- Vulnerability Analyst
- Wireless Security

CyberCorps®: SFS – Recruitment/Hiring Events

- Annual Virtual job fair in October/November
  - Aligns with NICE Framework
  - Over 50 agencies represented
  - Over 300 participants
  - Set up on demand or prescheduled appointments
- Annual In-Person job fair in the Washington, DC, area in early January
  - Aligns with NICE Framework
  - Over 90 agencies represented
  - Close to 500 participants
  - Open interview areas
  - Private interview areas

SFS Job Fairs & NICE Framework

- Work Roles with definitions added to virtual platform
- Participants can identify which work roles they are interested in
- Agencies can identify which work roles they are recruiting for
- Agencies can search participant profiles to identify participants with specific work roles.



US Eastern
10:00 AM - 10:15 AM

User Local
10:00 AM - 10:15 AM

Work Role:
Cyber Policy and Strategy Planner - 333
Data Analyst - 422

Agent Name:

DHS CISA Use of Work Roles

Allowed us to Schedule interviews quicker

Aligned candidates with Work Roles

Used work roles to build positions in platform

Made sorting through the 600+ candidates much easier!

CyberCorps®: SFS – Hiring SFS Students

Cybersecurity Enhancement Act, Public Law 113-274, Sec. 302e

– SFS participants appointed in the excepted service
  - Internships
  - Post graduation appointments

– Upon fulfillment of the service term, may be converted noncompetitively to term, career-conditional, or career appointment
  - Must have been appointed under this PL to be eligible for conversion

CyberCorps® Scholarship For Service (SFS)

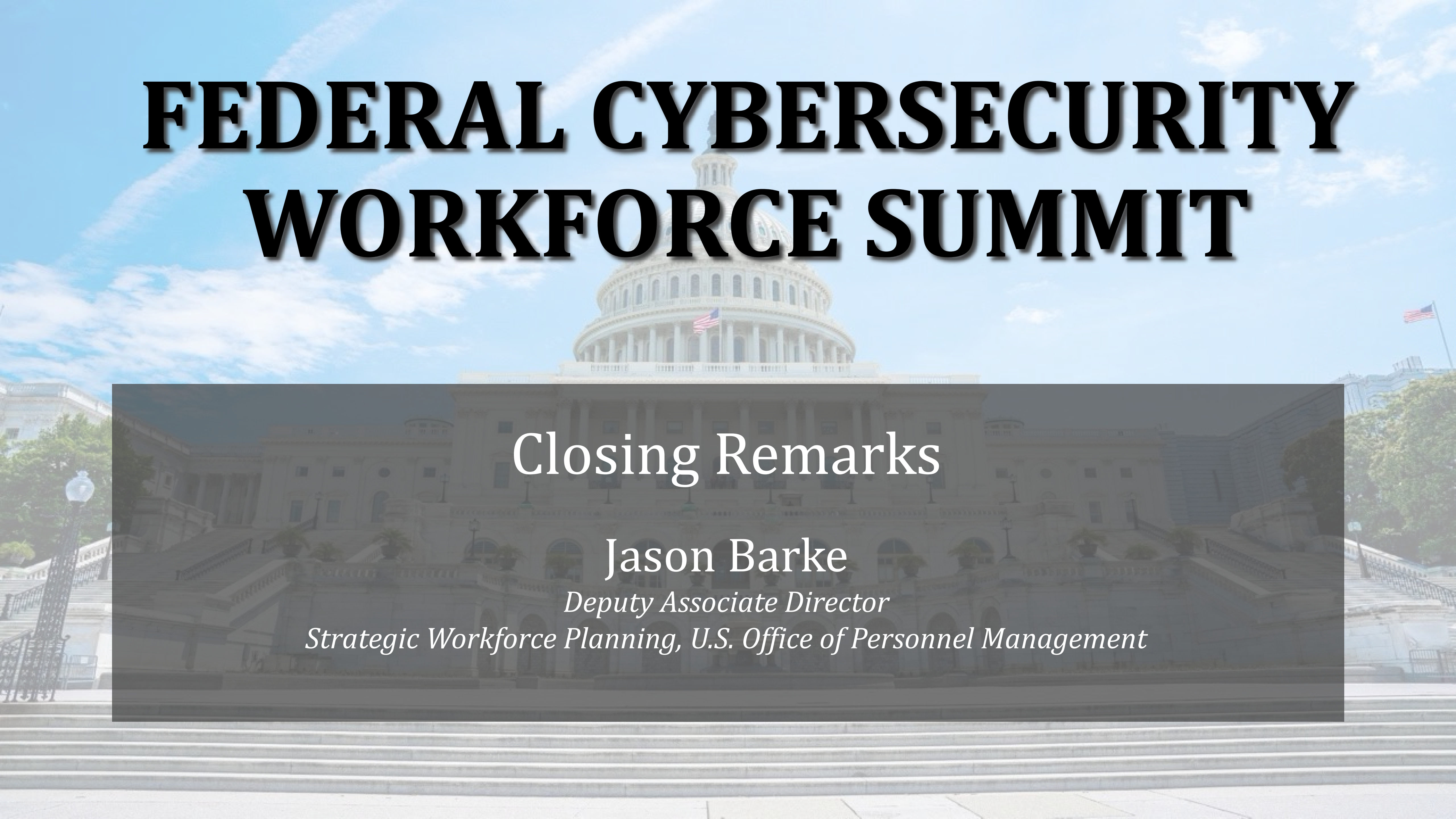
Stephanie Travis, OPM
SFS Program Office Rep
(202) 579-4951

Kathy Roberson, OPM
SFS Program Manager

Email: sfs@opm.gov
Phone: (816) 541-8103
Website: sfs.opm.gov

Sandra Cyphers, OPM
SFS Program Office Rep
(202) 706-8367

FEDERAL CYBERSECURITY WORKFORCE SUMMIT



Closing Remarks

Jason Barke

Deputy Associate Director
Strategic Workforce Planning, U.S. Office of Personnel Management

2022 Federal Cybersecurity Workforce Webinar Series

Tuesday, July 26, 2022, 1:30-3:00 p.m. ET

“Employee Development Through Rotational and Exchange Programs”

Register here: https://go.usa.gov/xuNpY

Tuesday, October 25, 2022, 1:30-3:00 p.m. ET

Topic to be determined

2023 Federal Cybersecurity Workforce Summit

SAVE THE DATE

Tuesday, April 25, 2023

Federal Cybersecurity Workforce Summit Survey

Don’t forget to submit an evaluation form!

https://www.surveymonkey.com/r/CQRMKFR