State of the Federal Cyber Workforce

A Call for Collective Action

LEADERS. PARTNERS. INNOVATORS.

Federal Cyber Workforce Management and Coordinating Working Group

September 2022

The Federal Cyber Workforce Challenge

Like a zero-day attack, the COVID-19 pandemic exposed the potential weaknesses of our Nation's digital and critical infrastructures, including our data centers, networks, healthcare system, food supply, financial services, and energy sectors.

The rapid shift to remote work, cloud-based infrastructures, the Internet of Things (IoT), and a geographically dispersed hardware and software supply chain have created a drastically expanded attack surface with inadequate security check points and safeguards. Combined with the appeal of the online ecosystem as a source for financial gain by cybercriminals, political influence by hacktivists, and espionage by nation-states, it's no surprise that COVID-19 has been linked to a 238% increase in cyber attacks[1].

The pandemic has also intensified the need to enhance and deliver digital government services with greater efficiency, security, and accessibility. Millions of people use and rely on the Federal Government's digital services during the most critical times in their lives, from locating a COVID-19 testing site, passing a security checkpoint, or claiming retirement benefits.

With these growing cyber and digital transformation needs, the introduction of new cyber technology and tool stacks alone will not stop each breach and protect our nation – our talent defenses must also be updated to match the emerging challenges.

DIGITAL GOVERNMENT AND THE CYBER THREAT LANDSCAPE

In 2021, an average of 2,215 cyberattacks occurred per day and cybercrime cost Americans a staggering $4.2 billion in losses. In the first quarter of 2022, U.S. government websites had more than 5.6 billion visits.[2]

Systemic changes to the development of our cyber workforce are vital for our nation to sufficiently govern and maintain our critical infrastructures and data security.

The federal workforce must be ready to counter the increasing threat of cyberattacks while also meeting the demand of U.S. citizens for a more responsive, digital government.

Now more than ever, it is essential that we expand our cyber workforce with diverse roles and develop talent to securely build, operate, and maintain our digital and critical infrastructures and protect and defend our data against cyber adversaries at home and abroad.

The following report details chronic workforce challenges faced by federal agencies trying to minimize the cyber workforce gap and build outstanding talent; and how with a coordinated, interagency approach, the Federal Government can break down barriers and empower agencies to recruit, develop, and retain a world-class cyber workforce.

[1] World Economic Forum - Global Technology Governance Report 2021

[2] Hackers Attack Every 39 Seconds; FBI:Surge in Internet Crime Cost Americans $4.2 Billion; Digital Analytics Program (DAP)

The Federal Cyber Workforce Management and Coordinating Working Group

Overview and History

Established in 2019, the Federal Cyber Workforce Management and Coordinating Working Group (Working Group) is an interagency coordinating body that collaborates on common cyber workforce challenges in the digital era by enhancing workforce management capabilities and reducing siloed efforts. Sponsored by the Federal Chief Information Officer and Chief Human Capital Officer Councils, the Working Group is comprised of **24 federal departments and agencies** and consists of over **250 workforce management professionals, human resource specialists, and cyber hiring managers**; who are on the ground and supporting over **90,000 federal employees performing Information Technology (IT), cybersecurity, and cyber-related functions**.

Centered by the tenet of “do once, help many,” the Working Group promotes the Federal Government’s collective talent defenses by devising strategy and actions to tackle workforce recruitment, development, and retention challenges head-on. Leveraging skills, passion, and partnership amongst its members while also forging new relationships across government, the Working Group rapidly develops and implements solutions to shared challenges to enhance the strength and maturity of the entire federal cyber workforce.

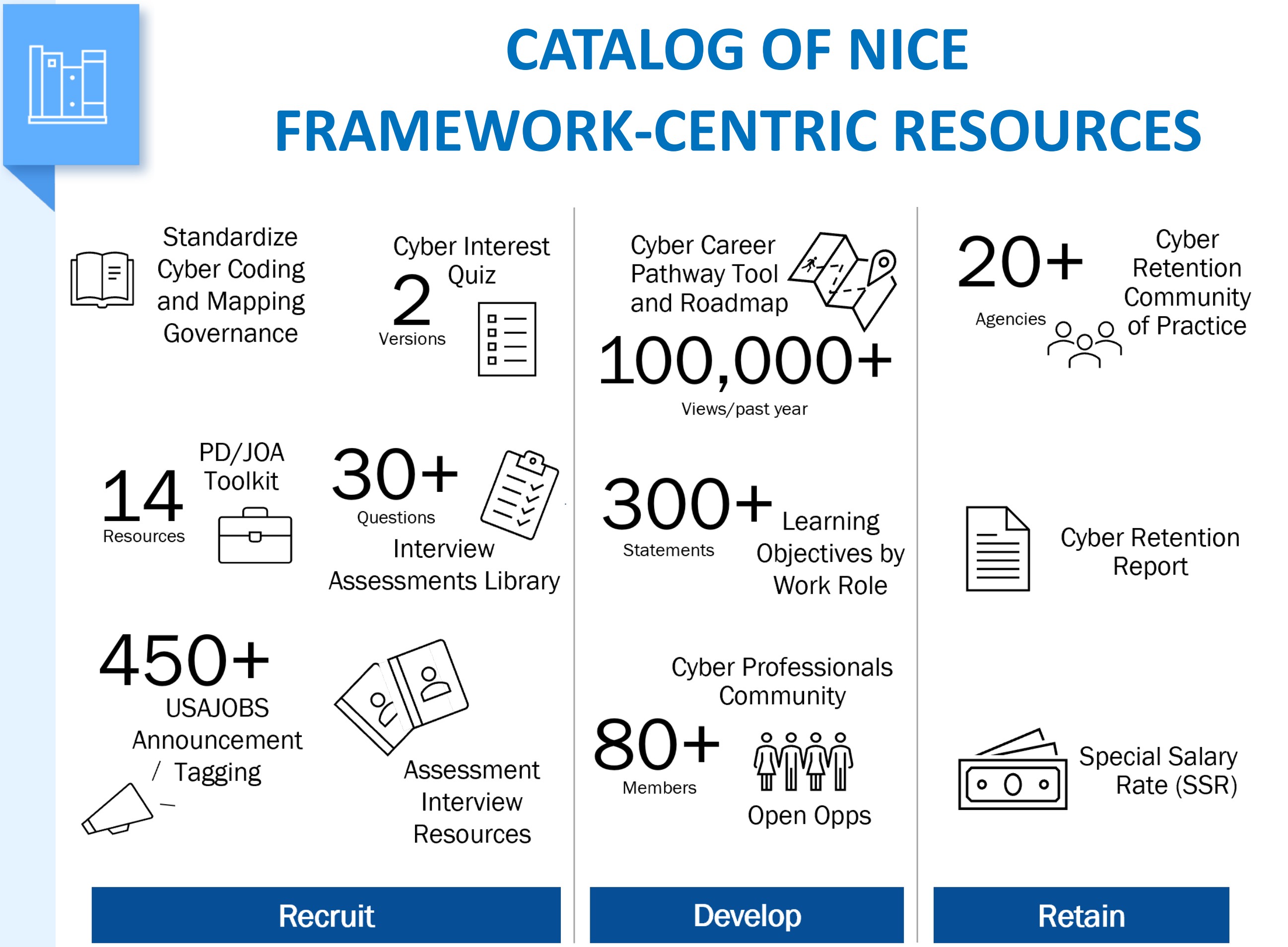
Tri-Chair Leadership

Federal Departments and Agencies

The Federal Cyber Workforce Management and Coordinating Working Group, Cont.

Progress and Accomplishments

Under its model of collective action, Working Group members are pushing the envelope of what's possible and creatively navigating limitations within existing federal policy, process, and personnel constructs. In the past two years, the Working Group has developed and released a catalog of National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework)-centric products, services, and tools to increase understanding and application of the NICE Framework into existing workforce management practices (see **Figure 1**).



CATALOG OF NICE FRAMEWORK-CENTRIC RESOURCES

Recruit

Standardize Cyber Coding and Mapping Governance

Cyber Interest Quiz
2 Versions

14 Resources
PD/JOA Toolkit

30+ Questions
Interview Assessments Library

450+ USAJOBS Announcement / Tagging

Assessment Interview Resources

Develop

Cyber Career Pathway Tool and Roadmap
100,000+ Views/past year

300+ Statements
Learning Objectives by Work Role

Cyber Professionals Community
80+ Members
Open Opps

Retain

20+ Agencies
Cyber Retention Community of Practice

Cyber Retention Report

Special Salary Rate (SSR)

Figure 1. NICE Framework-centric Resources

This catalog equips workforce management professionals, Human Resource (HR) specialists, and hiring managers with the knowledge and tools needed to integrate the NICE Framework into existing approaches for identifying, recruiting, developing, and retaining a skilled, diverse, and resilient cyber workforce. For additional information, refer to the Appendix.

Roles Within the Federal Cyber Workforce

The Cyber Workforce is occupationally cross-cutting, multi-faceted, and comprises a multitude of functionally diverse work roles. Cyber practitioners design, build, secure, operate, protect, and defend the data, systems, and networks that our digital economy and way of life depend on.

Cyber practitioners are not just technical operators conducting offensive and defensive actions from behind a wall of screens. They also perform roles within traditional as well as emerging technology, management, strategy, policy, and intelligence fields, along with cross functional roles that can operate in and amongst multiple communities of skill (see **Figure 2**).

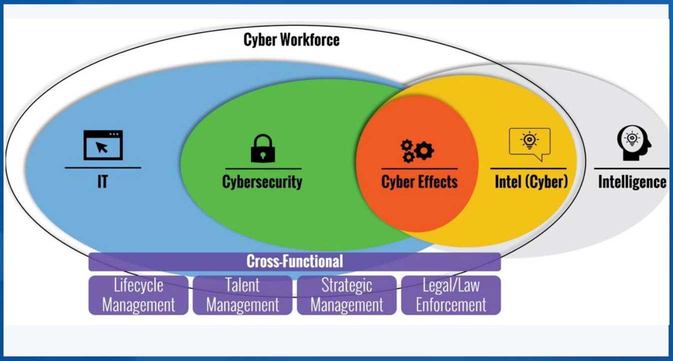


Figure 2. Cyber Workforce Skills Communities

The cyber workforce can be logically depicted by grouping work roles that share similar functions and skill sets into skills communities. To interactively explore these communities, visit the Cyber Career Pathways Tool.[3]

While Federal cyber practitioners are primarily aligned and classified to the 2210 Information Technology Management series, they are also found in over 34 occupational series ranging from 1811 Criminal Investigation, to 391 Telecommunications, to 905 General Attorney, among many others (see **Figure 3**).

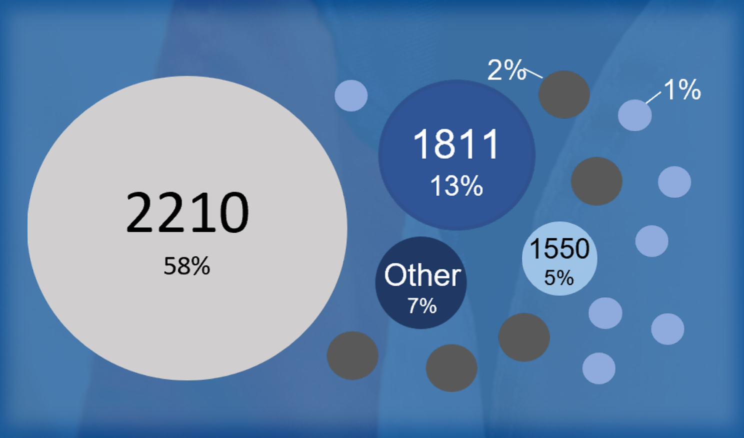


Figure 3. Cyber Practitioner Occupational Series Distribution

2210 – IT Management: 58%
1811 – Criminal Investigation: 13%
1550 – Computer Science: 5%
0391 – Telecom: 2%
0301 – Miscellaneous Admin and Programs: 2%
0132 – Intelligence: 2%
0855 – Electronics Engineering: 2%
0343 – Management and Program Analysis: 2%
0854 – Computer Engineering: 1%
0801 – General Engineering: 1%
0856 – Electronics Technology: 1%
0080 – Security Administration: 1%
0501 – Financial Admin and Programs: 1%
0340 – Program Management: 1%
0335 – Computer Clerk and Assistant: 1%
All **Other** Occupational Series: 7%

The Working Group's aim is to **expand the understanding of roles** included in the cyber workforce and increase awareness of the **breadth of career possibilities** available in the Federal Government to current practitioners and prospective federal employees.

[3] Cyber Career Pathways Tool

Current State of the Federal Cyber Workforce

Today, our federal cyber workforce is stretched thin—less than 6% are under the age of 30, and 30% are 55 or older (see **Figure 4**). Given expected retirements, lack of entry-level and diverse talent, turnover, and the growing need for new skill sets, there is a significant risk to our cyber mission effectiveness and the long-term health of our federal cyber workforce (see **Figure 5**).

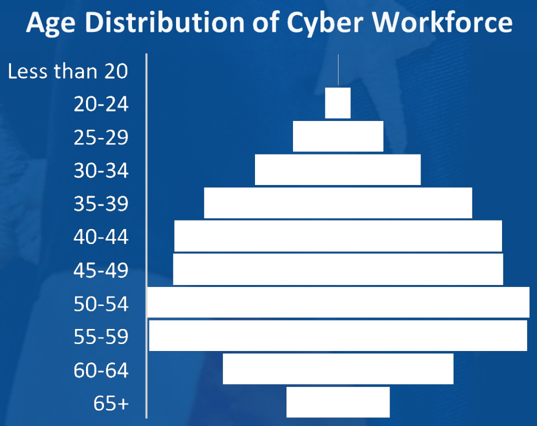
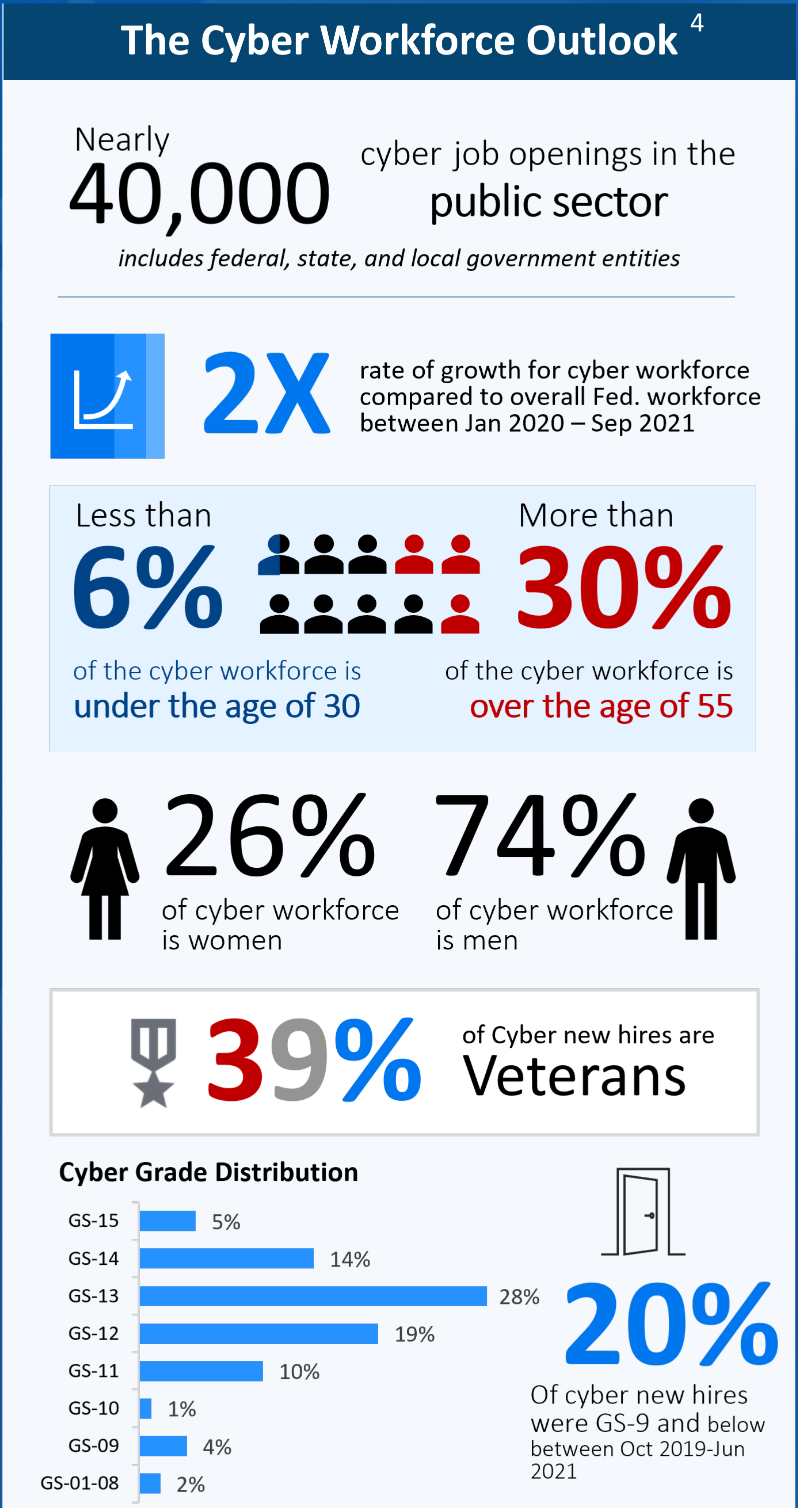


Figure 4. Age Distribution of the Federal Cyber Workforce, CY2021

The need for talent is now.

There are over 700,000 cyber jobs to fill nationwide, and nearly 40,000 are in the public sector[4]. The Bureau of Labor Statistics projects that the cyber job market will "grow 13 percent from 2020 to 2030, faster than the average for all occupations," with some cyber roles, such as information security analyst, growing by as much as 33%[5].



The Cyber Workforce Outlook [4]

Nearly **40,000** cyber job openings in the public sector

includes federal, state, and local government entities

2X rate of growth for cyber workforce compared to overall Fed. workforce between Jan 2020 – Sep 2021

Less than **6%** of the cyber workforce is under the age of 30

More than **30%** of the cyber workforce is over the age of 55

26% of cyber workforce is women

74% of cyber workforce is men

39% of Cyber new hires are Veterans

20% Of cyber new hires were GS-9 and below between Oct 2019-Jun 2021

Figure 5. The Cyber Workforce Outlook

[4] Department of Labor Occupational Outlook Handbook Summary Page for Information Security Analysts

[5] CyberSeek Cybersecurity Supply-Demand Heat Map; Federal Workforce Data; *based on FedScope data (March 2022)*

Filling technical individual contributor positions is difficult, as only 50% of applicants are well qualified for the positions. It's critical that we completely transform how we train and upskill our workforce with a special focus on our human skills and mastery of security controls.

- Information Systems Audit and Control Association (ISACA): State of Cybersecurity 2021

Shared Challenges

Five Shared Challenges Within Three Focus Areas

Do once, help many.

Recognizing Our Shared Challenges

With an almost nonexistent front end to our talent pipeline and a growing workforce age gap, we must take a people first approach to address the challenges preventing us from effectively recruiting, developing, and retaining cyber talent within the federal government. To that end, The Working Group conducted a scan of the federal environment to identify how and why current federal policy, process, and personnel constructs serve as stumbling blocks to agencies in achieving their recruitment, development, and retention goals.

Through numerous one-one-one sessions with agency partners - with representation from workforce management professionals, cyber hiring managers, HR specialists, and learning and development professionals - the Working Group sought answers to the following questions: what are the agency's cyber workforce needs, what's holding them back, and what would enable them to achieve their workforce goals.

The following section of this report details cyber workforce challenges, shared across multiple agencies, that were uncovered during the Working Group's environmental scan.

The Working Group identified five shared challenges within three focus areas:

1 Foundations

Cyber Workforce Policy and Classification
Cyber Workforce Data

2 Development

Entry-Level Cyber Talent
Current Cyber Talent

3 Recruitment and Retention

Cyber Workforce Recruitment and Retention

1 Foundations

Increase the size and diversity of the federal cyber workforce by first introducing more effective workforce policies and classification standards that enable agencies to accurately identify, describe, and track the specific activities, attributes, and qualifications needed by this highly specialized workforce.

The increased accuracy of cyber positions will better inform workforce planning and data analytics. Agencies need flexible tools that can readily identify emerging areas of need and growth, paving the way for data-driven near-and long-term strategies that respond appropriately to the ever-changing cyber domain.

Cyber Workforce Policy and Classification

Introduce cyber-specific workforce policies, classification standards, and qualification requirements. Current workforce policies, classification standards, and qualification requirements are insufficient in supporting the highly specialized nature of cyber work or the rate at which the cyber talent ecosystem evolves.

- The federal government lacks a consistent definition and understanding of cyber. Agencies struggle to identify related positions, their scope, and how to classify and code them to appropriate work roles.
- Current classification standards, like the general schedule (GS)-2200 job family for administrative work in Information Technology, do not encapsulate the breadth and depth of work performed by the federal cyber workforce.
- A lack of cyber-specific federal qualification standards prevents potential candidates from understanding the minimum education, training, credentials, and experience requirements necessary for a position. It also prevents the federal government from building a skilled, professionalized workforce.
- Limited familiarity of the NICE Framework and how to apply it to workforce management practices contributes to ineffective, disjointed approaches to identify, recruit, develop, and retain cyber practitioners.

Cyber Workforce Data

Introduce standard cyber workforce assessments and reporting mechanisms, coupled with centralized analytics to effectively capture accurate, up-to-date data and identify position and skill gap baselines and emerging needs at the agency and federal level. Lack of this data makes it increasingly difficult for the federal government to project the health and maturity of the cyber workforce, forecast near and long-term needs related to carrying out mission critical functions, and develop data-driven recruitment, development, and retention strategies.

- There is minimal data available on the number of vacancies and skill gaps by agency and across the federal government.
- It is challenging to forecast cyber work accurately and the skills needed (at current vs. future state) due to the lack of specificity around standard metrics, data governance, and guidance to follow.
- The absence of centralized analytics and reporting prevents executive leadership from making data-informed strategies to holistically address the entirety of the federal cyber landscape.

2 Development

Cultivate an integrated ecosystem of cyber education, training, and workforce development to strategically build and maintain the skill sets that are necessary and relevant in a rapidly evolving digital ecosystem.

The current constructs for incoming and current cyber professionals will not expeditiously meet the talent shortage and skill gaps. The federal government needs to instill cyber-specific baseline qualifications; offer more alternative ways to land and lead federal cyber jobs; define pathways to promote job mastery and career progression; and create training and developments opportunities to keep skills sharp.

Entry-Level Cyber Talent

Expand the cyber workforce by designing recruitment and development resources and programs that focus on entry talent pools from technical high schools, vocational programs, and other non-traditional avenues. Prioritize creating entry-level cyber positions that will serve as the front-end of the federal cyber workforce talent pipeline. Leadership support is essential to ensure successful implementation and launch of entry talent resources and programs. The lack of support and current structures in place impede the federal government from effectively defining, attracting, and screening candidates for entry-level positions. There needs to be clear career paths ready for entry-level talent to build their careers and skill sets.

- There is limited knowledge and prioritization of alternative pathways and programs to draw in talent from a broad array of educational backgrounds; thereby minimizing targeted recruitment efforts at more junior levels.
- Current education and experience qualification requirements serve as barriers for entry talent, oftentimes resulting in the federal government passing over otherwise qualified talent.
- There are limited tools to evaluate and gauge the technical skills proficiency of candidates, both pre-hire and post-hire.
- There isn't a standardized federal repository or training and development framework, with offerings such as on-the-job training and role-based curricula, to guide new hires in adapting and developing skills specific to their current or desired future position(s).

Current Cyber Talent

Create upskilling opportunities and define potential career paths to promote ongoing employee career development, maintain skillsets necessary for addressing evolving cyber mission requirements, and maintain fluidity within the cyber workforce pipeline. This will enable the cyber workforce to build and maintain adept skill sets to easily mobilize into other high-demand roles and those of emerging need.

- There is limited NICE Framework-aligned training and development available to ensure cyber practitioners receive the right training, for the right role, at the right time.
- There are minimal tools available to identify needed skills and evaluate employee proficiency in those skills; often at times, this results in poor prioritization and use of limited agency training funds.
- There is insufficient career path guidance to help cyber professionals identify, align, and prioritize training and development towards career mobility and growth.
- It is challenging to provide training and development tools and programs to stay at pace with the evolving digital ecosystem.

3 Recruitment and Retention

Focus Area and Challenges

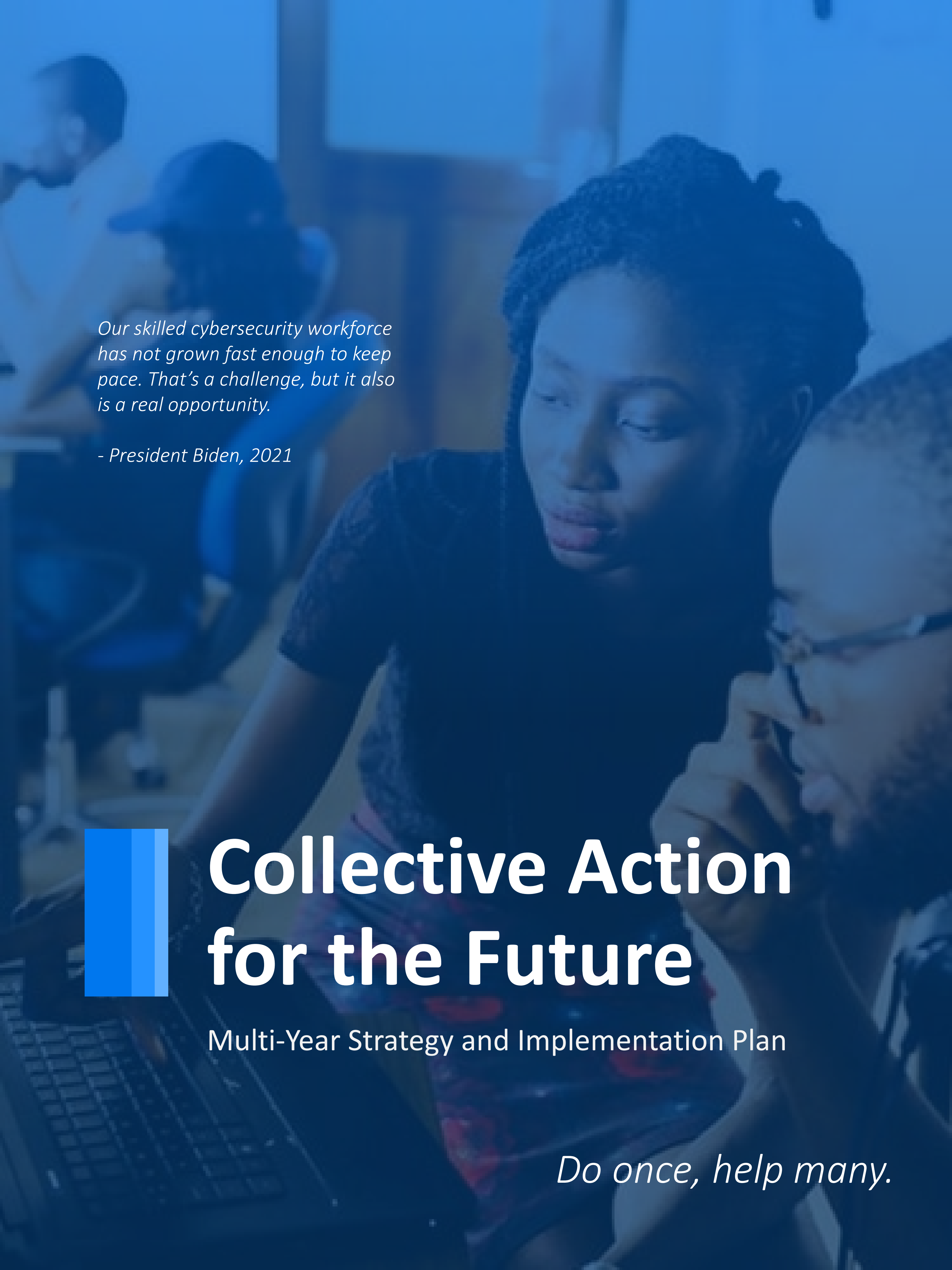
Revitalize and introduce new policies and programs that expand flexibilities revolving around compensation, benefits and rewards, entry qualifications, and workplace environment to improve recruitment and retention of the cyber workforce.

Increasing cyber attacks and a heightened talent shortage serves as a wake-up call that the federal government must reenergize and promote how it is a premier place of employment for cyber professionals.

Cyber Workforce Recruitment and Retention

Offer more competitive compensation, meaningful and challenging work tied to career growth opportunities, and a healthy work culture and environment through targeted recruitment to attract cyber talent to federal service.

- The current constructs do not offer the flexibility needed to effectively recruit and screen candidates that meet qualifications *and* have the right capabilities.
- There is a lack of employee-centric onboarding programs to streamline acculturation of new hires and provide resources necessary for career growth, including opportunities to establish and foster connections within their team, agency, and across the Federal Government.
- There is a gross disparity in pay for federal cyber positions in contrast to the private industry market.



Our skilled cybersecurity workforce has not grown fast enough to keep pace. That’s a challenge, but it also is a real opportunity.

- President Biden, 2021

Collective Action for the Future

Multi-Year Strategy and Implementation Plan

Do once, help many.

Multi-Year Strategy and Implementation Plan

To address the numerous workforce challenges agencies face, we must take a unified and coordinated approach that takes meaningful action to reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize the personal and professional needs of our cyber practitioners.

The Working Group has developed a multi-year strategy and implementation plan in response to identified Core Challenges; the goal of which is, put simply, to lead actions that will yield the highest return – or "move the needle" the most.

Solutions outlined in this report aim to remediate shared challenges impacting the Federal Government's ability to recruit, develop, and retain a world class cyber workforce, by addressing underlying pain points and driving toward a long-term, tangible vision of what's needed for the cyber workforce.

Within the strategy and plan, identified focus areas and their respective challenges are aligned to four workforce domains – each with specific goals, objectives, and solution sets.

Together, they seek to propel the Federal Government forward in realizing the tactical visions that have been created for each workforce domain.

Workforce Domains

1. Cyber Human Resources
2. Cyber Workforce Data
3. Cyber Workforce Development
4. Cyber Workforce Recruitment and Retention

Our Collective Approach

With the support of our 24 agency partners, the Working Group will lead multi-agency action teams that drive high priority, federal wide initiatives resulting in the development of new, NICE Framework-aligned resources. Where possible, the Working Group will seek to accelerate, amplify, and align existing and new federal cyber workforce efforts.

Cyber Human Resources

1

Multi-Year Strategy and Implementation Plan

VISION

Establish a cadre of expert cyber-HR practitioners to equip the HR community, hiring managers, and cyber leaders with the knowledge and resources needed to integrate the NICE Framework into workforce management practices.

GOAL

Promote understanding and application of the NICE Framework to enhance the management and development of the federal cyber workforce.

OBJECTIVES AND SOLUTIONS

PHASE ONE

Objective 1. Standardize the training and education of the HR community, hiring managers, and cyber leaders in applying the NICE Framework to workforce management practices.

Solution 1: Build a Cyber HR Train-the-Trainer program.

Solution 2: Create audience specific playbooks and training materials.

PHASE TWO

Objective 2. Demystify the definition and scope of the cyber workforce to streamline position description (PD) development and its work role-to-position accuracy.

Solution 1: Evaluate PushButton PD effectiveness and define requirements for Version 2.0.

Solution 2: Develop a cyber position-to-work-role coding quiz or tool.

PHASE THREE

Objective 3. Promote CyberCareers.gov as the central hub for federal cyber career resources.

Solution 1: Expand audience specific resources on CyberCareers.gov.

Solution 2: Develop audience specific messaging, media, and outreach campaign.

TRI-CHAIR LEADERSHIP

Solution 1: Partner with key legislative and policy makers to adopt a federal cyber qualifications policy and model (e.g., Department of Defense (DoD) 8140).

Solution 2: Facilitate alignment of NICE Framework knowledge and skill requirements in cyber contracts.

Solution 3: Inform next iteration of the Office of Personnel Management (OPM) Interpretative Guidance for Cybersecurity Positions.

Solution 4: Redefine 'cyber' to address emerging and critical technologies.

Solution 5: Support updates to the 2210 Occupational Series and evaluation of need and feasibility for cyber specific occupational series.

Cyber Workforce Data

2

Multi-Year Strategy and Implementation Plan

VISION

Develop an interactive, federal wide cyber workforce dashboard to enable federal agencies and leaders to deploy data-driven recruitment, development, retention, and workforce planning policies and strategies.

GOAL

Transform cyber workforce reporting and data analytics through standardization of metrics and data management.

OBJECTIVES AND SOLUTIONS

PHASE ONE

Objective 1. Redefine federal cyber workforce reporting requirements to improve data quality and integrity.

Solution 1: Assess and evaluate the current state of cyber workforce reporting.

Solution 2: Develop recommendations to improve reporting and data analytics.

PHASE TWO

Objective 2. Streamline and centralize the collection, analysis, and accessibility of baseline workforce metrics.

Solution 1: Define standard workforce metrics and data sources.

Solution 2: Create a federal cyber workforce dashboard.

PHASE THREE

Objective 3. Establish mechanisms to capture current and future cyber workforce needs and inform workforce policies and strategies.

Solution 1: Develop cyber skills gap analysis tools to forecast needs against emerging trends.

Solution 2: Conduct an environmental scan to identify diversity, equity, and inclusion (DEI) needs within the cyber workforce.

TRI-CHAIR LEADERSHIP

Solution 1: Establish partnership between HRStat community of practice and agency stakeholders to enhance the identification, measurement, and analysis of cyber workforce data.

Solution 2: Standardize integration of cyber workforce metrics and measures into agency human capital operating plans.

Cyber Workforce Development

3

Multi-Year Strategy and Implementation Plan

VISION

Launch a federal cyber academy to centralize training and development for current and future practitioners, aligned to cyber qualification requirements.

GOAL

Modernize cyber career development programs, tools, and resources to improve mobility and skill portability across the federal government.

OBJECTIVES AND SOLUTIONS

PHASE ONE

Objective 1. Streamline skill set development through alignment of career resources to the NICE Framework.

Solution 1: Partner with learning management system content providers (e.g., Skillsoft) to assess and align available training by work roles.

Solution 2: Build an interagency contest and campaign to expand the Cyber Professionals Community on Open Opportunities.

PHASE TWO

Objective 2. Create career guidance mechanisms to facilitate employee development and progression.

Solution 1: Build a career manager program model.

Solution 2: Develop audience specific training materials to adopt and implement the model.

PHASE THREE

Objective 3. Develop skills assessment tools to assess capabilities and gauge proficiency.

Solution 1: Create a skills maturity assessment test plan with supporting materials to pilot.

Solution 2: Pilot skills maturity assessments and gather feedback.

TRI-CHAIR LEADERSHIP

Solution 1: Update Career Pathway Roadmap Tool to produce career individual development plans.

Cyber Workforce Recruitment and Retention

4

Multi-Year Strategy and Implementation Plan

VISION

Establish an end-to-end recruitment and onboarding program to cultivate employee engagement early on and promote growth of a cyber career within the federal government.

GOAL

Position the Federal Government as a competitive employer for incoming and future cyber professionals.

OBJECTIVES AND SOLUTIONS

PHASE ONE

Objective 1. Enhance the candidate screening process with skills proficiency evaluation tools.

Solution 1: Create a test plan and supporting materials to pilot Working Group developed, role-based interview assessments.

Solution 2: Pilot role-based interview assessments and gather feedback for future enhancements.

PHASE TWO

Objective 2. Create a "candidate first" hiring and onboarding process through curated, cohort-based experiences at the onset of the recruitment stage.

Solution 1: Evaluate and re-energize the induction ceremony of the federal cyber orientation program.

Solution 2: Develop a new hire pal program model.

PHASE THREE

Objective 3. Promote awareness of cyber employment opportunities within the federal government and increase diversity through targeted recruitment strategies.

Solution 1: Research recruitment programs and efforts across federal agencies to identify best practices.

Solution 2: Build a targeted, federal wide cyber workforce recruitment campaign.

TRI-CHAIR LEADERSHIP

Solution 1: Develop cyber-specific filters within USAJOBS.

Solution 2: Facilitate Shared Hiring Action(s) for cyber work roles.

Solution 3: Propose a 2210 Special Salary Rate (SSR).

"Without talented cyber professionals working the keyboard, all the cutting-edge technology in the world cannot protect the United States in cyber space. If we do not act now to ensure that our talented and experienced workforce continues to grow, we are leaving our country vulnerable for future cyber attacks."

- Cyberspace Solarium Commission: Growing a Stronger Federal Cyber Workforce

For Policymakers

Recommendations and Considerations

Do once, help many.

Recommendations and Considerations for Policymakers

The need for talent is now, as evidenced by the Working Group's evaluation and cataloging of challenges across the federal landscape. Collectively, we require rapid, comprehensive improvements to our federal recruitment, development, and retention programs and policies. True to the tenant, "do once, help many," the Working Group continues to work collaboratively with agency partners, Councils, and the Executive Office of the President on addressing these needs.

Our multi-year strategy and implementation plan will require agencies to pool their resources to increase working capacity, accelerate efforts, and unify coordination in support of the federal cyber workforce.

However, **our unified federal efforts alone will not be able to address the most fundamental causes behind these challenges** – the lack of a unified national strategy, dedicated resources, and cyber-specific policies.

To help address these areas and more rapidly create the desired future state of the federal cyber workforce, we recommend the following actions:

1. **National Cyber Workforce Strategy**
   The Office of the National Cyber Director (ONCD) should create and implement a National Cyber Strategy that would address the needs of the federal cyber workforce. Through this strategy, ONCD can provide the direction, mandate, and coordination needed to unify efforts and effectively manage the health and welfare of the federal cyber workforce. The Working Group, uniquely positioned in its current role as leaders, partners, and innovators of federal cyber workforce solutions, stands ready to support ONCD in addressing the day-to-day development and operation of Federal cyber workforce programs.
2. **Dedicated Resources**
   The Office of the National Cyber Director, in partnership with agency Chief Financial Officers and the Chief Financial Officers Council, should align appropriated funds to drive implementation of initiatives within the National Cyber Strategy. Policymakers should introduce or support legislation that dedicates funding and resources toward modernizing cyber-specific classification, qualification, and assessment policies; developing centralized workforce analytics and reporting tools; and standing-up a federal cyber training academy to address role-based training and development needs for new and existing practitioners.
3. **Cyber-Specific Policies and Flexibilities**
   The Office of Personnel Management (OPM) should update existing classification, qualification, and assessment policies to address the specialized, evolving needs of the federal cyber workforce and in alignment with the NICE Framework. Federal policymakers should introduce or support legislation that provides agencies with additional, cyber-specific recruitment, hiring, pay, and promotion flexibilities; to include, but limited to, a cyber specific occupational series or cyber excepted service.

Working Group Membership

Members, Partners and Special Thanks

Do once, help many.

Members and Partners

The past and future accomplishments of the Working Group would not be possible without the support and collaboration of the membership of 24 agencies and council partnerships.

MEMBERS

UNITED STATES AGENCY INTERNATIONAL DEVELOPMENT USAID

U.S. DEPARTMENT OF HOMELAND SECURITY

U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA

UNITED STATES NUCLEAR REGULATORY COMMISSION

DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA

DEPARTMENT OF JUSTICE QUI PRO DOMINA JUSTITIA SEQUITUR

DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION U.S.A.

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA ·

UNITED STATES DEPARTMENT OF AGRICULTURE 1862 1889

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

DEPARTMENT OF LABOR UNITED STATES OF AMERICA

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

SMALL BUSINESS ADMINISTRATION 1953

THE DEPARTMENT OF THE TREASURY 1789

GENERAL SERVICES ADMINISTRATION

DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

DEPARTMENT OF STATE UNITED STATES OF AMERICA

SOCIAL SECURITY ADMINISTRATION USA

NSF

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

DEPARTMENT OF VETERANS AFFAIRS UNITED STATES OF AMERICA

PARTNERS

U.S. CYBERSPACE SOLARIUM COMMISSION

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

CLO COUNCIL

CIO COUNCIL

CHIEF HUMAN CAPITAL OFFICERS COUNCIL CHCO COUNCIL UNITED STATES OF AMERICA

Special Thanks

We would like to extend special thanks to members and support staff of the Working Group who have dedicated extra time and effort to continue to go above and beyond the call of duty; each of which has contributed their talents and skills to the greater good of the federal cyber workforce.

Warren Adams
Scott Anderson
Marion Andrews
Selina Arboleda
Jason Barke
Don Bartley
Cynthia Beard
Bill Bodine
Monica Bradley
Norma Brandon
Will Branham
Wendy Brodhead
Katie Burkert
D'Angelo Burks
Patrice Burnett
Mary Calogero
Caitlin Candhi
Megan Caposell
Edgar Carpenter
Christopher Chase
Brenda Chestnut
Deborah Coleman
Marcos Correa
Paul Darmony
April Davis
Alexander Dean
Nicole Diehl
Nicholas Di Mauro
Lewis Dix
John Doggett
Leigha Doherty
Mia Dozier
Gina Fisher
Landa Fox
Pam Frugoli
Brie Gamble
Jonathan Gardner
Anju George
Robert Gettings
Christopher Gojcz
Alan Greilsamer
Jodi Guss
Carrie Hallum
Ann Hannon
Kim Hemby
Richard Hersh
Briana Hila
Kimberly Holden
Shannon Hughes
Matthew Isnor
Lauren Jagtiani
Ilka Johnson
Lisa Johnson
Carey Jones
Jacqueline Jones-Peters
Stephanie Keith
Lance Kelson
Ann Konecky
Tamara Kravitz
Duane Lee
Nancy Limauro
Kevin Luu
Kathy Lyons-Burke
John Malgeri
Shawn Mason
Jenny Mattingley
Sara Mattix
Fernando Menendez
Jessica Merrell
Dylan Mitchell
Keisha Monroe
Marianne Ndekey
Jennifer Nelden
Tina Newell
Mark Nguy
Alba Nunez
Won Palisoul
Christopher Paris
Ryan Petho
Deborah Pierre-Louis
Megan Poore
Maureen Premo
Curtis Rasmussen
Michael Robins
Bianca Robinson
Kevin Sanchez-Cherry
Antoinetta Scott
Robert Sell
Sarah Scholl
Janet Silcox
Will Slack
Antoine Smith
Mark Smith
Gail Sprinkle
Christopher Stenger
Rachel Surick
Kari Szakal
Robert Tagalicod
TJ Thomas
Erika Viola
Edward von Ruess
Erin Weiss Kaya
Wendy Wells
Lemmuel West
Laurie Williams
Clarence Williams
Jasmin Williams
Bernard Wilson
Donovan Wilson
Jennifer Yee
Darla Yoos
Saad Zulgadar

Appendix

Catalog of Cyber Workforce Management Tools and Resources

Do once, help many.

Catalog of Cyber Workforce Management Tools and Resources (1 of 3)

Recruitment	
Standardize Cyber Coding and Mapping Governance (Completed, July 2021)	In partnership with OPM, the Working Group provided recommendations to promote consistent implementation and utilization of cyber coding and mapping by classification personnel and workforce management professionals across the federal government. By revising the current guidance, federal departments and agencies will enhance their processes and practices on how to identify cyber positions; define cyber-related roles and responsibilities; manage cyber-related position issues; recruit, hire, and develop qualified cyber professionals to meet mission needs; implement effective training, performance, and retention programs; and conduct cyber workforce assessments.
Position Description (PD) and Job Opportunity Announcement (JOA) Gold Standards (Completed, October 2021)	The Working Group created gold standard PD and JOA templates, along with how-to guides, to offer guidance to federal departments and agencies on how to incorporate cyber work roles into their existing PD and JOA development processes. Updating the way the federal government describes its PDs and, more importantly, advertises its open positions will attract talent with the right skills to the right positions while also establishing tailored, relevant position criteria.
Work Role-based Interview Assessments Library (Completed, February 2022)	The Working Group developed a repeatable process, along with supporting examples, where federal departments and agencies can leverage the core tasks of cyber work roles to create work role-based interview questions. The set of interview questions can assess applicants' technical capability of performing required tasks of a position. Federal departments and agencies can use tailored, role-specific questions to help determine high qualified applicants based on their task, knowledge, and skill proficiency and whether they should proceed forward in the hiring process. The assessment results provide informal insight on how an applicant will carry out the tasks outlined in the job description.
USAJOBS Announcement Tagging (Completed, May 2021)	In partnership with OPM, the Working Group enhanced the way the federal government advertises announcements for permanent and professional development opportunities related to cyber. The Working Group partnered with USAJOBS to create a special indicator field (SIF) that enables Federal departments and agencies to specify the work roles that support the requirements of the advertised position. With the field, hiring managers, human resource specialists, and potential candidates can quickly locate job opportunities by work roles of interest.
Cyber Career Interest Quiz (In Progress)	In partnership with the Department of Defense and Department of Interior, the Working Group is developing two cyber career interest quizzes that enable individuals interested in pursuing or advancing a Federal cyber career to quickly match personal interests, skills, and experience to relevant cyber work roles. Once matched, individuals will be presented with options to pursue open Federal announcements or professional development opportunities.

Catalog of Cyber Workforce Management Tools and Resources (2 of 3)

Development	
Cyber Career Pathways Tool and Roadmap **(Completed, Aug 2020 and Sept 2021 respectively)**	In partnership with Cybersecurity and Infrastructure Security Agency's (CISA) Chief Learning Office, The Working Group defined the requirements for, and guided the iterative development of, the Cyber Career Pathways Tool and Career Pathway Roadmap Tools; These tools offer interactive and engaging ways for individuals to explore the NICE Framework work roles; identify, build, and navigate a potential cyber career pathway by increasing their understanding of the knowledge and skills needed to begin, transition, or advance a cyber career.
Work Role-Specific Learning Objectives **(Completed, February 2022)**	The Working Group developed a repeatable process and supporting examples to demonstrate how Federal departments and agencies can leverage the core tasks of cyber work roles to create interview questions that assess an individual's technical capability of performing the required tasks of a position. Work role-based interview questions enable agencies to rely less on the educational and credential-based qualifications that previously served as barriers to Federal employment. Instead, use tailored, role-specific questions that serve as mechanisms to determine whether an applicant will be able to apply the skills necessary to perform on the job.
Cyber Professionals Community – Open Opps **(Completed, October 2021)**	The Working Group developed a Cyber Professionals Community where interagency partners can create and solicit participation in stretch assignments, details, and rotations by cyber work role. The offerings not only promote increased adoption of the NICE Workforce Framework but also streamline the way job and professional development seekers identify and pursue cyber-related opportunities aligned to their interests, skills, experience, and career aspirations.

Catalog of Cyber Workforce Management Tools and Resources (3 of 3)

Retention	
Cyber Retention Community of Practice (In Progress)	In partnership with the Department of Energy, the Working Group supported an agency wide Cyber Retention Community of Practice (CoP). The CoP aimed to bring interested, Federal agencies and departments together to learn about existing retention incentive programs and identify best practices and procedures that can be used to stand up their own program. In addition, the CoP highlighted the growing need for a permanent solution to the increasing pay disparity between Federal cyber practitioners and industry.
Special Salary Rate (In Progress)	In partnership with OPM, the Working Group is currently pursuing a government wide Special Salary Rate (SSR) for positions within the 2210-Information Technology Management occupational series. Leveraging labor market analysis conducted by Cybersecurity and Infrastructure Security Agency (CISA), combined with Fiscal Year 2021 position and staffing data supplied by Veterans Affairs (VA), Health and Human Services (HHS), Department of Energy (DoE), Department of State (DoS), and DHS CISA, the Working Group aims to submit a multi-agency SSR justifying grade-specific supplements for the 2210 occupational series. This 2210-specific SSR intends to address the growing compensation gap between government and industry (in some cases as high as 50%), increase the competitiveness of government offers and attractiveness of Federal civil cyber service, and enable agencies to use retention incentives as they are intended – for highly skilled personnel who are likely to leave in absence of an incentive.
Cyber Retention Report (In Progress)	Through the support of the Cyber Retention CoP, the Working Group is compiling a comprehensive report that outlines recommended best practices and lessons learned to instill a cyber retention program at an organization.