NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Tools in the Federal Cybersecurity Workforce Toolbox

June 19, 2019

TOOLS IN THE FEDERAL CYBERSECURITY WORKFORCE TOOLBOX

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Katika Floyd
Senior Human Resources Specialist
Hiring Policy Section, Employee Services Division
Office of Personnel Management

PRESIDENT'S MANAGEMENT AGENDA

Leading the process to define the future Civil Service

The President's Management Agenda (PMA) is a comprehensive strategy to make government more efficient, effective, and accountable through three pillars:

Mission

A modern workforce will deliver mission outcomes the public expects by focusing on high value, high impact work in order to deliver effective outcomes the public expects.

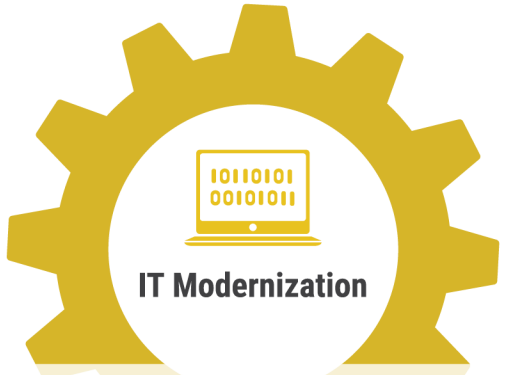
Service

A modern workforce will improve customer service for the 21st century by facilitating faster, more convenient, and more cost-effective customer experiences.

Stewardship

A modern workforce leads to better stewardship of taxpayer dollars by utilizing new approaches, increasing transparency, and delivering better services.

This Administration will pursue lasting progress through the holistic efforts of these three key drivers:



Modern information technology (IT) will serve as the core resource for Government to meet the needs and expectations of Americans while keeping sensitive data secure.

Data, accountability, and transparency will provide the foundation to deliver better outcomes to the public and hold agencies accountable to taxpayers.

A modern workforce calls for civil service reforms to empower everyone from senior leaders to front-line managers to better align skills with evolving mission needs.

"We must change the way that the Federal Government serves its citizens. A Federal Government that is accountable to all Americans is one that is nimble and evolves with technological changes. My plan will enable Americans to be better served by their government."

—President Donald J. Trump

- **Mission**: The American people count on the Federal Government every day, from national security to infrastructure to food and water safety. Public servants must be accountable for mission-driven results but must also have the necessary tools and resources to deliver.

- **Service**: Federal customers range from small businesses seeking loans, to families receiving disaster support, to veterans owed proper benefits and medical care. They deserve a customer experience that compares to—or exceeds—that of leading private sector organizations, yet most Federal services lag behind the private sector.

- **Stewardship**: Effective stewardship of taxpayer funds is a crucial responsibility of Government, from preventing fraud to maximizing impact. Taxpayer dollars must go to effective programs that produce results efficiently.

Cyber Flexibilities and the PMA

- Supports the President's vision of "…enabling simple and strategic hiring to attract top talent" and
- "…maximizing the use of currently available tools and authorities to help address some of our most pressing hiring needs"

Hiring Authorities/Flexibilities

- **Pathways Programs for cybersecurity students and recent graduates** (includes Internship, Recent Graduates and Presidential Management Fellows (PMF) Programs)
- **Government-wide Direct Hire Authorities for certain cybersecurity occupations**
- **CyberCorps®: Scholarship for Service (SFS) Program** provides scholarships to cybersecurity students in exchange for government service upon graduation
- **Delegated Direct Hire Authority for IT positions**
- **Presidential Innovation Fellows (PIF) Program**

Pathways Internship Program

- Provides students with paid opportunities to work and explore Federal careers while still in school
- Successful students are eligible for a permanent or term position in the competitive service upon completing degree requirements
- Interns may:
  - Work full- or part-time
  - Be hired on a temporary basis for up to one year, or an indefinite period

Pathways Recent Graduates Program

- 1-year program with formal training and developmental opportunities to meet specific agency needs
- Appointed at the GS-5/7/9 *(GS-11 or 12 for certain scientific or professional positions)*
- Eligibility for permanent appointment to the competitive service

Pathways Presidential Management Fellows Program

- 2-year leadership development program
- Fellows appointed at the GS-9, 11, or 12
- Rigorous training requirements
- Eligible for permanent placement if…
  - Fellow successfully completes fellowship
  - Fellow is certified by agency Executive Resources Board

Government-wide Direct Hire Authorities

- Information Technology Management (Information Security), GS-2210-09 through GS-2210-15
- Computer Engineers (Cybersecurity) GS-0854-12 through 15
- Computer Scientists (Cybersecurity) GS-1550-12 through 15
- Electronics Engineers (Cybersecurity) GS-0855-12 through 15
- IT Cybersecurity Specialist GS-2210-12 through 15
- Resource: https://www.opm.gov/policy-data-oversight/hiring-information/competitive-hiring/#url=directhire

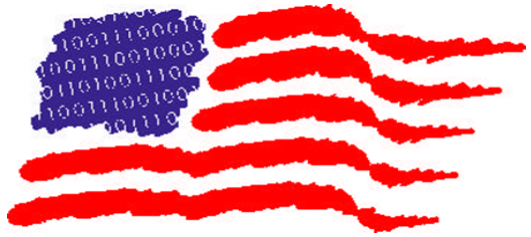
Delegated Direct Hire Authority for IT Positions

- OPM delegated to agency heads the authority to approve DHA for certain IT positions
- *Agencies* must determine a critical hiring need or severe shortage of candidates exists before using

Delegated Direct Hire Authority for IT Positions (cont)

- Information Technology Management Series, General Schedule, GS-2210 or equivalent
- No restriction on:
  - grade level, or
  - geographic location
- Resource: https://chcoc.gov/content/delegation-direct-hire-appointing-authority-it-positions

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). This initiative reflects 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 Scholarship Track

Scholarship Components:

- Funding: tuition, fees, stipends ($25K/$34K per year), and professional allowance ($6,000)
- Length: 1-3 year scholarship for final years of undergraduate or graduate (master's or doctoral) education
- Obligation: Summer internship, post-graduation service requirement (work in government agency equal to scholarship length)

CyberCorps®: SFS Scholarship Track

Eligibility:

- Citizen or lawful permanent resident of the United States
- Full-time student in a coherent formal program focused on cybersecurity; 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 3,600 scholarships awarded since 2001
- 94% placement rate in more than 140 federal/state/local tribal agencies and FFRDC/national labs
- As of January, 2019: Over 70 participating universities in 31 states, DC, and Puerto Rico (see list at https://www.sfs.opm.gov/contactsPI.aspx)
- Over 300 graduating in 2019
- Currently over 700 enrolled
- Surveys show that over 70% of graduates stay with the government beyond their obligation

CyberCorps®: SFS – Recruiting SFS Students

- Attend our Virtual job fair in October and our In-Person event in the Washington, DC, area in early January to connect directly with the students and provide information on your agency and jobs you are recruiting for, conduct interviews, and even make offers.
- Work directly with OPM's SFS Program Office to advertise positions.
- Collaborate with participating universities in your recruitment for cybersecurity positions.
- Use the SFS database to review resumes and recruit directly from SFS students in the program.

CyberCorps®: SFS – Hiring SFS Students

- Cybersecurity Enhancement Act, Public Law 113-74, 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
  - Agency established policy

CyberCorps®: Scholarship for Service (SFS)

Kathy Roberson, OPM
SFS Program Manager
(405) 259-8277
SFS@opm.gov
kathy.roberson@opm.gov
www.sfs.opm.gov

Stephanie Travis, OPM
SFS Program Staff
(202) 579-4951
SFS@opm.gov
Stephanie.Travis@opm.gov
www.sfs.opm.gov

Sandra Cyphers, OPM
SFS Program Staff
(202) 706-8367
SFS@opm.gov
Sandra.Cyphers@opm.gov
www.sfs.opm.gov

Other Available Authorities

- **Presidential Innovation Fellows (PIF) Program** is a 12-month program, during which a Fellow will work on innovation projects across federal agencies. Fellows and agency partners can mutually agree to extend the Fellowship for up to a total of 4 years.
- https://presidentialinnovationfellows.gov/

Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

SANS | CyberTalent

Federal Cyber Reskilling Academy

Pilot 1 Summary

Max Shuftan, SANS Institute

FEDERAL CYBER RESKILLING ACADEMY

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- Innovative training program to develop new cyber professionals that can move into hard-to-fill US Government (USG) jobs
- The FCRA is a USG initiative to reskill members of the current federal workforce, per the President's Management Agenda and the recent Executive Order on America's Cybersecurity Workforce
- Collaboration between the Office of Management and Budget (OMB), the CIO Council, and the US Department of Education
- Pilot 1 supported by the SANS Institute and Patriot Strategies – only open to current, non-IT/cyber USG employees
- This initial pilot aims to find that "hidden" cybersecurity talent from non-IT backgrounds within the current USG workforce

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- **Pilot 1: Hypothesis**
  - Even if individuals have zero IT experience, by identifying those with aptitude & passion you can find future cyber talent
  - These individuals can be reskilled into technical, highly-capable cyber professionals in a matter of months via an immersive skills development and certification program
- Pilot 1 draws from and aims to build on past success of similar programs run by the UK Government and various scholarship Academies in the US for veterans, women, and minorities
- The UK Cyber Retraining Academy saw a journalist, psychiatrist, two police officers, and a bartender among those who were successfully reskilled and deployed into their cyber workforce

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- **Aptitude – who does well?**
  - People who like puzzles and brain teasers
  - Individuals with critical thinking, logic, and information parsing skills
  - Those who liked to take apart toys, equipment, etc. and see how they worked
  - People with a passion and tenacity for constant learning, problem solving, etc.

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- **Pilot 1 Admissions Process**
  1. Submit Application (1,500 applied)
  2. Cyber Aptitude Test
  3. Personal Statement submission
  4. Candidate review by USG
  5. Interviews by USG (approx. 50 top candidates)
  6. Selection (30 cohort members: 24 live and 6 virtual)

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- **Pilot 1 Academy structure**

1. CyberStart Essentials training and CyberStart Game
2. Ongoing mentorship
3. SEC401: Security Essentials course and GSEC certification
4. SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling course and GCIH certification
5. NetWars cyber range
6. Graduation

SANS | CyberTalent

Federal Cyber Reskilling Academy (FCRA)

- **Pilot 1 – Current Status**
  - All 30 students successfully completed Stage 1 (CyberStart Essentials)
  - 24 students took SEC401 in Washington, DC from May 16-24. 23 of 24 successfully achieved the GSEC, an ANSI-accredited certification.
  - 13 scored 90% or higher! One student is receiving a retake.
  - Six virtual students are currently taking SEC401 online
  - 23 students are taking SEC504 in Washington, DC this week. Will take the GCIH, an ANSI-accredited certification, by July 15.
  - Virtual students will take SEC504 after achieving GSEC
  - Graduation for the live cohort is July 15
- *How do we measure success?* **New Skills and Jobs!**

SANS | CyberTalent

Questions?

For additional information, please contact
mshuftan@sans.org or reskilling.academy@gsa.gov

Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Talent Initiative

Margot Conrad
Director
Federal Workforce Programs
Partnership for Public Service

cybersecurity talent initiative.

Cybersecurity Workforce

Our nation's ability to deliver important services, protect privacy and safeguard classified information requires an effective and secure digital infrastructure overseen by highly skilled cybersecurity professionals.

The number of cybersecurity job openings in the Unites States

313,000

Globally, projections suggest a cybersecurity workforce shortage of

1.8 million by 2022

The annual cost of data breaches is expected to rise to

$2.1 trillion by 2020

cybersecurity talent initiative.

Cybersecurity Talent Initiative
Overview

Participants will:

- Work for some of the **most important and innovative federal organizations** for two years
- Be invited to apply for select positions with some of the **world's cutting-edge private sector companies**
- Receive robust **leadership training and mentoring**
- Gain an opportunity for **student loan assistance up to 75,000 (inclusive of tax)**

Founding Corporate Partners

Operating Partner

Participating Federal Agencies

- Central Intelligence Agency
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Veterans Affairs
- Environmental Protection Agency
- Federal Bureau of Investigation
- Federal Election Commission
- National Oceanic and Atmospheric Administration
- Naval Intelligence
- Small Business Administration

Sample Positions

Federal Government

- **Cyber Exploitation Officer at CIA**
  - Evaluates and analyzes digital and all source intelligence information to identify and assess key adversaries and while extracting valuable information from digital data and presenting findings to inform operations, drive collection and support customers.
- **Cybersecurity Analyst at HHS**
  - Detects, monitors, and conducts forensic analysis of cyber threats, then translates that technical threat information into language to convey the risk and how to address it in a manner that is easily understood by healthcare professionals.

Private Sector

- **Security Threat Analyst at Microsoft**
  - Engages with partners across Microsoft to innovate new approaches for detecting and tracking threats, attacker techniques, and their tools and infrastructure while using threat research and data science to hunt for real cyber threats and produce intelligence reports and analysis.
- **Corporate Security, Vulnerability Management at Mastercard**
  - Identifies, tests, and reports security weaknesses in systems and applications, while overseeing efforts throughout the enterprise to secure vulnerabilities.

Application Process
Eligibility Requirements

- U.S. citizenship
- Current enrollment at an accredited educational institution in an undergraduate or graduate cybersecurity-related degree program
- Completion of cyber-related degree (for example, computer science, engineering, information science, and mathematics) with an expected graduation date of **spring 2020**
- Superior academic achievement
- Outstanding student loans

Application Process
Required Documents

- **Personal information** (name, address, contact information)
- **Supplemental** information
- **Endorsement** form
- **Two** references
- **Three** short essay questions

Submitting an Application
Applicants Should Highlight

- Commitment to public service, team work, leadership, problem solving, and communication skills
- Any professional or IT security certifications
- Classes related to cybersecurity or a related field
- Participation in student organizations or volunteer work
- Any awards or special recognitions relating to cybersecurity
- Internships or jobs in cybersecurity or related field
- Participation in a cybersecurity competition

Security Clearances

Timing

- Agencies will have different clearance processes—timing could vary between 6-12 months
- Agencies may require different levels of clearances

Encourage applicants to

- Be aware of their public profile (e.g., social media)
- Refrain from drug use
- Begin to track references and personal contacts
- Keep tabs on international travel
- Respond truthfully

Learn More

Margot Conrad
MConrad@ourpublicservice.org

To learn more visit:
www.CyberTalentInitiative.org

cybersecurity talent initiative

Q & A

Thank You for Joining Us!

Upcoming Webinar: "How Talent Management Systems Help You Manage Your Cybersecurity Human Capital"

When: Wednesday, July 17, 2019 at 2:00pm EDT

Register: https://nist-nice.adobeconnect.com/webinar-jul2019/event/registration.html

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION