CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA Cyber Services & Educational Opportunities

Alex Salazar
Chief of Cybersecurity Region 10
Cybersecurity Advisor (CSA) Program
Cybersecurity and Infrastructure Security Agency

Chris Callahan
May 3, 2023

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity & Infrastructure Security Agency (CISA)

The Nation's Risk Advisors

VISION

Secure and resilient infrastructure for the American people

MISSION

Lead the National effort to manage risk to our critical infrastructure

CORE COMPETENCIES

Our Perspective

Our goal is to foster resilience across the system, increasing capacity and ability of critical infrastructure to secure their assets. This is what we know works.

Information-sharing

Rapidly identifying cyber and insider threats and techniques, and sharing among a broader community

Risk Assessments

Understanding the threat to you and your systems and assets; identifying gaps in your security program; and understanding tools available to meet your needs

Capacity-Building

Increasing the strength of your organization's security program and building resilience in the overall ecosystem

Public and Stakeholder Engagement

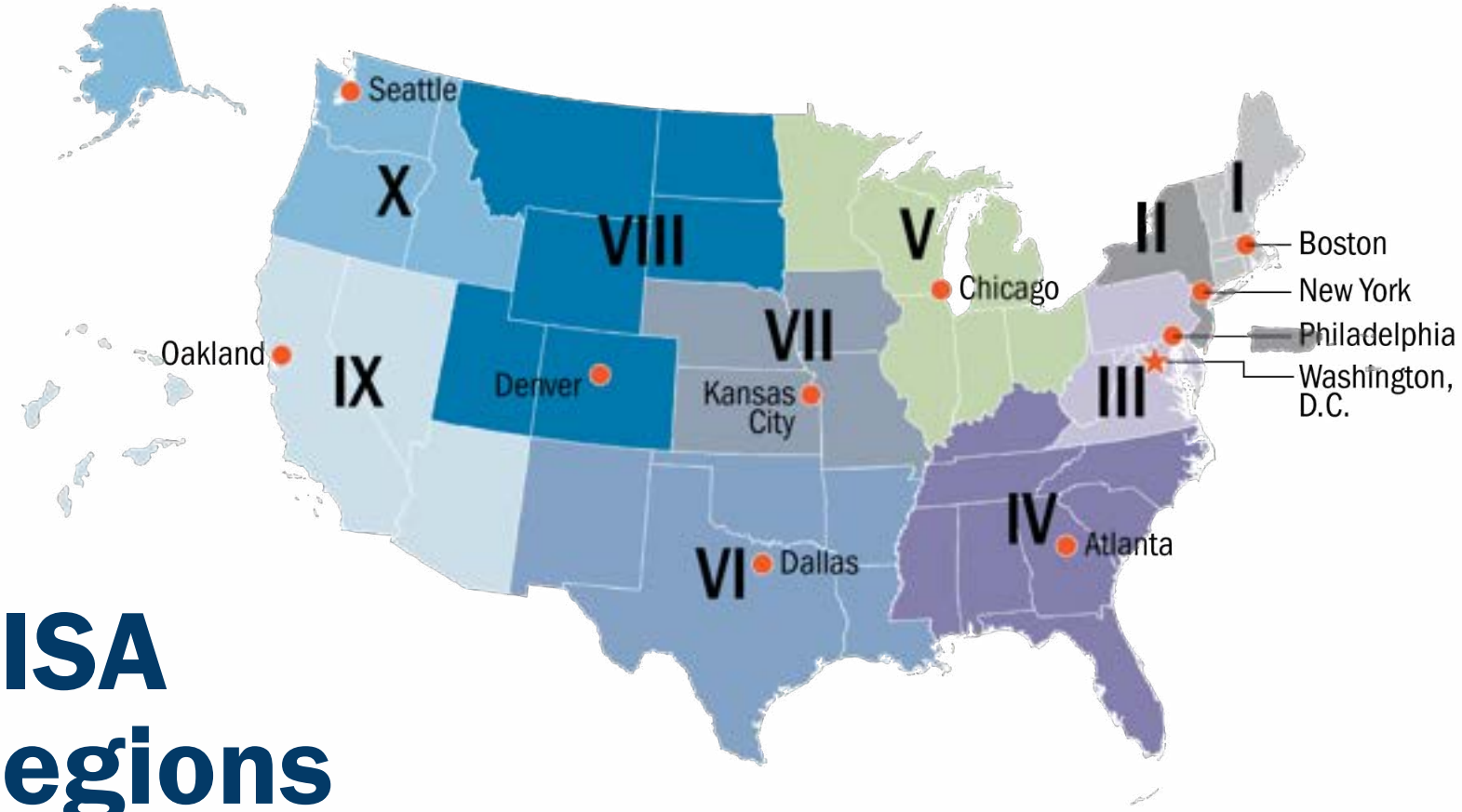
Highlighting a threat or known risk to the general public and stakeholders; understanding evolving and changing needs; and educating on potential responses and resources available

Critical Infrastructure Impact on the Nation

- 16 critical infrastructure sectors create a widely dispersed network, but sectors are interconnected and interdependent
- Critical infrastructure includes:
  - Vital physical and cyber systems, and networks
  - Thousands of essential energy, water and health facilities, transportation networks, agriculture, defense industry, information technology and other systems

Chris Callahan
May 3, 2023

Region 10: CISARegion10@hq.dhs.gov

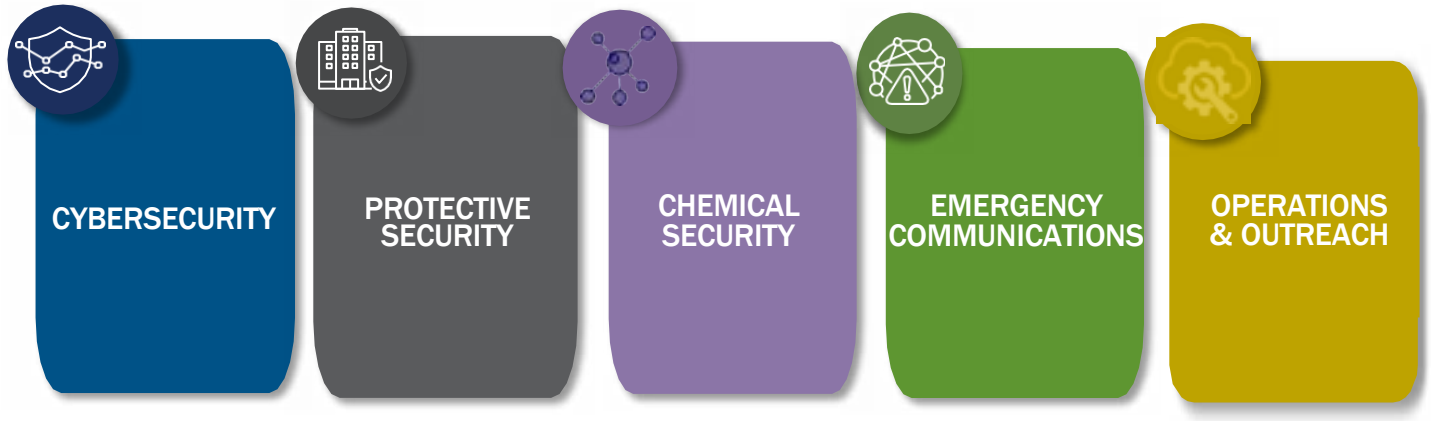


CISA Regions

Information Exchange	Incident Response	Risk & Cybersecurity Assessments	Exercises & Training

CISA Region 10 Overview

- Expertise and a history of success providing services to Unclassified Information and Operational Technology (IT and OT) environments
- Proactive services to government and critical infrastructure clients to assess and improve cybersecurity posture, understand risk, and identify operational strengths and weaknesses



Services are provided at "no cost" to our customers

Our "payment" is authorization to use anonymized, non attributable, data to enhance national situation awareness and enable our stakeholders to make data driven decisions

Chris Callahan
May 3, 2023

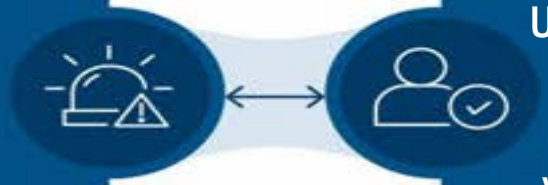
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

How We Can Work Together

- Exchange information and intelligence
- Understand the strategic threat
- Identify your assets and risks
- Analyze your relationships
- Know your people and their access

Know the Threat

Understand malicious actors strategic goals and objectives. Know the capabilities and tactics, techniques, and procedures of malicious actors.



Know Yourself

Understand what your high-value assets are, to malicious actors and any other adversary. Assess your security programs and their ability to mitigate this risk.

Range of Cybersecurity Offerings

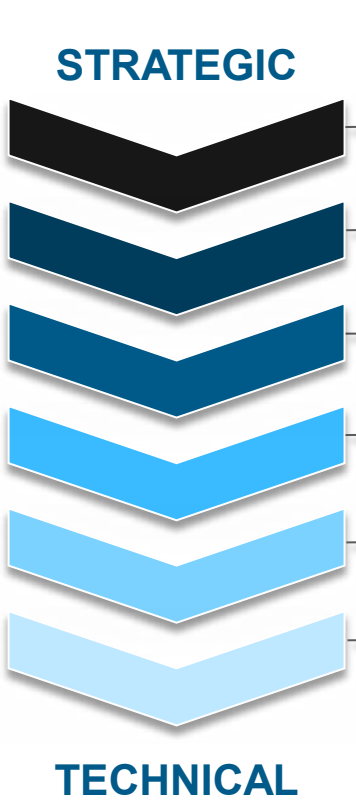
Cyber Resilience Review (CRR)

External Dependencies Management (EDM)

Cyber Infrastructure Survey (CIS)

Cybersecurity Evaluations Tool (CSET)

Vulnerability (CyHy) /Tabletop Exercise



CRR
- 6-8 hours

EDM
- 4 Hours
- Supply Chain Risk Mgmt
- Relationships

CSET
- Self Assessment Tool
- Ransomware Readiness Assessment

Vuln / Scans
- Weekly scans
- Weekly reports
- External network presence
- External Internet Scans

Cyber Protective Visits (CPV) – To determine additional services

Exercise and Training

Exercises

- Tabletop Exercises
- “Tabletop in a Box”

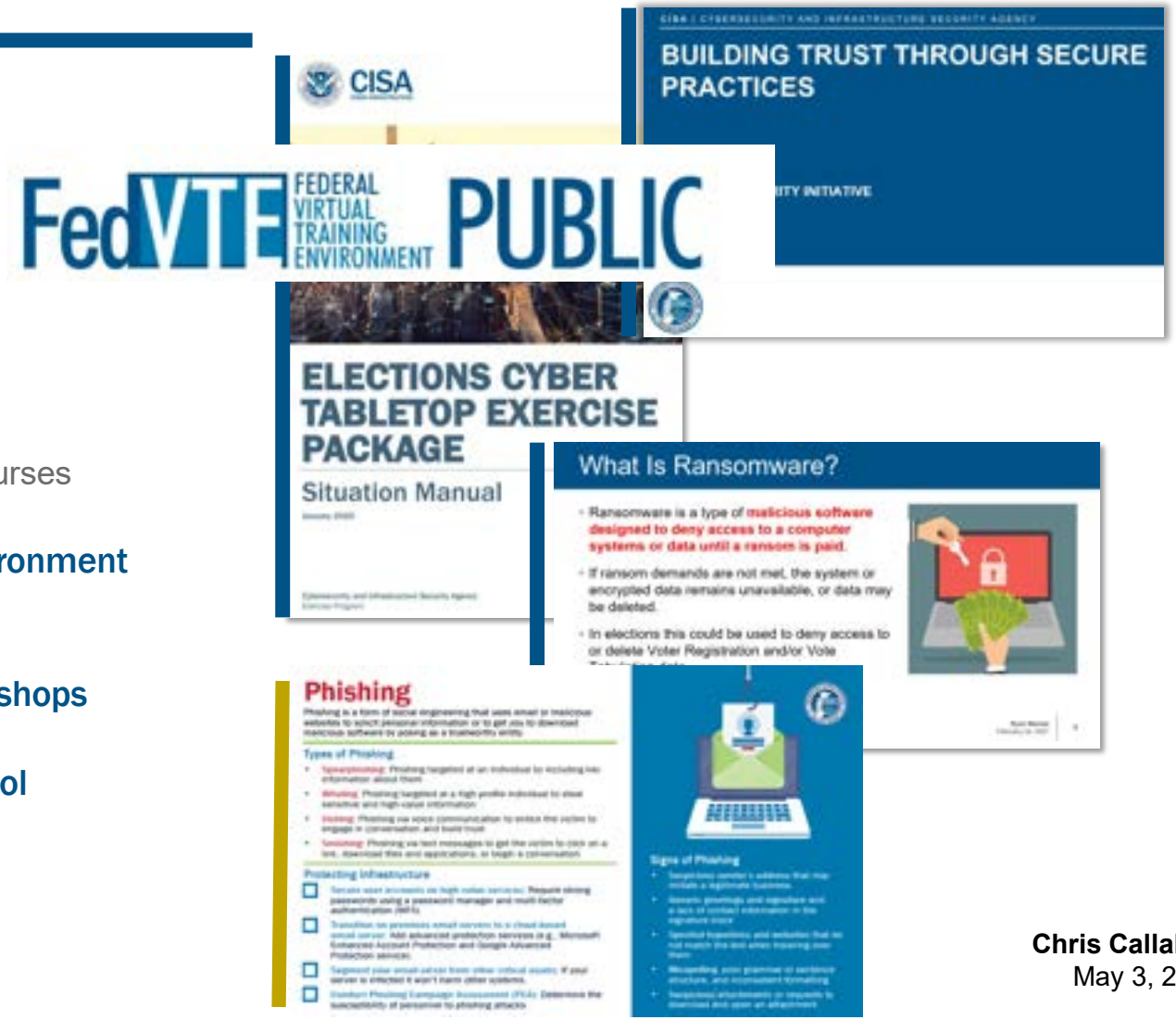
Training Offerings

- Ransomware
- Phishing
- In-person cybersecurity courses

Federal Virtual Training Environment (FedVTE)

Incident Management Workshops

Cyber Security Evaluation Tool (CSET)

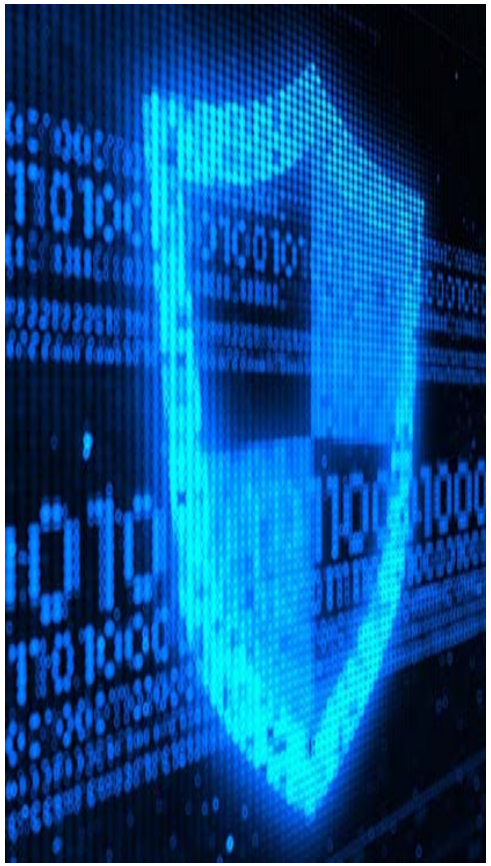


Chris Callahan
May 3, 2023

Protected Critical Infrastructure Information Program

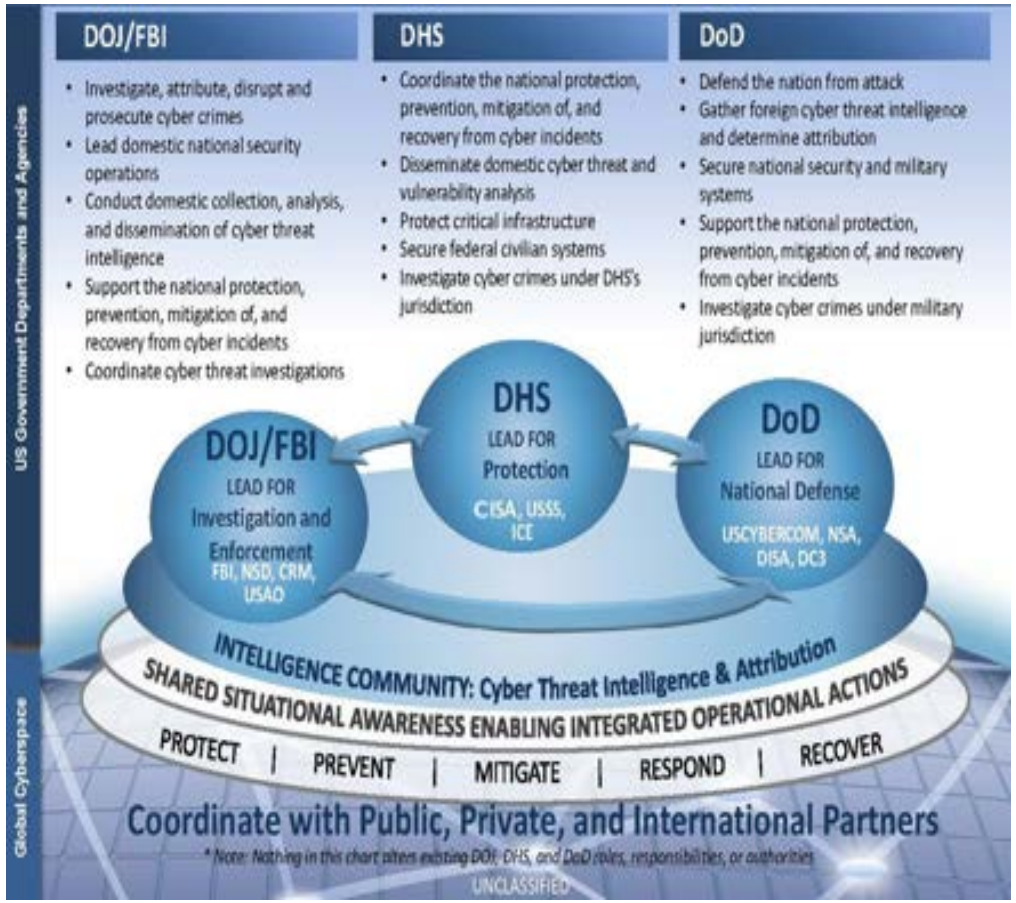
Protected Critical Infrastructure Information (PCII)
Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is ***protected*** by law from
  - Public release under Freedom of Information Act (FOIA) requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.
- Find out more: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program



Chris Callahan
May 3, 2023

All Of Government Approach



Alerts, Bulletins, Security Updates, Best Practices

https://us-cert.cisa.gov/

Contact CISA to report a cyber incident
Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Chris Callahan
May 3, 2023

People

How does the federal government recruit and retain world-class cybersecurity talent to protect and defend our systems? TRAIN, Certify and Experience!

OBJECTIVE:
1550, 0854 and 2210

CISA uses the NICE Cybersecurity Workforce Framework to define duties and responsibilities of our cyber workforce.

Cybersecurity/IT Jobs | CISA

- Develop Internal Training Programs, IDPs and ensure you have diversity in skill sets in workforce
- Invest in “right” professional certifications, mobile training teams, specific technology training in environment

Chris Callahan
May 3, 2023

What To Look For from a Prospective Candidate?

- US Citizenship for Security Clearance (Interim upon start)
- Major, Degree, Graduation Date (3.5 GPA preferable) (1550, 0854, 2210)
- Professional Certifications for Cybersecurity (Security+ =<6 months)
- Community Service/Activities
- Geographical Availability – Independent Self Starter - Remote Employees
- Work experience related to position – Passion and Impact
- Communication Skills – Do they go dark during the process?
- Experience - Breadth & Depth
- Progressive/Leadership Experience
- Interpersonal Skills – Can do Attitude

Chris Callahan
May 3, 2023

Sample Candidate Evaluation Form

Candidate Evaluation Form

Applicant Name:	Position:

Please use this form as a guide to evaluate the applicant's qualifications for employment. Check the appropriate numeric value corresponding to the applicant's level of qualification and provide appropriate comments in the space below.

Rating Scale:

5. **Outstanding**
4. **Excellent-exceeds requirements**
3. **Competent—acceptable proficiency**
2. **Below Average—Does not meet requirements**
1. **Unable to determine or not applicable to this candidate**

	Rating				
	5	4	3	2	1
Relevant Background/Special Skill Set: Explore the candidate's knowledge and past working experiences in training.					
Professional Impression: Consider self-confidence, maturity, and presence to assess the candidate's level of professionalism.					
Motivation/Initiative: Analyze applicant's ability to think and act independently, and goal orientation. Why does this person want to work at the ERDC?					
Interpersonal/Communication Skills: Assess ability to express ideas and thoughts clearly, as well as experiences involving team settings and customer orientation.					
Flexibility: Assess candidate's responsiveness to change, tolerance for ambiguity.					
Organizational Fit: Review the candidates' potential to fit the unique ERDC organization and culture.					
Presentation Skills: Overall assessment of candidate's 20 min. presentation for organization and stand-up /facilitation skills.					
Overall Evaluation: Please add appropriate comments below:					

Supervisor Hiring Toolbox

- Direct Hiring Authority: https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Fact-Sheet (Find a great candidate hire today!) (E&S and Cybersecurity DHAs)

- Veteran Recruitment Act: https://www.opm.gov/policy-data-oversight/hiring-information/veterans-authorities/ (Lots of great military departing that are cleared and certified from SOCs, NOCs, Cyber Protection Teams and CERTs)

- Tentative Job Offers to Candidates same day utilizing DHA or VRA for critical skill fills.

- Maintain open USAJOBS announcements for candidates to apply (30-180)

- Educational Partnership Agreements – Visit local and regional Universities and Community Colleges and establish EPAs with Computer Science Departments

Chris Callahan
May 3, 2023

Student Employment Opportunities

Three ways to gain Federal experience https://www.opm.gov/about-us/careers-at-opm/students-recent-graduates/

- **Internship Program** - This program is intended to provide meaningful work experience for students who are currently enrolled in qualifying institutions.

- **Recent Graduates Program** - This program is intended to promote careers in the government by providing recent graduates' experience with the federal government. Participants must have obtained a qualifying degree or completed a qualifying career or technical education program within the preceding two years.

- **Presidential Management Fellow (PMF) Program** - This program is applicable to individuals from a variety of academic disciplines at the graduate level. Participants will continue to be known as PMFs or Fellows and must have received, within the preceding two years, a qualifying advanced degree.

Visit https://www.usajobs.gov/ to check for open announcements for Pathways students.

PATHWAYS FOR STUDENTS & RECENT GRADUATES TO FEDERAL CAREERS

Chris Callahan
May 3, 2023

Scholarships

Science, Mathematics, And Research for Transformation (SMART) – (Undergraduates, MS, PhD) DoD Scholarship for Service Program

- The SMART Defense Education Program is part of a concentrated effort to improve the flow of new, highly skilled technical labor into DoD laboratories and agencies and to enhance the technical skills of the workforce already in place.
- DoD offers scholarships to undergraduate, master's, and doctoral students who have demonstrated ability and special aptitude for training and education in Science, Technology, Engineering and Mathematics (STEM) fields.
- http://www.usaeop.com/
- https://smart.asee.org/

Scholarship for Services (SFS) (Undergraduate, MS, PhD):is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure.

- This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning.
- The scholarships are funded through grants awarded by the National Science Foundation.
- https://www.sfs.opm.gov/

Internships

Department of Homeland Security (DHS) —Internship Program – (Undergraduates)

- The DHS HS-STEM Summer Internship Program provides a 10-week summer research experience for undergraduate students majoring in homeland security related science, technology, engineering and mathematics (HS-STEM) disciplines.
- Students will have the opportunity to conduct research in DHS mission-relevant areas at federal research facilities located across the country.
- Participants receive a stipend of $500 each week plus transportation expenses to/from their internship location.
- http://www.dhs.gov/national-hs-stem-summer-internship-program

Oak Ridge Institute for Science and Engineering (ORISE) - (Undergraduate, MS, PhD):

- The U.S. Department of Energy (DOE) and more than a dozen other federal agencies rely on the Oak Ridge Institute for Science and Education (ORISE) to help meet future needs in critical science and technology areas through the recruitment and training of our nation's next generation of scientists and engineers.
- To meet these pressing demands, ORISE assesses current science and technology labor needs and then designs and implements programs that meet the unique goals of each agency.
- Research participants are recruited nationally, including special outreach to Historically Black Colleges and Universities and other Minority-Serving Education Institutions.
- http://orise.orau.gov/science-education/internships-scholarships-fellowships/

Internships (cont.)

AEOP - Science and Engineering Apprentice Program (SEAP) – High School Level– (HS Sophomores - Seniors)

- The Science and Engineering Apprentice Program (SEAP), sponsored by the American Society of Engineer Education (ASEE) and the Department of Defense, is an eight week summer program for high school students.
- SEAP is designed so that students can apprentice in fields of their choice with experienced scientists and engineers.
- http://www.usaeop.com/

AEOP - College Qualified Leaders (CQL) – (Undergraduate, MS, PhD):

- CQL offers undergraduates and graduate students the opportunity for research internships in DoD labs. Internships are available year round and during the summer. The CQL students will do research with a mentor, but, at many labs, they also serve as mentors/advisors to some of the high school SEAP students.
- They may also be involved in the GEMS program as near-peer mentors and some take on leadership roles in developing and teaching the GEMS students.
- http://www.usaeop.com/

Women In Science Program (WISP) (Pre-college, Undergraduate):

- WISP's mission at Dartmouth College is to collaborate in creating a learning environment where women can thrive in science, engineering and mathematics.
- http://www.dartmouth.edu/~wisp/

Region 10 Cybersecurity Contacts and Questions?

Chris Callahan
Chief, Cybersecurity (CCY)
(206) 601-4575
CHRISTOPHER.CALLAHAN@cisa.dhs.gov

Theresa Masse / Leslie Kainoa
CSC/CSA for Oregon
503-930-5671 / 503-462-5626
Theresa.Masse@cisa.dhs.gov
Leslie.Kainoa@cisa.dhs.gov

Ron Watters / Alex Salazar
Region 10 (Private Industry)
Western WA Cybersecurity Advisors
206-348-4071 / 206-225-5546
Ronald.Watters@cisa.dhs.gov
Alexander.Salazar@cisa.dhs.gov

Josh Stemp
CSC for Idaho
208-761-9882
Joshua.Stemp@cisa.dhs.gov

Mark Breunig / Troy Lofven
CSC/CSA for Alaska
907-795-5673 / 907-
Mark.Breunig@cisa.dhs.gov
Troy.Lofven@cisa.dhs.gov

Dan Brown
Region 10 (Private Industry)
Inland NW Cybersecurity Advisor
509-981-9920
Daniel.Brown@cisa.dhs.gov

Ian Moore
CSC for Washington
360-594-1832
Ian.Moore@cisa.dhs.gov

For inquiries or further information, contact cyberadvisor@cisa.dhs.gov

Contact CISA (via the reporting portal or by phone at 1-888-282-0870) to report an intrusion or to request either technical assistance or additional resources for incident response. CyberLiaison@cisa.dhs.gov
and
FBI 24/7 CyWatch (855) 292-3937
CyWatch@fbi.gov