# 16TH ANNUAL CYBERSECURITY DAY AT IUP

## OCTOBER 31, 2023

**9:00 AM - 4:00 PM**

**HUB - OHIO ROOM, 319 PRATT DRIVE**
**INDIANA, PA 15705**

## FEATURING:

**A number of recognized security experts from government, academia, and industry.**

**FREE AND OPEN TO ALL. VISIT BIT.LY/IUP-CSDAY OR SCAN THE QR CODE FOR MORE INFORMATION.**

**THE 2023 CYBERSECURITY DAY IS PROUDLY SPONSORED BY PC4A AND IUP**

PC4A
PA Community College
Consortium Cooperative Agreement

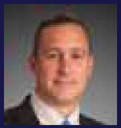
IUP

## BIO INFO CONTINUED

### Raju Namburu, Chief Technology Officer, US Army Information Technology Laboratory

Raju Namburu is CTO for Information Technology Laboratory's computational sciences and engineering. In this role, he provides directions to DoD HPC Modernization Office, computational sciences and engineering, and cyber research and development programs. Namburu represents DoD as a member of the US National Science and Technology Council subcommittee for the future advanced computing echo system. Prior to coming to ITL, Namburu was chief scientist, division chief, Computational Sciences Division, and director, DoD Supercomputing Resource Center at the Computational and Information Sciences Directorate, US Army Research Laboratory. Namburu led various DoD scalable software development projects in computational sciences, including establishing DoD mobile network modeling institute. Namburu obtained his PhD in mechanical engineering from the University of Minnesota. During his career, Namburu has worked at IBM Almaden Research Lab, Cray Research, and various US Army research, development, and engineering labs. Namburu has more than 100 refereed publications in journals and has presented at international conferences and symposiums. Namburu is a Fellow of American Society of Mechanical Engineers.

### Dom Glavach, Chief Security and Technology Officer, CyberSN



Dom Glavach is the chief security officer and chief security strategist at CyberSN. In this executive role, he is responsible for leading the company's information security strategy, policy, IT operations, security engineering, security operations, data privacy, and cyber threat detection. Prior to CyberSN, Glavach spent 20 years working with Concurrent Technologies Corporation, where he served as the chief information security officer and research fellow. He played a critical role in the company's cyber risk management, providing cyber technical leadership and subject matter expertise to commercial and government clients. Glavach is a CISSP, an active member of the Armed Forces Communications and Electronics Association Cyber Committee, chairs a subcommittee on Vehicle and Embedded Systems Cyber Security, and mentors at cybersecurity meet-ups. He has presented on various security topics to a wide range of public and government audiences, including the National Institute of Standards and Technology and the National Security Agency.

## GUEST SPEAKER TITLES AND ABSTRACTS

***Cyber Security Workforce Development and the Department of Defense***
**Presenters:** Louie Lopez, Star Hardison
**Abstract**: DoD STEM's mission is to inspire, cultivate, and develop exceptional STEM talent through a continuum of opportunities to enrich our current and future Department of Defense workforce poised to tackle evolving defense technological challenges. By inspiring new and future talent in Science, Technology, Engineering and Mathematics (STEM) fields, we are poised to prepare the next generation for the ever changing landscapes of threats that our nation may face, and cyber security is one such field. DoD is the largest employer of scientists and engineers in the federal government with over 60 Defense Laboratories and Engineering Centers at more than 200 locations across the country. There are nearly 300,000 STEM professionals, with about 60,000 of the STEM workforce doing research at our Labs and Centers. In order to maintain our Nation's competitive advantage, we require a diverse and sustainable STEM talent pool. We will discuss broadly the cyber security workforce needs for the Department of Defense.

***Panel Discussion: Building IT and Cybersecurity Careers; from Student to Executive***
**Presenters**: Tom Dugas, Bill Ballint, Todd Cunningham
**Abstract**: This panel discussion will provide attendees with key personal experiences, important career decisions, and tips taken from their careers spanning from undergraduates through the career ladder to their current executive-level roles.

***Advanced Computing Ecosystem and Cyber Analytics***
**Presenter**: Raju Namburu
**Abstract**: Advanced computing ecosystem is rapidly evolving across multiple dimensions due to the introduction of new and potentially disruptive technologies and paradigms, increased hardware heterogeneity, internet of battlefield things, data volumes, software complexity, cyber challenges, and novel approaches such as those based on AI and ML. Now, and even more so in the future, the battlespace is characterized by highly distributed processing, heterogeneous and mobile assets with limited power, communications-dominated but restricted network capacity, and operating with time-critical needs in a rapidly changing hostile cyber environment. Predictive data-intensive electromagnetic cyber analytics leveraging data from numerous sources, advanced computing ecosystem, and robust AI/ML algorithms will allow rapid and decisive action on the emerging DoD multi-domain battlefield. In this talk, I will discuss this topic including cyber programs within our lab and related research directions. I will briefly highlight summer internship opportunities within our lab.

***An Executive Perspective of Cybersecurity***
**Presenter:** Susan Koski
**Abstract**: Susan Koski, one of the region's most prominent Chief Information Security Officers (CISO), will provide her perspectives on cybersecurity-related topics. The talk will reflect on Susan's established expertise in the field as the CISO at PNC and Pittsburgh CISO of the Year among the region's largest corporations. Susan was recently featured in Cybercrime Magazine and presented at the prestigious RSA Conference. Her expertise spans much of the cybersecurity industry.

***Clean Up on Aisle 4: Active Cyber Defenses***
**Presenter**: Dom Glavach
**Abstract**: Today's cyber industry is flush with an array of protective solutions, spanning from Multi-Factor Authentication (MFA) to AI-powered Attack Surface Management tools. Yet, with all these technological advancements, adversaries continue to hide in plain sight, often exploiting the very complexities that were meant to thwart them. As regulatory bodies like the SEC intensify the requirements for swifter and more detailed incident reporting, and with the rapid adoptions of evolving technologies coupled with the continually shifting threat landscape demands more than just conventional detection and response mechanisms - proactive threat hunting. This session discusses the essential techniques of threat hunting, shedding light on the nuances of actively seeking out hidden adversaries beyond the existing and traditional cyber defenses. Attendees will be introduced to open-source tools and a career path to the world of threat hunting

***National Cybersecurity Awareness Month 2023 – How To Stay Safe Online***
**Presenter**: Derek Mueller
**Abstract**: Technology is part of everything that makes our life function—from the classroom to the office, from financial transactions to how we travel to how we communicate with family and friends. Cybersecurity and Infrastructure Security Agency (CISA) launched the Secure Our World program, a new and enduring cybersecurity awareness program aimed at engaging audiences and emphasizing the four simple steps everyone should implement and continuously improve upon. The brief will provide resources and specific examples on steps to take to keep our devices, such as computers, phones, tablets, and other connected devices, safe and secure. The brief will also aim to educate the audience on how to stay safe online by encouraging action and driving behavior change and incorporate many of CISA's other awareness products and initiatives.

PC4A
PA Community College
Consortium Cooperative Agreement

IUP

THE 16TH ANNUAL

# CYBERSECURITY DAY AT IUP

OCTOBER 31, 2023

OHIO HUB
IUP MAIN CAMPUS

# CYBERSECURITY DAY AT IUP

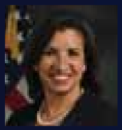
| TIME SLOT | SESSION TITLE AND PRESENTER |
|---|---|
| 9:00 AM to 9:02 AM | ***Introduction to the 16th Annual Cybersecurity Day at IUP.***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |
| 9:02 AM to 9:07 AM | ***Opening Remarks***<br>Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics |
| 9:07 AM to 9:10 AM | ***Welcome Message***<br>Timothy Flowers, Chair, Department of Mathematical and Computer Sciences |
| 9:10 AM to 9:20 AM | ***Event History, ICS Work, Recent Achievements, and Logistics***<br>Waleed Farag, Director, Institute for Cybersecurity, Professor of Computer Science |
| 9:20 AM to 10:05 AM | ***Cybersecurity Workforce Development and the Department of Defense***<br>Louie Lopez, Director of STEM, US Department of Defense and Star Hardison, Chief of Cyber Workforce Governance Branch, US Department of Defense |
| 10:15 AM to 11:00 AM | ***National Cybersecurity Awareness Month 2023 - How to Stay Safe Online***<br>Derek Mueller, Cyber Security Advisor, US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency |
| 11:10 AM to 11:55 AM | ***Panel Discussion: Building IT and Cybersecurity Careers; From Student to Executive***<br>Tom Dugas, Associate VP and Chief Information Security Officer, Duquesne University, Bill Balint, Chief Information Officer, Indiana University of PA, and Todd Cunningham, Executive Director of Information Technology Services, Indiana University of PA |
| 11:55 AM to 1:00 PM | Lunch Break |
| 1:00 PM to 1:05 PM | ***Welcome Back and Afternoon Logistics***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |
| 1:05 PM to 1:10 PM | ***President's Remarks***<br>Michael Driscoll, President, Indiana University of PA |
| 1:10 PM to 1:55 PM | ***An Executive Perspective on Cybersecurity***<br>Susan Koski, Chief Information Security Officer, The PNC Financial Services Group |
| 2:05 PM to 2:50 PM | ***Advanced Computing Ecosystem and Cyber Analytics***<br>Raju Namburu, Chief Technology Officer, US Army Information Technology Laboratory |
| 2:50 PM to 3:05 PM | Afternoon Break |
| 3:05 PM to 3:50 PM | ***Clean Up on Aisle 4: Active Cyber Defenses***<br>Dom Glavach, Chief Security and Technology Officer, CyberSN |
| 3:50 PM to 4:00 PM | ***Event Conclusion***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |

## BIOGRAPHICAL INFORMATION ON GUEST SPEAKERS

### Louie Lopez, Director, US Department of Defense Science, Technology, Engineering and Mathematics

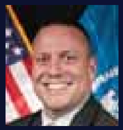
Mr. Lopez is the Director of the Department of Defense's Science, Technology, Engineering and Mathematics Education and Outreach office, also known as DoD STEM, located in the Office of the Undersecretary of Defense in Research and Engineering's Science and Technology Foundations Office. Mr. Lopez is responsible for the management and execution of the Department's Pre-K through Post-Secondary STEM efforts under the National Defense Education Program (NDEP).

### Wistar (Star) Hardison, Chief of Cyber Workforce Governance Branch, US Department of Defense



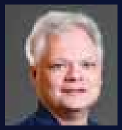
Ms. Star Hardison is the Chief of Cyber Workforce Governance Branch for the Department of Defense (DoD) Chief Information Office in Arlington, Virginia. In this role, she oversees the policy that governs efforts to identify, recruit, retain, and develop an effective and agile Cyber Workforce. A graduate of Villanova University and a proud veteran with 26 years in the U.S. Navy, she's made significant contributions both in service and in her community.

### Derek Mueller, Cyber Security Advisor, US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency



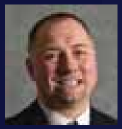
Derek Mueller serves as the Cyber Security Advisor, Cyber State Coordinator for Pennsylvania at the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), where he leads the effort to protect and advance the resilience of the nation's cyber infrastructure within the critical infrastructure while working with federal, state, local, and other stakeholders to maximize collaboration and minimize risk on matters of homeland security or emergency management.

### Bill Balint, Chief Information Officer, Indiana University of Pennsylvania



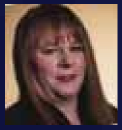
Bill Balint has 34 years of IT experience and became IUP's chief information officer in 2006. Bill has presented at more than 50 industry events at the regional, state, national, and international levels and has authored, co-authored, or been interviewed for more than 35 publications and websites via written, audio, and video formats. He is also a member of the Pittsburgh Executive CIO governing board

### Tom Dugas, Associate Vice President and Chief Information Security Officer, Duquesne University



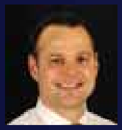
Tom Dugas is responsible for leading the information (cyber) security program to protect the availability, confidentiality, and integrity of data and systems at Duquesne University. Tom is a certified information systems security professional and is a graduate of Robert Morris University with a master's degree in communication and information systems and a bachelor's degree in business administration with majors in accounting and management information systems. In 2019, Tom was recognized as the CISO of the Year by the Pittsburgh Technology Council. Tom serves as a leader within the region as a co-leader of the Greater Pittsburgh CISO Group, a member of the Advisory Board for the Pittsburgh CIO Forum, and part of the Governing Body of the Pittsburgh CIO Executive Summit.

### Susan Koski, Chief Information Security Officer, The PNC Financial Services Group



Susan Koski serves as the Chief Information Security Officer (CISO) and Head of Enterprise Information Security for The PNC Financial Services Group. She is a 2023 Pittsburgh CISO of the Year winner and is a nationally recognized CISO in the financial services sector. She has presented at many major events and has appeared on various video and podcast programs. She is featured in the 2021 book entitled "Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders". Among her many achievements is converging cyber, physical, fraud and insider monitoring into PNC's 24x7x365 Global Security Fusion Center. Susan is a Governing Board member for the Evanta Pittsburgh CIO & CISO Executive Summit and related program and is a leader in the Pittsburgh Technology Council community. She earned a bachelor's degree in electrical engineering from the University of Pittsburgh and a Master's in Business Administration from Duquesne University.

### Todd Cunningham, Executive Director, IT Services, Indiana University of PA



Todd Cunningham is responsible for the operational management and leadership of the IT Services organization at IUP. This includes the oversight of enterprise systems, network, cloud, mobile devices, customer service, etc. He has over 30 years of experience in IT and has been in his current role since 2006.

**For more information about Cybersecurity Day at IUP, please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu, 724-357-7995.**

# 16TH ANNUAL

# CYBERSECURITY DAY AT IUP

| TIME SLOT | SESSION TITLE AND PRESENTER |
|---|---|
| 9:00 AM to 9:02 AM | ***Introduction to the 16th Annual Cybersecurity Day at IUP.***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |
| 9:02 AM to 9:07 AM | ***Opening Remarks***<br>Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics |
| 9:07 AM to 9:10 AM | ***Welcome Message***<br>Timothy Flowers, Chair, Department of Mathematical and Computer Sciences |
| 9:10 AM to 9:20 AM | ***Event History, ICS Work, Recent Achievements, and Logistics***<br>Waleed Farag, Director, Institute for Cybersecurity, Professor of Computer Science |
| 9:20 AM to 10:05 AM | ***Cybersecurity Workforce Development and the Department of Defense***<br>Louie Lopez, Director of STEM, US Department of Defense and Star Hardison, Chief of Cyber Workforce Governance Branch, US Department of Defense |
| 10:15 AM to 11:00 AM | ***National Cybersecurity Awareness Month 2023 - How to Stay Safe Online***<br>Derek Mueller, Cyber Security Advisor, US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency |
| 11:10 AM to 11:55 AM | ***Panel Discussion: Building IT and Cybersecurity Careers; From Student to Executive***<br>Tom Dugas, Associate VP and Chief Information Security Officer, Duquesne University Bill Balint, Chief Information Officer, Indiana University of PA, and Todd Cunningham, Executive Director of Information Technology Services, Indiana University of PA |
| 11:55 AM to 1:00 PM | Lunch Break |
| 1:00 PM to 1:05 PM | ***Welcome Back and Afternoon Logistics***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |
| 1:05 PM to 1:10 PM | ***President's Remarks***<br>Michael Driscoll, President, Indiana University of PA |
| 1:10 PM to 1:55 PM | ***An Executive Perspective on Cybersecurity***<br>Susan Koski, Chief Information Security Officer, The PNC Financial Services Group |
| 2:05 PM to 2:50 PM | ***Advanced Computing Ecosystem and Cyber Analytics***<br>Raju Namburu, Chief Technology Officer, US Army Information Technology Laboratory |
| 2:50 PM to 3:05 PM | Afternoon Break |
| 3:05 PM to 3:50 PM | ***Clean Up on Aisle 4: Active Cyber Defenses***<br>Dom Glavach, Chief Security and Technology Officer, CyberSN |
| 3:50 PM to 4:00 PM | ***Event Conclusion***<br>Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science |

# It’s Not a Project:

## *Creating & Maintaining a Sustainable Cybersecurity Program*

Bill Balint, Chief Information Officer

Indiana University of Pa. (IUP)

# Session Goal

*“To share how a data exposure outside of central IT’s responsibility led to the creation of a comprehensive cybersecurity program at a mid-sized public university.*

*A specific goal is to review the components of the program in a manner that would allow other entities to leverage, modify and enhance it for their own purposes.”*

# Agenda

- About IUP
- The Crisis
- Objective 1:  “Begin The Journey at Home”
- Objective 2:  “Get The IT Policy House in Order”
- Objective 3:  “Pass The Word”
- Objective 4:  “Get Some Outside Help”
- Objective 5:  “Make It Sustainable”
- What’s Next?

# About IUP

- Main campus located in Indiana, PA
  - 55 miles from University of Pittsburgh main campus
  - Four small satellite locations in Western Pa.
- Doctoral, High Research Activity Designation
- 9,250 students, 1,350 employees and affiliates
- Member, Pa. State System of Higher Education (PASSHE)
- Five 501(c)3 public, non-profit affiliates

# By The Numbers

- 15,400 active wired network jacks
- 2,400 wireless access points
- 5,700-sq. foot Tier 2 primary data center
- Opened secondary data center in late 2010s
- 16,200 user accounts
- 45 IT employees excluding contractors & student workers
- 1.1 PB of raw storage

# The Crisis – What Happened?

- User published sensitive data on non-IT web server
  - Applicant SSNs, transcripts, addresses, etc.
  - Some were from applicants that had been rejected
- Created substantial investigation to identify exposure
  - Much of the data was on scanned images, requiring manual review of more than 1,000 images

# The Crisis – Reaction

- Significant legal and executive-level engagement
  - Letters to all impacted individuals, some of whom were difficult to find since some of the exposed information was dated

- President had been in place only six weeks
  - Tough explaining why Central IT was unable to address how decentralized web servers were configured, administered and the related data practices

# The Crisis – Resolution

- Security responsibility for ALL servers moved to Central IT

- Challenges were numerous and complex
  - No direct new budget or positions
  - Decentralized IT had existed for 20 years
  - Security (but not server ownership) was transferred to Central IT
  - Some systems administered by unionized, tenured faculty

# The Crisis - Resolution

- Challenges (cont.)
  - Dean of College ‘responsible’ was interim, tenured faculty member
  - Some deans and several faculty did not agree with decision to further empower Central IT
  - Central IT had its own ‘gaps’ in IT security

- General attitude: *“Why change everything due to the careless behavior of a single person?”*

# Begin The Journey at Home - People

- Raised the priority of cybersecurity in Central IT
  - New job descriptions and setting of expectations
  - Performance evaluations

- Increased cybersecurity professional development for IT staff
  - SANS Institute
  - Gartner
  - REN-ISAC, Internet2, Educause Security Professionals,
  - Pittsburgh Technology Council/CyBurgh Initiative, C-CUE, KINBER

# Begin The Journey at Home - Organization

- Created PASSHE’s first IT Security Office
  - Led by Executive Director of IT Security
    - Direct report to CIO
    - Dedicated four senior-level FTE even though Central IT was losing positions
  - Policies, procedures, guidelines, best practices, etc.
  - Network administration
  - Security-related monitoring, alerts, resolutions, etc.
  - Legal/Right-to-Know engagements (now part of IT compliance)

# Begin The Journey at Home - Investment

- Made tangential major investments
    - Significant upgrades and renovation to primary data center
    - Creation of alternate data center
    - Border firewall
    - Added network monitoring
    - Numerous softwares (such as sensitive data finder, Microsoft A5, etc.)
- Migrated from passwords to passphrases
- Toughened cybersecurity language in SaaS contracts

# Get The IT Policy House in Order

- Avoided re-hashing items embedded in laws or existing policies
  - Examples:  records retention, civility, codes of conduct

- Used procedures, guidelines and/or best practices to address anything where policy was not required

- IT serves only as SMEs for data governance
  - Example: Data Classification Policy

# Get The IT Policy House in Order

- Modernized remaining two IT-centric and one ‘affiliated’ policies – primarily to address cybersecurity
  - Acceptable Use of Information Technology Resources (AUP)
  - Information Protection Policy
  - Email as an Official Means of Communication

- Eliminated other legacy IT-centric policies
- Kept policies very short and to the point

# Get The IT Policy House in Order

- Focus procedures, guidelines, best practices and FAQs
  - Request for Enhanced Privilege Procedure
  - System Administrator Best Practices
  - Mobile Device Security Guidelines
  - Acceptable Use Policy FAQ
- Easier to regulate, administer and modify than policies
- Can add new elements as needs are identified

# Pass The Word – Market/Educate

- Bolstered cybersecurity web presence
  - Cybersecurity mini-site
- Added safe computing practice expectations to new employee and student orientations
  - Freshmen courses, posters, welcome packets, residence hall materials
- Added mandatory annual cybersecurity awareness education program for all employees and affiliates in 2022

# Pass The Word – Market / Educate

- Leveraged ‘teachable’ moments
  - Users responding to phishing schemes (including simulations)
  - Participation in student information literacy events
  - Asked business office to include cybersecurity - FERPA, GLBA training

- Embraced October as a focal point
  - National Cyber Security Month
  - Cybersecurity Day
  - Cybersecurity “tip of the week”, contests, etc.

# Get Some Outside Help – No/Low Cost

- Leveraged free resources
  - National Cyber Security Alliance
    - “Stay Safe Online”
  - Educause, Internet2
  - CIS CSAT annual self-assessment
  - Colleagues in higher education
  - Government Agencies focused on IT security (NIST, FTC)
  - Industry websites and publications

# Get Some Outside Help – No/Low Cost

- Reviewed Educause HECVAT for Cloud Vendor Assessment
- Used CIS critical controls for baseline hardware configurations
- Spent extensive planning time to exploit free resources
- Worked to avoid spikes in third-party engagement, preferring to factor in sustainability - ‘money, people and time’ constraints

# Get Some Outside Help - Investments

- Conducted two third-party ‘simulated audits’
  - Center for Internet Security Critical Security Controls
  - NIST Framework
- Leverage other third-party engagements
  - As needed: PCI compliance and penetration tests
  - On-going: Incident Response Retainer contract
  - One time: Third party to study sensitive data identification techniques
- REN-ISAC membership

# Make It Sustainable – ‘Where to Spend?’

- Increased investment despite overall IT budget reductions
  - MFA
  - Cybersecurity awareness education platform
  - Backup/recovery
  - Border Firewall
  - Specific compute/storage for logs, forensics

# Make It Sustainable – 'Where to Spend?'

- Additional Increased investments
  - Mobile device management
  - Sensitive data identification/data encryption
  - Incident response retainer
  - Endpoint device management
  - Anti-virus, anti-malware, anti-phishing, etc. tools; Microsoft A5

# Make It Sustainable - ‘Forever’

- Largest concern is cybersecurity priority may wane over time and funding for making sustainable investments will falter
  - Will funds exist to:
    - continue expanding toolset?
    - continue maintenance on current tools?
    - fund on-going professional development?
  - Can IT security FTE be maintained as overall IT staffing shrinks
  - *“Big investments do not help if we do not have the money and/or staff to leverage them for the long run”*

# What's Next?

- Continue to enhance the cybersecurity posture of IUP
  - Evolve the toolset, such as endpoint device management
  - Grow cybersecurity awareness education program
  - Continue to meet with executives or board semi-annually
  - Continue cloud move of confidential/sensitive data
  - Implement Identity and Access Management System
  - Grow use of Microsoft A5 capabilities
  - Comply annually with CIS Controls risk mitigation
  - Mature internal IT Security/IT Compliance partnership

# What’s Next?

Most importantly:

***“Constantly remind the university community that cybersecurity needs never go away and are therefore components of a permanent program and not just a collection of projects!”***

# Q&A

Contact information:

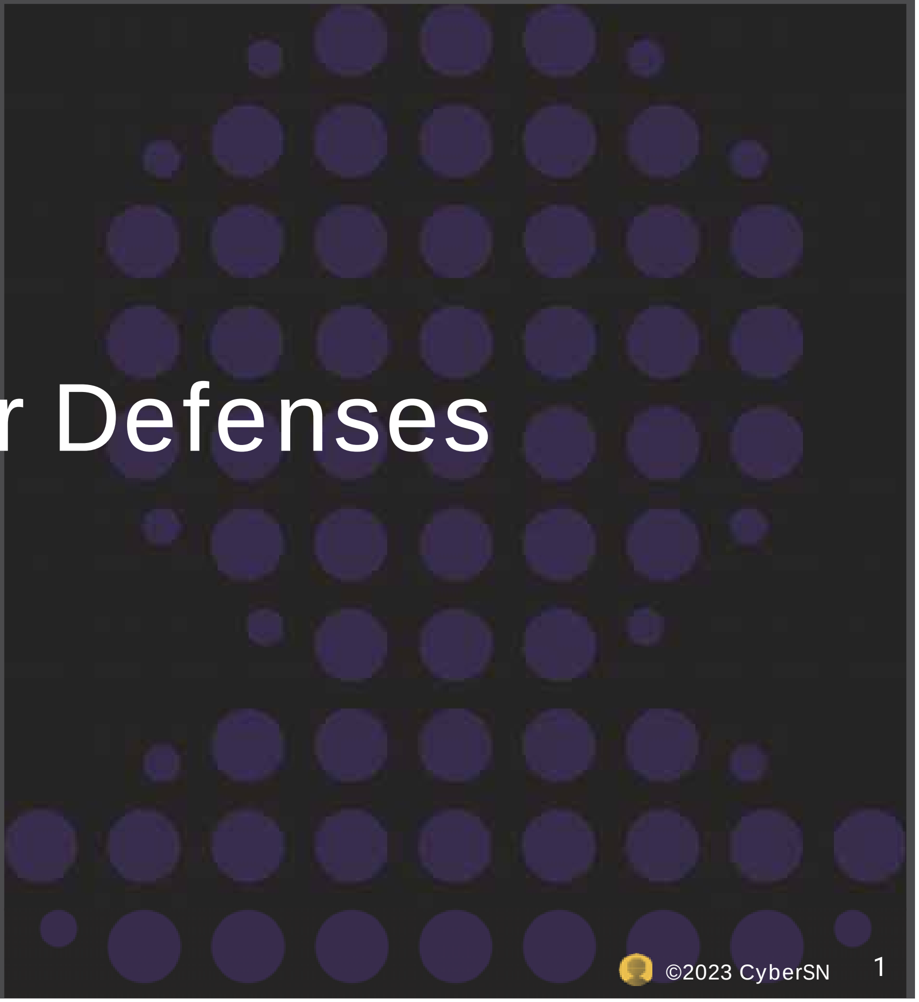
Bill Balint

wsbalint@iup.edu

CyberSN

Pwn your career

# Active Cyber Defenses



2023 Cyber Security Day

Dom Glavach, CISSP

Chief Security and Technology Officer

# Whoami

**Dom Glavach – IUP CS Alumni**

- CISO, Research Fellow, *Red/Blue/Purple*
- Cyber Organization SME
- Cyber Diligence & Breach Assessment (M&E/PE Investments)
- 20+ Government Contactor
- AFCEA Cyber Committee Chair (embedded and vehicle security)
- DNS junkie, prefer IRC over chat and coach a little hockey

**https://CyberSN.com/cybersecurity-career-center**

## Cyber Threat Landscape (reported)

- **9,334** New vulnerabilities in the last 90 days
  - *National Vulnerability Database*
- **40%** year to year increase of interactive attacks
  - *Crowdstrike*
- **1 in 3 breaches** were identified by an organization’s team or tools
  - *IBM Cost of a Data Breach Report*
- **Many many more**
  - *Phishing*
  - *Identity*
  - *Industry*
  - *Cloud vs on-premise*
  - *Time to discover*

## Current Approaches

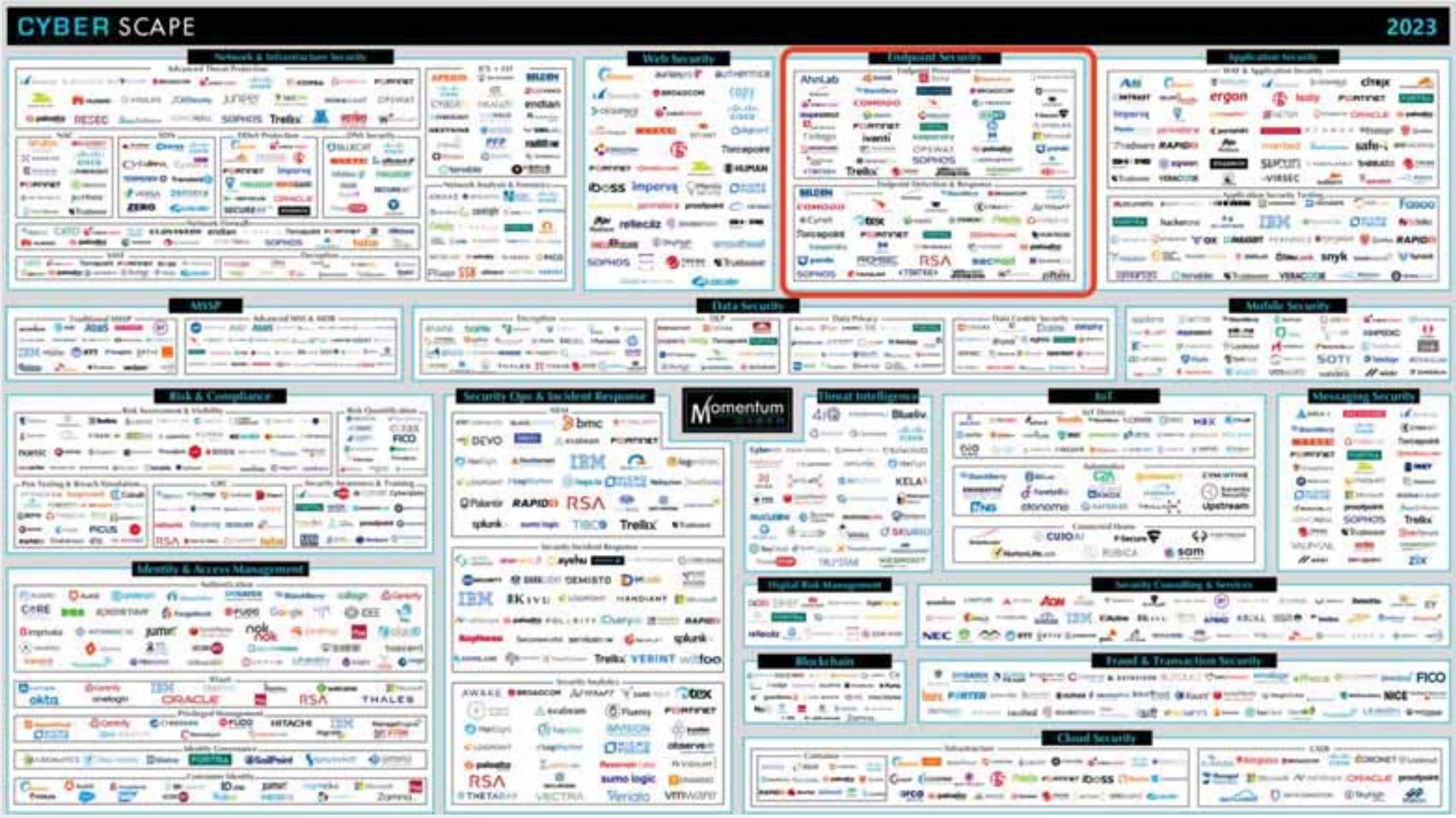
- Evolved over time as perimeters blurred
- Then
  - Patch
  - Defend
  - Detect
  - Respond
- Now
  - Hygiene
  - Identity
  - Visibility
  - Resilience
  - Reporting

Evolved and similar results

## Product overcrowding

- Defense in Depth
  - Founding cyber principle
  - Not intended to become a purchasing strategy
- Complexity
  - Environment/Architecture
  - Regulatory Compliance
  - The People
- Cyber industry and organizations require solutions

# Overcrowding



*Momentum Cyber – Q1 2023 Cybersecurity Market Review*

## Adversaries

- Opportunistic
- Organized (sometimes)
- Innovative
    - LLM
    - Endless examples
- Cost effective *or lazy*
- Persistent and persistence
- Disruptive

***“What keeps you up at night?”***

## Question?

Do you think adversaries can bypass cyber solutions?

## Answer(s)

Depends on who we are asking…

## While (yes)

- From our standpoint (attackers and defender) the answer is: **Yes**
    - Can we detect (discover) the evasion?
    - How long to respond and remediate?
    - How can we build resiliency?

- Better question
    - Can we find the threat before the incident?

- No silver bullets
    - Solutions, Visibility SOAR, IR, Pen Testing, Red Teaming
    - Pairing data, environment and people
        - Threat Hunting

# Flash back

- Evolved over time as perimeters blurred
- Then
  - Patch
  - Defend
  - Detect
  - Respond
- Now
  - Hygiene
  - Identity
  - Visibility
  - Resilience
  - Reporting

**Security Analyst Perspective**

## Threat Hunting

*Threat hunting is a proactive and ongoing cybersecurity practice that aims to uncover hidden threats that may evade traditional security measures. Leveraging people expertise, data analysis, and continuous monitoring to identify and remediate (respond) potential cyber incidents before they can cause significant damage to an organization.*

- Actively searching for advanced adversaries
  - Beacons, anomalies, tactics
  - Environment and activities
    - Point in time hunt example
- Beyond automations and solutions
  - *Can we find the threat before the incident?*

## Attributes

- **Proactivity:** Proactive searching for any unusual or suspicious activities that may indicate a cyber threat.
- **Expertise:** Leverage knowledge, experience, and data to identify potential threats.
- **Continuous:** Continuously monitoring and searching rather than on an ad-hoc basis.
- **Data:** Analyze large volumes of data, including logs, network traffic, and endpoint information, to identify patterns, anomalies, and potential threats.
- **Indicators:** Indicators of compromise (IOCs) and indicators of attack that can be behavioral, technical, or contextual in nature.
- **Hypothesis-Driven:** Develop hypotheses based on the understanding of the organization's environment and the evolving threat landscape.
- **Collaborative:** Collaboration between different cybersecurity teams, incident responders, analysts, and  leadership to share information and insights.
- **Evolving:** As threats evolve, threat hunting techniques and strategies must also adapt
- **Prescriptive:** Once a potential threat is identified, mitigate and initiate remediation measures.

## Common Threat Hunting Models

- **Intel-based Hunting:** Information from threat intelligence sources
  - IoCs, hash values, IP addresses, domain names and networks or host artifact
  - Threat Intelligence providers, CERTS, Information Sharing and Analysis Centers (ISACs)
  - Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII)

- **Hypothesis hunting:** Leverages frameworks, and global detection playbooks to identify advanced persistent threat groups and malware attacks
  - Attacker IoAs and TTPs
  - Searching threat actors based on the environment, domain and attack behaviors

- **Custom hunting:** Situational awareness and industry-based hunting methods.
  - Anomalies in the SIEM and EDR tools and is customizable based on environment requirements
  - Targeted attacks and geopolitical issues

## Good Threat Hunters

- Curious
- Informed
- Collaborative

- Building a career
  - Security Analyst
  - Incident Response
  - Threat Intelligence

**Artificial Intelligence impact?**

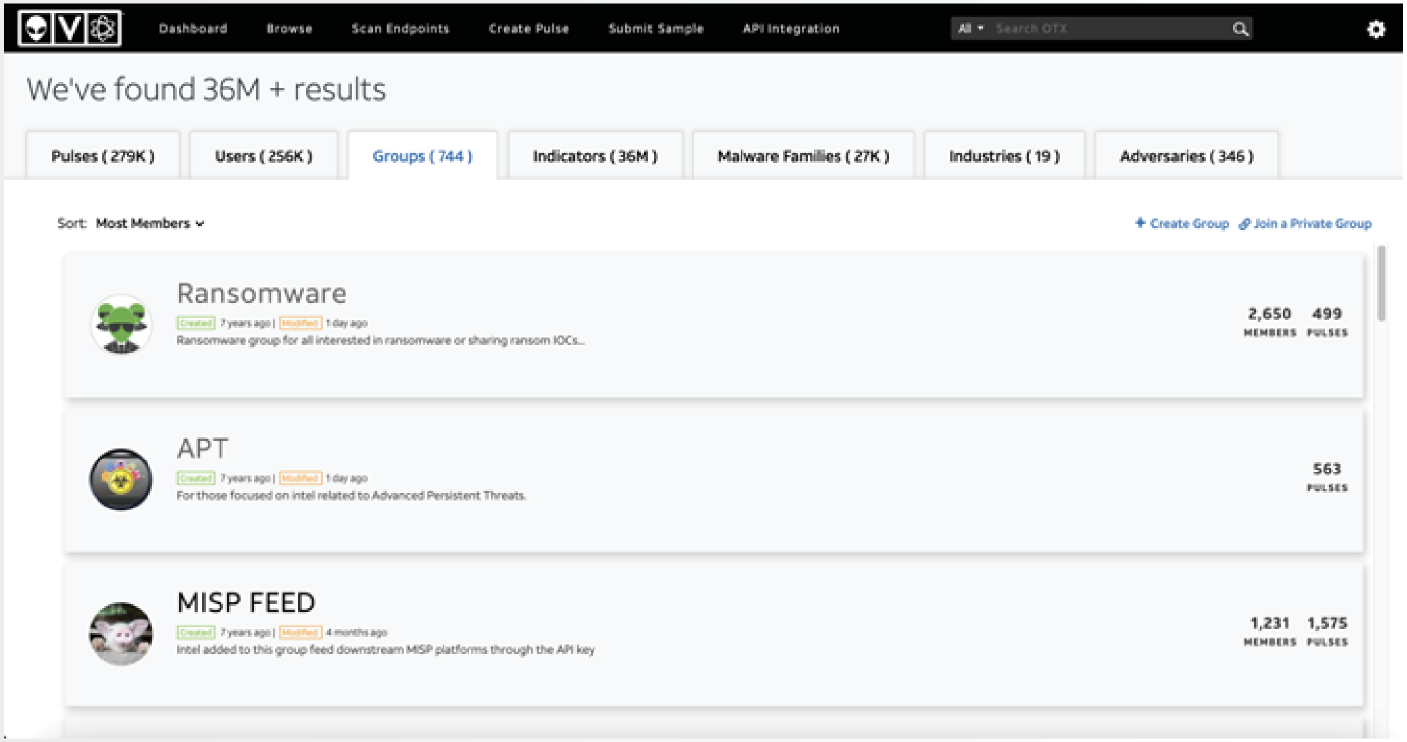
# Available Tools & Resources

- **Threat Intelligence Feeds**
  - Knowing the trends
- **MITRE ATT&CK Framework**
  - Knowing the adversary
- **Velociraptor**
  - Intel-based and custom hunts
- **Real Intelligence Threat Analytics (RITA)**
  - Finding the adversary beacon
- **HTB Hunts**
  - CTF style hunting

## Threat Intelligence Feeds

- **AlienVault – Open Threat Exchange**
  - Personal favorite – free access to over 20 million threat indicators and collaboration
  - **https://otx.alienvault.com/**
- **SANS Internet Storm Center**
  - Daily incident handler diaries summarize and analyze cyber events and new trends
  - **https://isc.sans.edu/**
- **VirusShare Malware Repository**
  - Repository of malware samples – excellent for research, forensics, and hunting
  - **https://virusshare.com/**
- URLhaus (Abuse.ch)
  - Tracks and share malware URLs
  - **https://urlhaus.abuse.ch/browse/**
- FBI InfraGard Portal
  - Information related to the 16 critical infrastructure of sectors.
  - **https://www.infragard.org/** *- Membership may vary*

# AlienVault OTX



We've found 36M + results

Ransomware

Created 7 years ago | Modified 1 day ago

Ransomware group for all interested in ransomware or sharing ransom IOCs...

2,650 MEMBERS 499 PULSES

APT

Created 7 years ago | Modified 1 day ago

For those focused on intel related to Advanced Persistent Threats.

563 PULSES

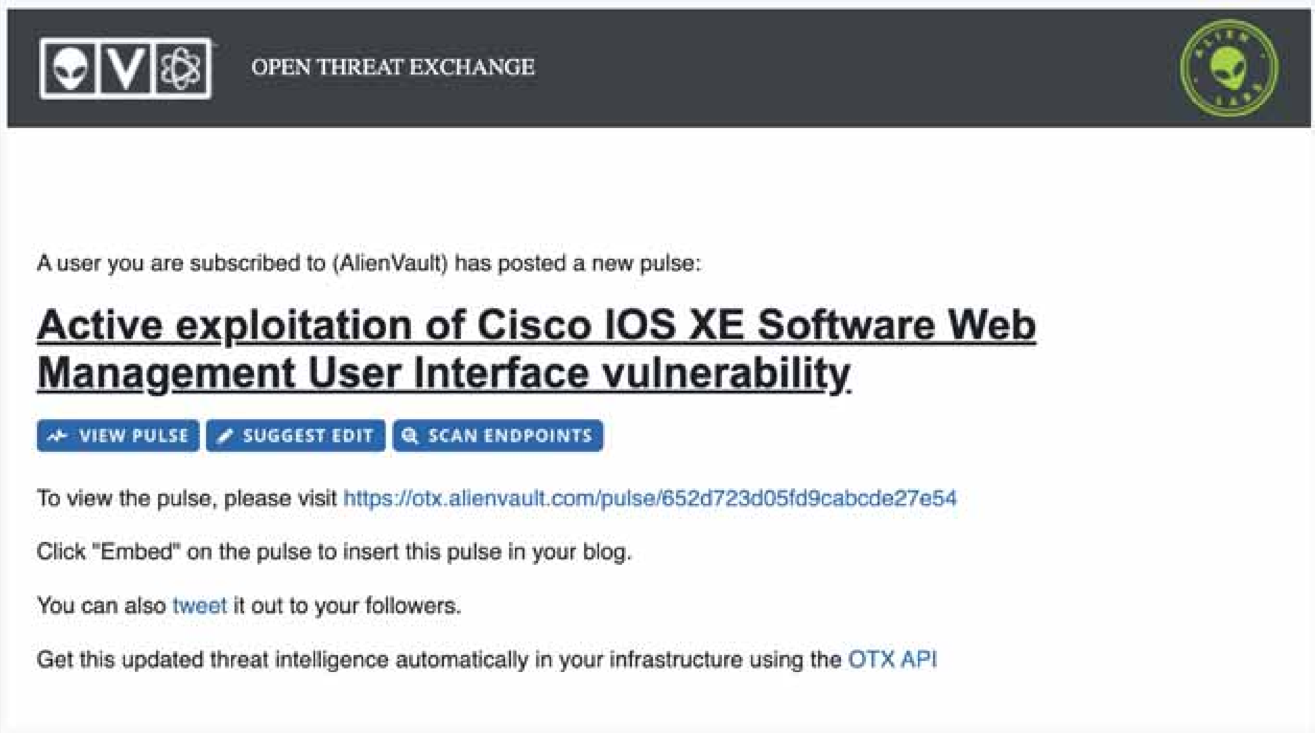
MISP FEED

Created 7 years ago | Modified 4 months ago

Intel added to this group feed downstream MISP platforms through the API key

1,231 MEMBERS 1,575 PULSES

# AlienVault OTX Pulses



A user you are subscribed to (AlienVault) has posted a new pulse:

## Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

To view the pulse, please visit https://otx.alienvault.com/pulse/652d723d05fd9cabcde27e54

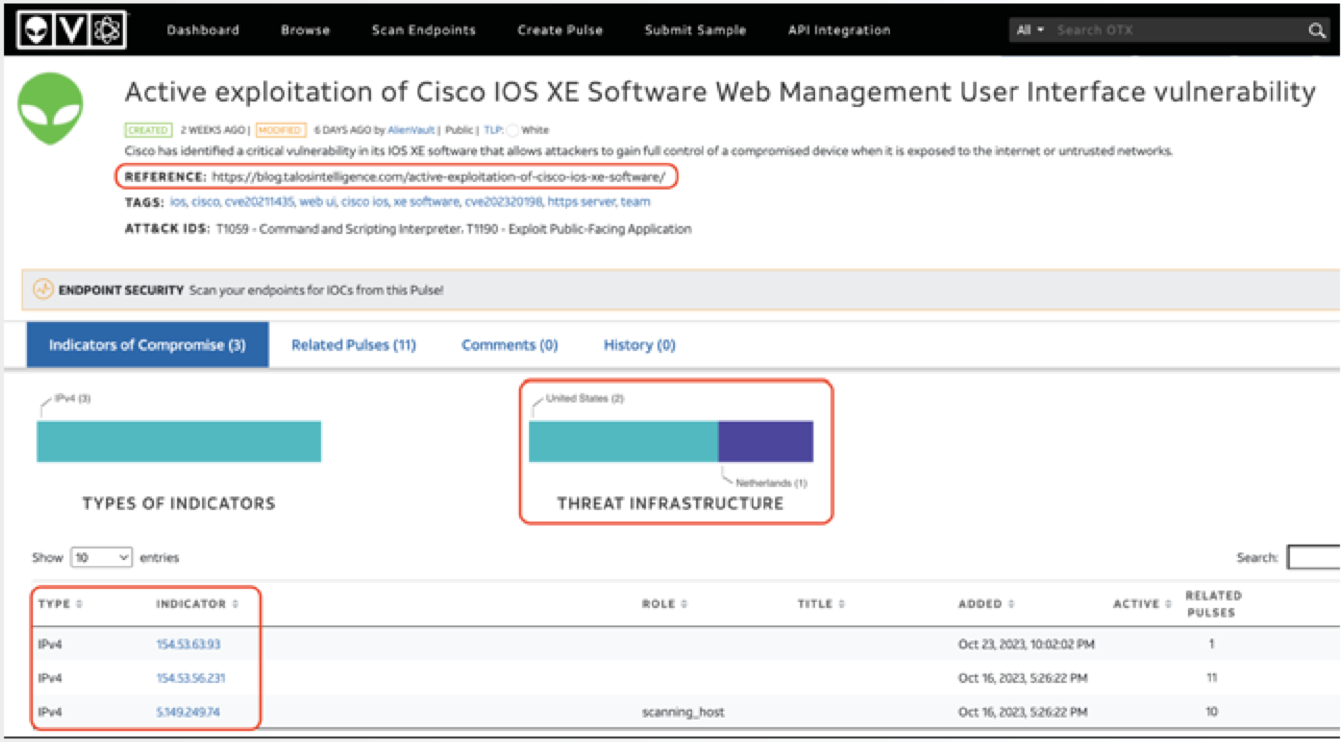
Click "Embed" on the pulse to insert this pulse in your blog.

You can also tweet it out to your followers.

Get this updated threat intelligence automatically in your infrastructure using the OTX API

©2023 CyberSN

# AlienVault OTX Pulses Details



## Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

CREATED 2 WEEKS AGO | MODIFIED 6 DAYS AGO by AlienVault | Public | TLP: ○ White

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks.

**REFERENCE:** https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

**TAGS:** ios, cisco, cve20211435, web ui, cisco ios, xe software, cve202320198, https server, team

**ATT&CK IDS:** T1059 - Command and Scripting Interpreter. T1190 - Exploit Public-Facing Application

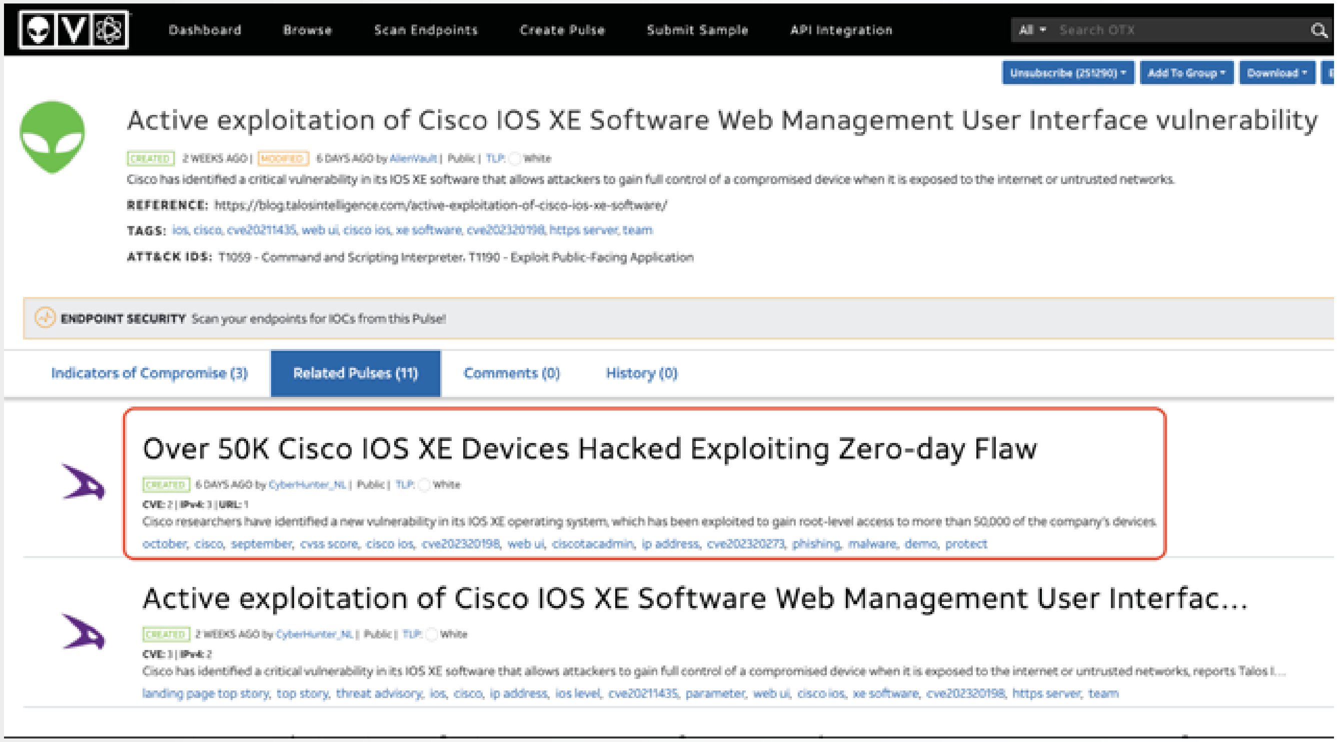
**ENDPOINT SECURITY** Scan your endpoints for IOCs from this Pulse!

Show 10 entries

Search:

| TYPE | INDICATOR | ROLE | TITLE | ADDED | ACTIVE | RELATED PULSES |
|---|---|---|---|---|---|---|
| IPv4 | 154.53.63.93 | | | Oct 23, 2023, 10:02:02 PM | | 1 |
| IPv4 | 154.53.56.231 | | | Oct 16, 2023, 5:26:22 PM | | 11 |
| IPv4 | 5.149.249.74 | scanning_host | | Oct 16, 2023, 5:26:22 PM | | 10 |

# AlienVault OTX Pulses Evolution



## Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability

CREATED 2 WEEKS AGO | MODIFIED 6 DAYS AGO by AlienVault | Public | TLP: White

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks.

**REFERENCE:** https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

**TAGS:** ios, cisco, cve20211435, web ui, cisco ios, xe software, cve202320198, https server, team

**ATT&CK IDS:** T1059 - Command and Scripting Interpreter. T1190 - Exploit Public-Facing Application

**ENDPOINT SECURITY** Scan your endpoints for IOCs from this Pulse!

### Over 50K Cisco IOS XE Devices Hacked Exploiting Zero-day Flaw

CREATED 6 DAYS AGO by CyberHunter_NL | Public | TLP: White

**CVE:** 2 | **IPv4:** 3 | **URL:** 1

Cisco researchers have identified a new vulnerability in its IOS XE operating system, which has been exploited to gain root-level access to more than 50,000 of the company's devices.

october, cisco, september, cvss score, cisco ios, cve202320198, web ui, ciscotacadmin, ip address, cve202320273, phishing, malware, demo, protect

### Active exploitation of Cisco IOS XE Software Web Management User Interfac...

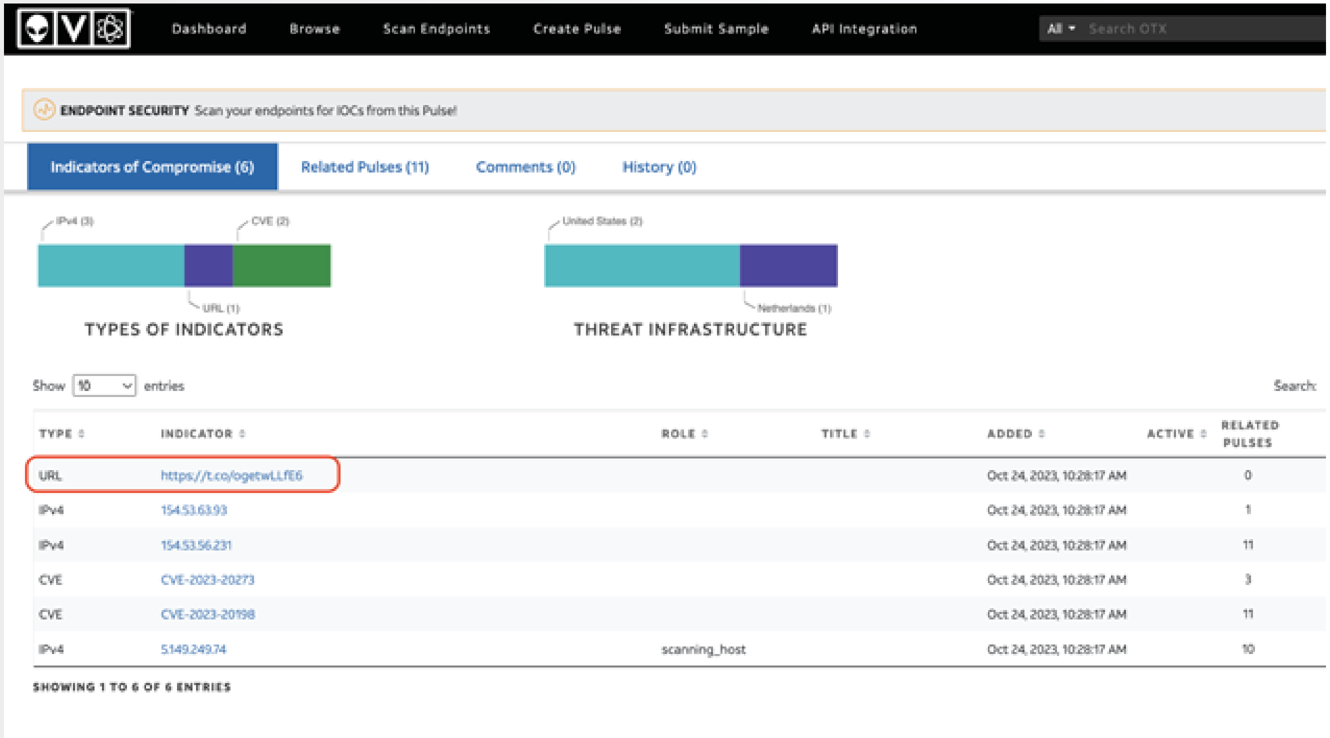
CREATED 2 WEEKS AGO by CyberHunter_NL | Public | TLP: White

**CVE:** 3 | **IPv4:** 2

Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is exposed to the internet or untrusted networks, reports Talos I...

landing page top story, top story, threat advisory, ios, cisco, ip address, ios level, cve20211435, parameter, web ui, cisco ios, xe software, cve202320198, https server, team

# AlienVault OTX Pulses Evolution Details



**ENDPOINT SECURITY** Scan your endpoints for IOCs from this Pulse!

| TYPE | INDICATOR | ROLE | TITLE | ADDED | ACTIVE | RELATED PULSES |
|---|---|---|---|---|---|---|
| URL | https://t.co/ogetwLLfE6 | | | Oct 24, 2023, 10:28:17 AM | | 0 |
| IPv4 | 154.53.63.93 | | | Oct 24, 2023, 10:28:17 AM | | 1 |
| IPv4 | 154.53.56.231 | | | Oct 24, 2023, 10:28:17 AM | | 11 |
| CVE | CVE-2023-20273 | | | Oct 24, 2023, 10:28:17 AM | | 3 |
| CVE | CVE-2023-20198 | | | Oct 24, 2023, 10:28:17 AM | | 11 |
| IPv4 | 5.149.249.74 | scanning_host | | Oct 24, 2023, 10:28:17 AM | | 10 |

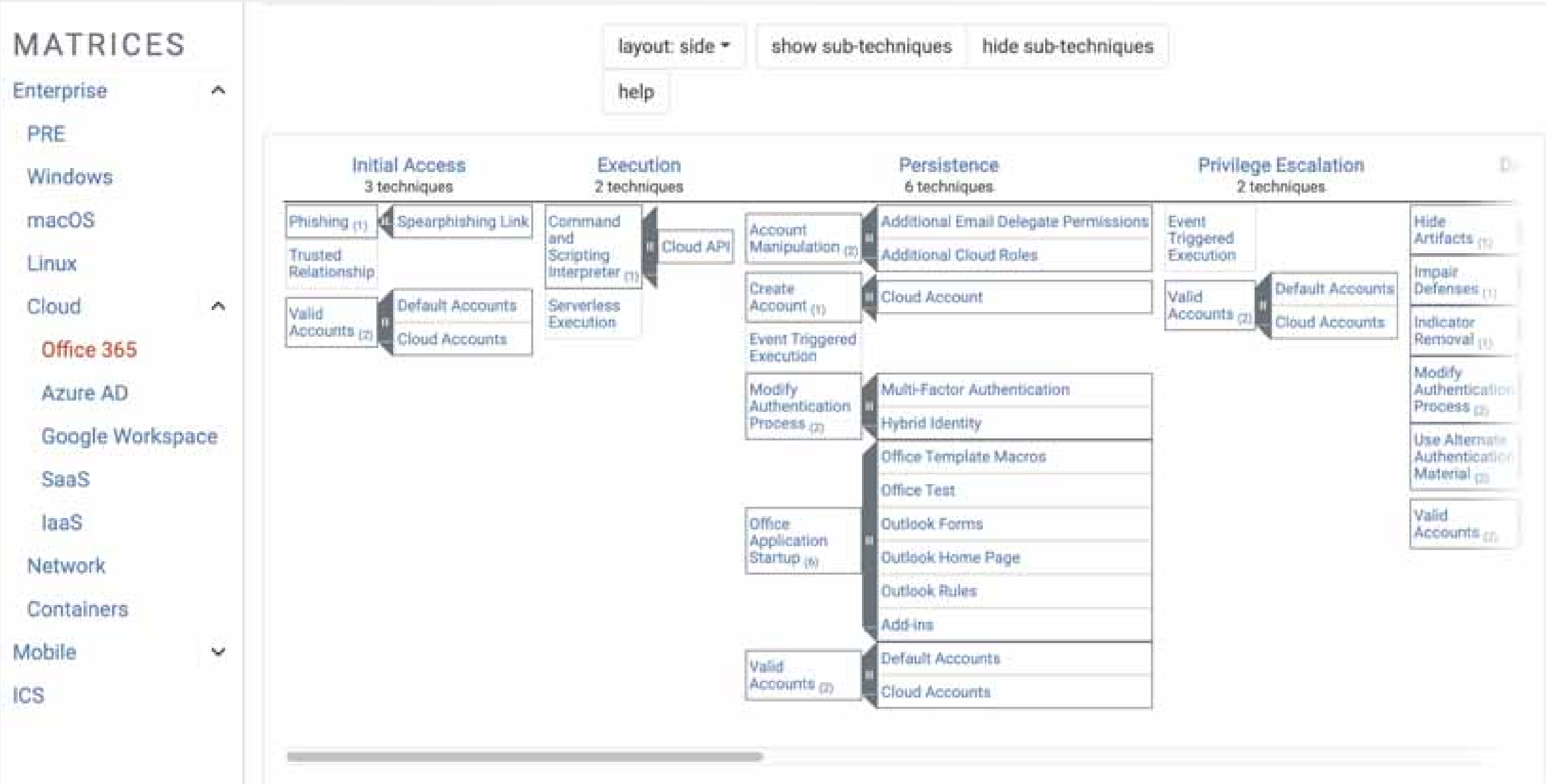
SHOWING 1 TO 6 OF 6 ENTRIES

## MITRE ATT&CK Framework

- ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework
  - Version 14 is being released today (10/31/2023)
  - **https://attack.mitre.org/**

- Starting points
  - **https://attack.mitre.org/matrices/enterprise/**
  - **https://attack.mitre.org/tactics/enterprise/**

# MITRE ATT&CK Framework – Office 365 Matrix



**Initial Access** – 3 techniques

- Phishing (1)
  - Spearphishing Link
- Trusted Relationship
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

**Execution** – 2 techniques

- Command and Scripting Interpreter (1)
  - Cloud API
- Serverless Execution

**Persistence** – 6 techniques

- Account Manipulation (2)
  - Additional Email Delegate Permissions
  - Additional Cloud Roles
- Create Account (1)
  - Cloud Account
- Event Triggered Execution
- Modify Authentication Process (2)
  - Multi-Factor Authentication
  - Hybrid Identity
- Office Application Startup (6)
  - Office Template Macros
  - Office Test
  - Outlook Forms
  - Outlook Home Page
  - Outlook Rules
  - Add-ins
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

**Privilege Escalation** – 2 techniques

- Event Triggered Execution
- Valid Accounts (2)
  - Default Accounts
  - Cloud Accounts

**D**

- Hide Artifacts (1)
- Impair Defenses (1)
- Indicator Removal (1)
- Modify Authenticatio Process (2)
- Use Alternate Authenticatio Material (2)
- Valid Accounts (2)

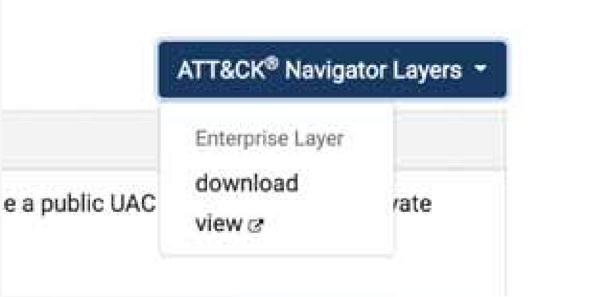
Explore more: **https://attack.mitre.org/matrices/enterprise/cloud/office365/**

# MITRE ATT&CK Navigator

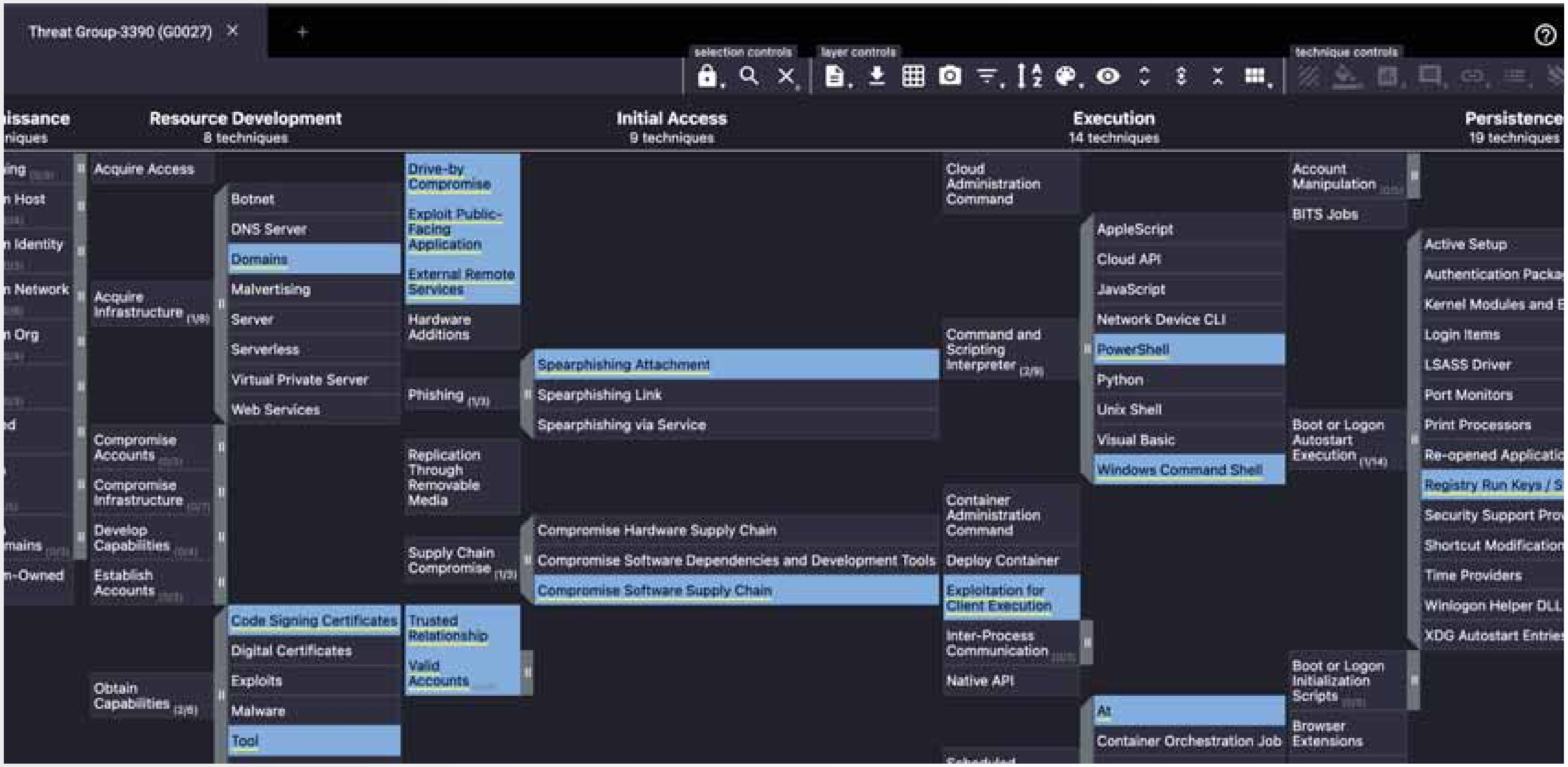
- ATT&CK Interactive navigator
  - Web-based tool for annotating and exploring ATT&CK matrices.
  - Visualize defense coverage, red team planning and more
  - https://mitre-attack.github.io/attack-navigator/

  - Quick sample of comparing two adversary groups
    - **https://youtu.be/78RIsFqo9pM**

  - Also available within the browsable framework



# MITRE ATT&CK Navigator – Threat Group 3390



**…issance**
…niques

- …ing
- …n Host
- …n Identity
- …n Network
- …n Org
- …ed
- …mains
- …n-Owned

**Resource Development**
8 techniques

- Acquire Access
- Acquire Infrastructure (1/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities (2/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool

**Initial Access**
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
- Trusted Relationship
- Valid Accounts

**Execution**
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (2/9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled…
  - At
  - Container Orchestration Job

**Persistence**
19 techniques

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Packa…
  - Kernel Modules and E…
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applicatio…
  - Registry Run Keys / S…
  - Security Support Prov…
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts
- Browser Extensions

©2023 CyberSN

## Velociraptor

- Inspired by Google Rapid Response and OSQuery.
- Hunting endpoint activity
  - Agent-based tool
  - Web Interface and API
  - Velociraptor Query Language (VQL)
  - Strong community support and well documented
  - Other DFIR applications

- Starting point
  - **https://docs.velociraptor.app/**

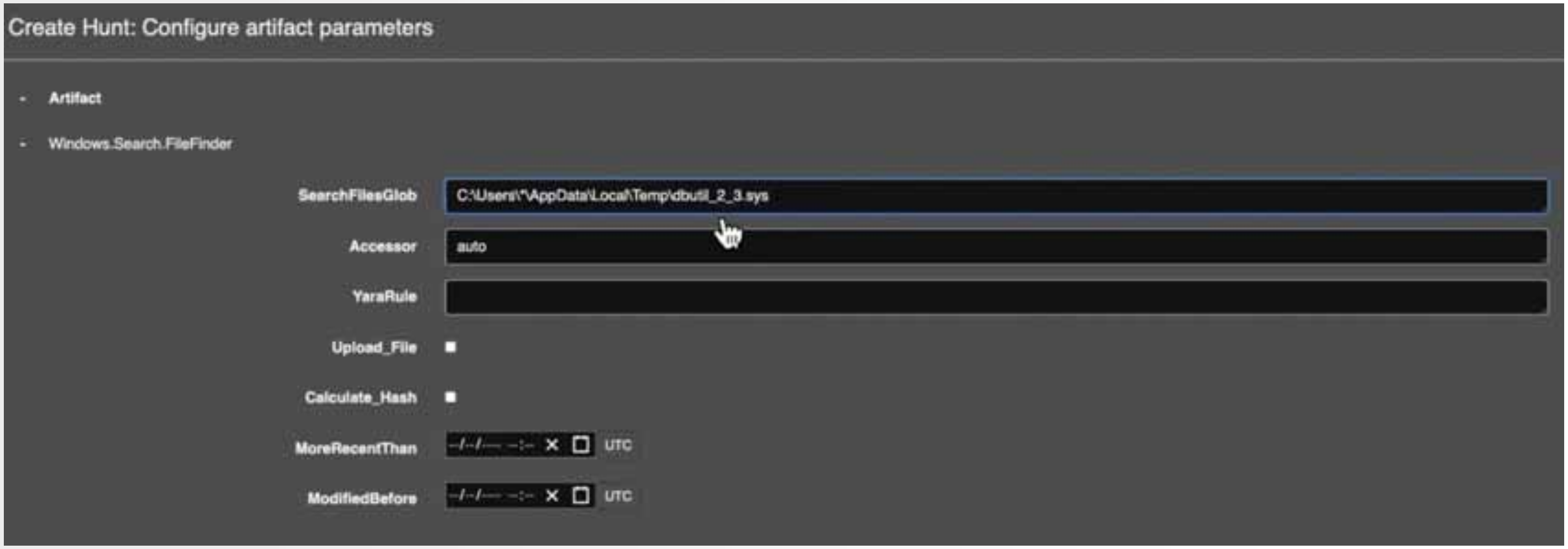
## Velociraptor Hunting

- From basic to complex endpoint hunting
  - Simple file search
  - Complex VQL queries
  - Search the Artifact Exchange
    - MacOS.Application.Firefox.History – Reads firefox history
    - MacOS.UnifiedLogHunter – Live hunting of unified logs

- Labs
  - Server VM
  - Various OS Clients

- Training
  - https://docs.velociraptor.app/training/

# Velociraptor – Basic Hunt

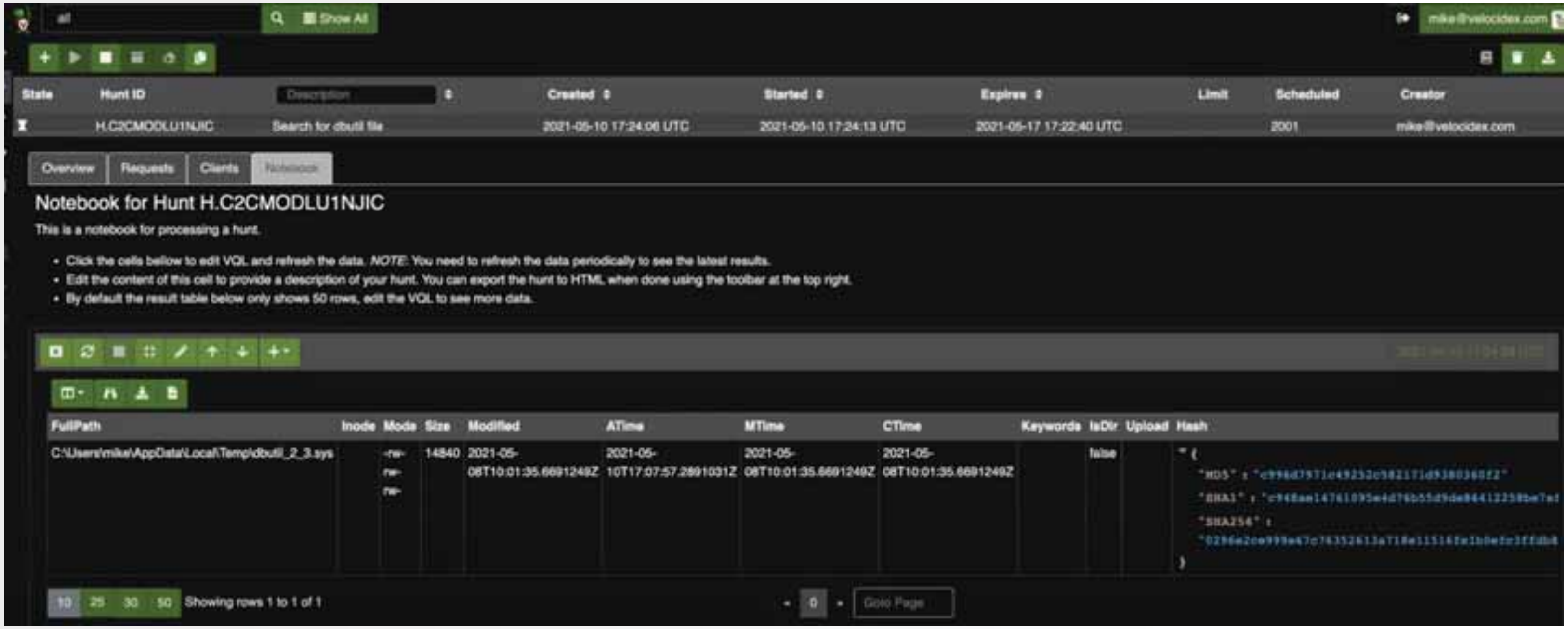


Create Hunt: Configure artifact parameters

- Artifact
- Windows.Search.FileFinder

| | |
|---|---|
| SearchFilesGlob | C:\Users\*\AppData\Local\Temp\dbutil_2_3.sys |
| Accessor | auto |
| YaraRule | |
| Upload_File | □ |
| Calculate_Hash | □ |
| MoreRecentThan | --/--/---- --:-- UTC |
| ModifiedBefore | --/--/---- --:-- UTC |

# Velociraptor – Basic Hunt Results



| State | Hunt ID | Description | Created | Started | Expires | Limit | Scheduled | Creator |
|---|---|---|---|---|---|---|---|---|
| ⧗ | H.C2CMODLU1NJIC | Search for dbutil file | 2021-05-10 17:24:06 UTC | 2021-05-10 17:24:13 UTC | 2021-05-17 17:22:40 UTC |  | 2001 | mike@velocidex.com |

## Notebook for Hunt H.C2CMODLU1NJIC

This is a notebook for processing a hunt.

- Click the cells bellow to edit VQL and refresh the data. *NOTE*: You need to refresh the data periodically to see the latest results.
- Edit the content of this cell to provide a description of your hunt. You can export the hunt to HTML when done using the toolbar at the top right.
- By default the result table below only shows 50 rows, edit the VQL to see more data.

| FullPath | Inode | Mode | Size | Modified | ATime | MTime | CTime | Keywords | IsDir | Upload | Hash |
|---|---|---|---|---|---|---|---|---|---|---|---|
| C:\Users\mike\AppData\Local\Temp\dbutil_2_3.sys |  | -rw-rw-rw- | 14840 | 2021-05-08T10:01:35.6691249Z | 2021-05-10T17:07:57.2891031Z | 2021-05-08T10:01:35.6691249Z | 2021-05-08T10:01:35.6691249Z |  | false |  | ▾ {<br>"MD5" : "c996d7971e49252c982171d9380360f2"<br>"SHA1" : "c948ae14761095e4d76b55d9de86412258be7e<br>"SHA256" :<br>"0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8<br>} |

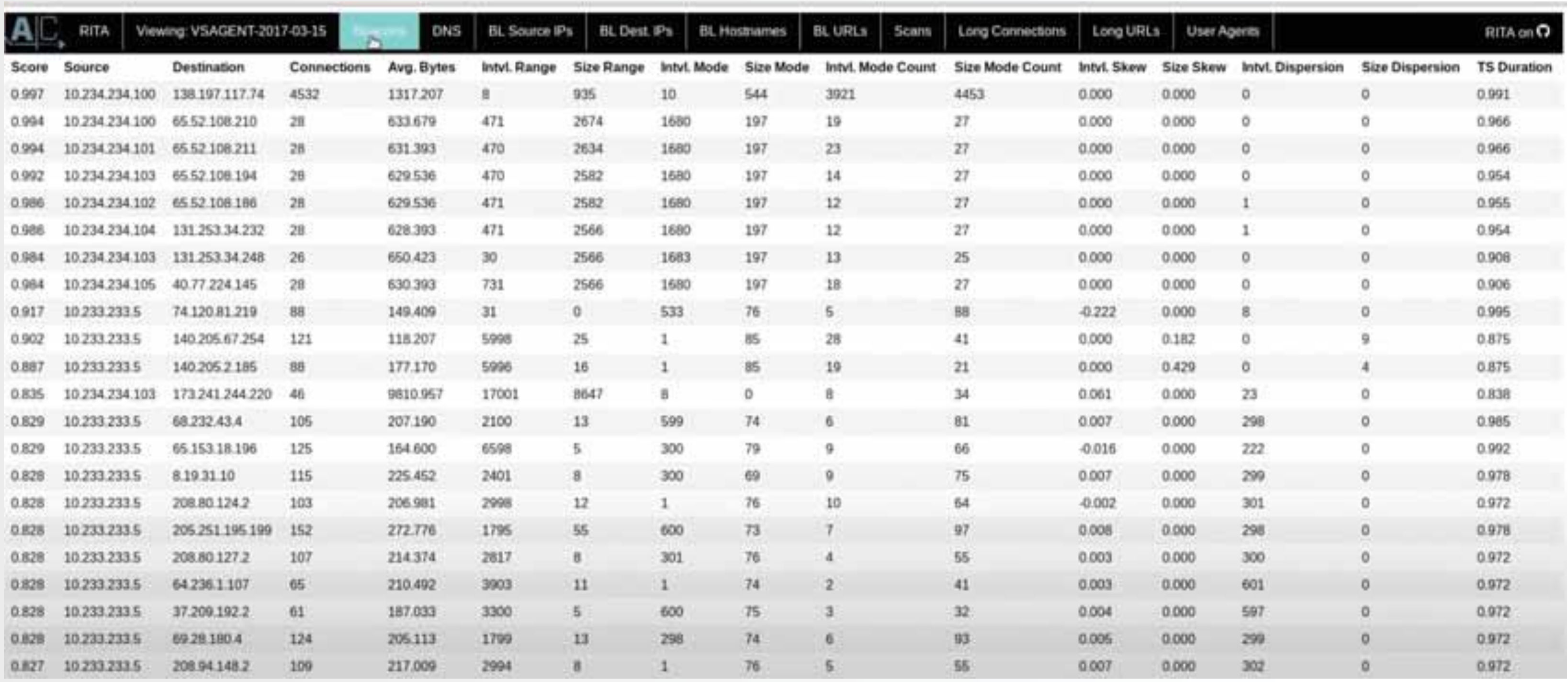
Showing rows 1 to 1 of 1

# RITA

- Real Intelligence Threat Analytics
  - Zeek logs or PCAPs for analysis
  - Beacon hunting using behavior-based analytics
  - DNS Tunnelling and User-Agents
  - Web Interface and CLI

- Starting point
  - https://www.activecountermeasures.com/free-tools/adhd/
    - Active Defense Harbinger Distribution
    - RITA

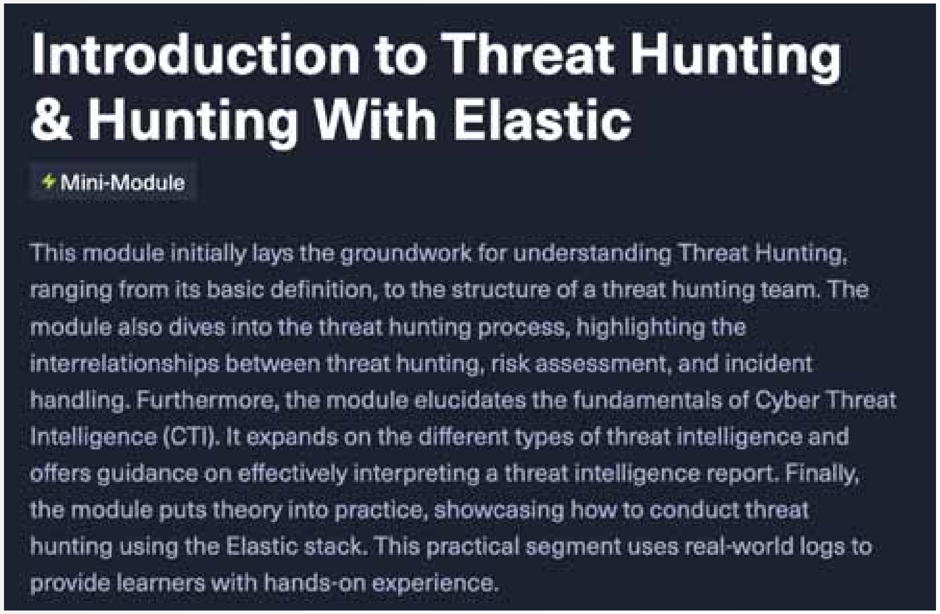
# RITA Beacon Search



| Score | Source | Destination | Connections | Avg. Bytes | Intvl. Range | Size Range | Intvl. Mode | Size Mode | Intvl. Mode Count | Size Mode Count | Intvl. Skew | Size Skew | Intvl. Dispersion | Size Dispersion | TS Duration |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.997 | 10.234.234.100 | 138.197.117.74 | 4532 | 1317.207 | 8 | 935 | 10 | 544 | 3921 | 4453 | 0.000 | 0.000 | 0 | 0 | 0.991 |
| 0.994 | 10.234.234.100 | 65.52.108.210 | 28 | 633.679 | 471 | 2674 | 1680 | 197 | 19 | 27 | 0.000 | 0.000 | 0 | 0 | 0.966 |
| 0.994 | 10.234.234.101 | 65.52.108.211 | 28 | 631.393 | 470 | 2634 | 1680 | 197 | 23 | 27 | 0.000 | 0.000 | 0 | 0 | 0.966 |
| 0.992 | 10.234.234.103 | 65.52.108.194 | 28 | 629.536 | 470 | 2582 | 1680 | 197 | 14 | 27 | 0.000 | 0.000 | 0 | 0 | 0.954 |
| 0.986 | 10.234.234.102 | 65.52.108.186 | 28 | 629.536 | 471 | 2582 | 1680 | 197 | 12 | 27 | 0.000 | 0.000 | 1 | 0 | 0.955 |
| 0.986 | 10.234.234.104 | 131.253.34.232 | 28 | 628.393 | 471 | 2566 | 1680 | 197 | 12 | 27 | 0.000 | 0.000 | 1 | 0 | 0.954 |
| 0.984 | 10.234.234.103 | 131.253.34.248 | 26 | 650.423 | 30 | 2566 | 1683 | 197 | 13 | 25 | 0.000 | 0.000 | 0 | 0 | 0.908 |
| 0.984 | 10.234.234.105 | 40.77.224.145 | 28 | 630.393 | 731 | 2566 | 1680 | 197 | 18 | 27 | 0.000 | 0.000 | 0 | 0 | 0.906 |
| 0.917 | 10.233.233.5 | 74.120.81.219 | 88 | 149.409 | 31 | 0 | 533 | 76 | 5 | 88 | -0.222 | 0.000 | 8 | 0 | 0.995 |
| 0.902 | 10.233.233.5 | 140.205.67.254 | 121 | 118.207 | 5998 | 25 | 1 | 85 | 28 | 41 | 0.000 | 0.182 | 0 | 9 | 0.875 |
| 0.887 | 10.233.233.5 | 140.205.2.185 | 88 | 177.170 | 5996 | 16 | 1 | 85 | 19 | 21 | 0.000 | 0.429 | 0 | 4 | 0.875 |
| 0.835 | 10.234.234.103 | 173.241.244.220 | 46 | 9810.957 | 17001 | 8647 | 8 | 0 | 8 | 34 | 0.061 | 0.000 | 23 | 0 | 0.838 |
| 0.829 | 10.233.233.5 | 68.232.43.4 | 105 | 207.190 | 2100 | 13 | 599 | 74 | 6 | 81 | 0.007 | 0.000 | 298 | 0 | 0.985 |
| 0.829 | 10.233.233.5 | 65.153.18.196 | 125 | 164.600 | 6598 | 5 | 300 | 79 | 9 | 66 | -0.016 | 0.000 | 222 | 0 | 0.992 |
| 0.828 | 10.233.233.5 | 8.19.31.10 | 115 | 225.452 | 2401 | 8 | 300 | 69 | 9 | 75 | 0.007 | 0.000 | 299 | 0 | 0.978 |
| 0.828 | 10.233.233.5 | 208.80.124.2 | 103 | 206.981 | 2998 | 12 | 1 | 76 | 10 | 64 | -0.002 | 0.000 | 301 | 0 | 0.972 |
| 0.828 | 10.233.233.5 | 205.251.195.199 | 152 | 272.776 | 1795 | 55 | 600 | 73 | 7 | 97 | 0.008 | 0.000 | 298 | 0 | 0.978 |
| 0.828 | 10.233.233.5 | 208.80.127.2 | 107 | 214.374 | 2817 | 8 | 301 | 76 | 4 | 55 | 0.003 | 0.000 | 300 | 0 | 0.972 |
| 0.828 | 10.233.233.5 | 64.236.1.107 | 65 | 210.492 | 3903 | 11 | 1 | 74 | 2 | 41 | 0.003 | 0.000 | 601 | 0 | 0.972 |
| 0.828 | 10.233.233.5 | 37.209.192.2 | 61 | 187.033 | 3300 | 5 | 600 | 75 | 3 | 32 | 0.004 | 0.000 | 597 | 0 | 0.972 |
| 0.828 | 10.233.233.5 | 69.28.180.4 | 124 | 205.113 | 1799 | 13 | 298 | 74 | 6 | 93 | 0.005 | 0.000 | 299 | 0 | 0.972 |
| 0.827 | 10.233.233.5 | 208.94.148.2 | 109 | 217.009 | 2994 | 8 | 1 | 76 | 5 | 55 | 0.007 | 0.000 | 302 | 0 | 0.972 |

# HackTheBox Threat Hunting

- Practical threat hunting module
  - https://academy.hackthebox.com/course/preview/introduction-to-threat-hunting--hunting-with-elastic



Introduction to Threat Hunting & Hunting With Elastic

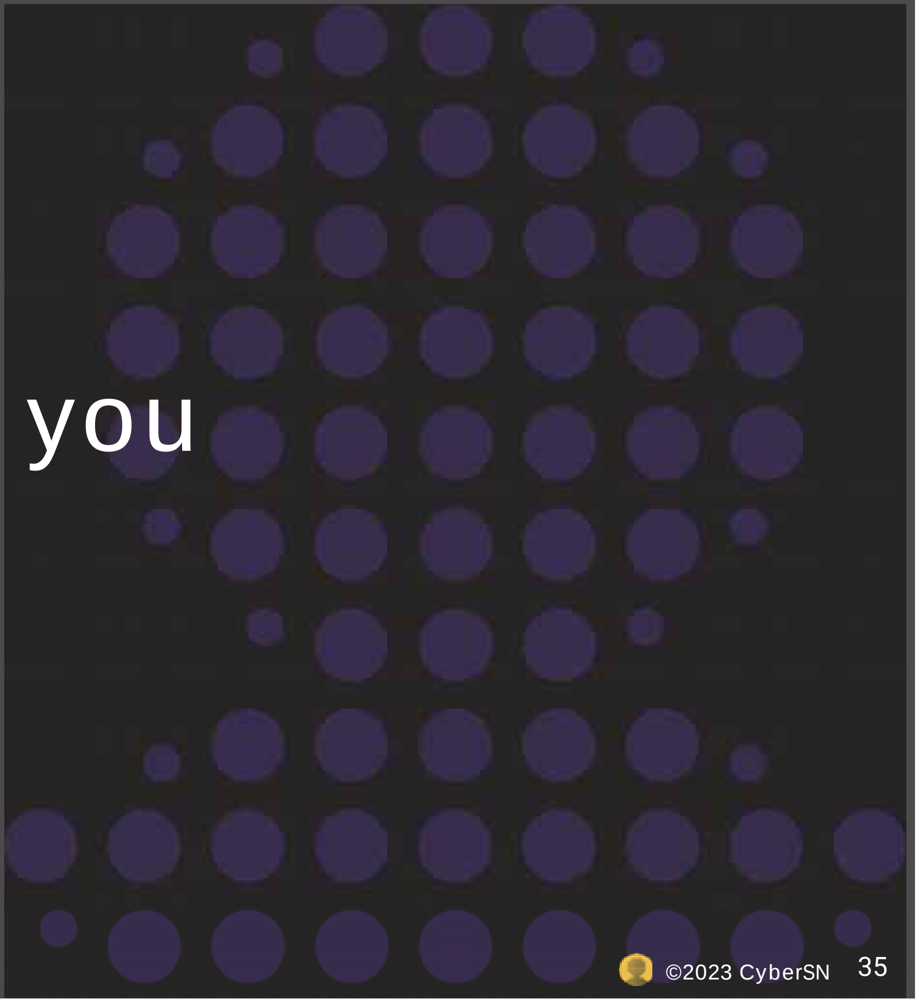
This module initially lays the groundwork for understanding Threat Hunting, ranging from its basic definition, to the structure of a threat hunting team. The module also dives into the threat hunting process, highlighting the interrelationships between threat hunting, risk assessment, and incident handling. Furthermore, the module elucidates the fundamentals of Cyber Threat Intelligence (CTI). It expands on the different types of threat intelligence and offers guidance on effectively interpreting a threat intelligence report. Finally, the module puts theory into practice, showcasing how to conduct threat hunting using the Elastic stack. This practical segment uses real-world logs to provide learners with hands-on experience.

## Additional Resources

- **https://www.crowdstrike.com/resources/reports/threat-hunting-report/**
  - Kerberoasting
- **https://attack.mitre.org/resources/related-projects/**
  - GitHub Repo
  - CASCADE
- **https://github.com/ThreatHuntingProject/hunter**
  - Threat Hunting Project
  - Complete threat hunting and analysis docker image
- **https://www.activecountermeasures.com/free-tools/**
  - Free hunting tools
- **https://www.activecountermeasures.com/hunt-training/**
  - **Free** Threat Hunting training – December 1, 2023 (6 hours)

CyberSN

Pwn your career



# Thank you

DEPARTMENT OF DEFENSE
SCIENCE, TECHNOLOGY, ENGINEERING, MATHEMATICS

# DoD STEM

## Cybersecurity Workforce Development
## 16th Annual Cybersecurity Day at IUP

**Louie Lopez**
*Director, STEM*
Office of the Under Secretary of Defense
for Research and Engineering
Basic Research Office
October 31, 2023

Department of Defense
DoDSTEM
Science · Technology · Engineering · Mathematics

Distro A: approved for public release

dodstem.us

## Why STEM?

# The Department of Defense requires **diverse, high quality, and agile STEM talent**.

National security makes it imperative that the United States have available a **substantial, high quality STEM workforce.**

*(National Academies of Sciences, 2012)*

Distro A: approved for public release

dodstem.us

Why STEM?

# The Need for Diversity in DoD STEM Workforce – **Diversity Drives Innovation**!

Shifting demographics: the U.S. population is projected to be **more than 40% minority** in upcoming decades.

*(Census, 2020)*

Distro A: approved for public release

## Why STEM?

# Preparation of students for future STEM careers **starts at K-12**.

Only **20% of college bound seniors** are ready for courses typically required for a STEM major.

*(National Science Foundation, 2018)*

Distro A: approved for public release

# What encompasses DoD STEM?

DoD STEM is inclusive of Department-wide efforts that aim to **inspire, cultivate, and develop a diverse and exceptional STEM talent** through a continuum of meaningful STEM learning opportunities across the Pre-K-Postdoc continuum.

The **National Defense Education Program** (NDEP) is one of the largest STEM efforts in the Department.

DoD STEM reaches about **944K students** & **31K educators** annually

## DoD STEM Vision

A **diverse and sustainable STEM talent pool** ready to serve our Nation and extend the DoD's competitive edge.

## DoD STEM Mission

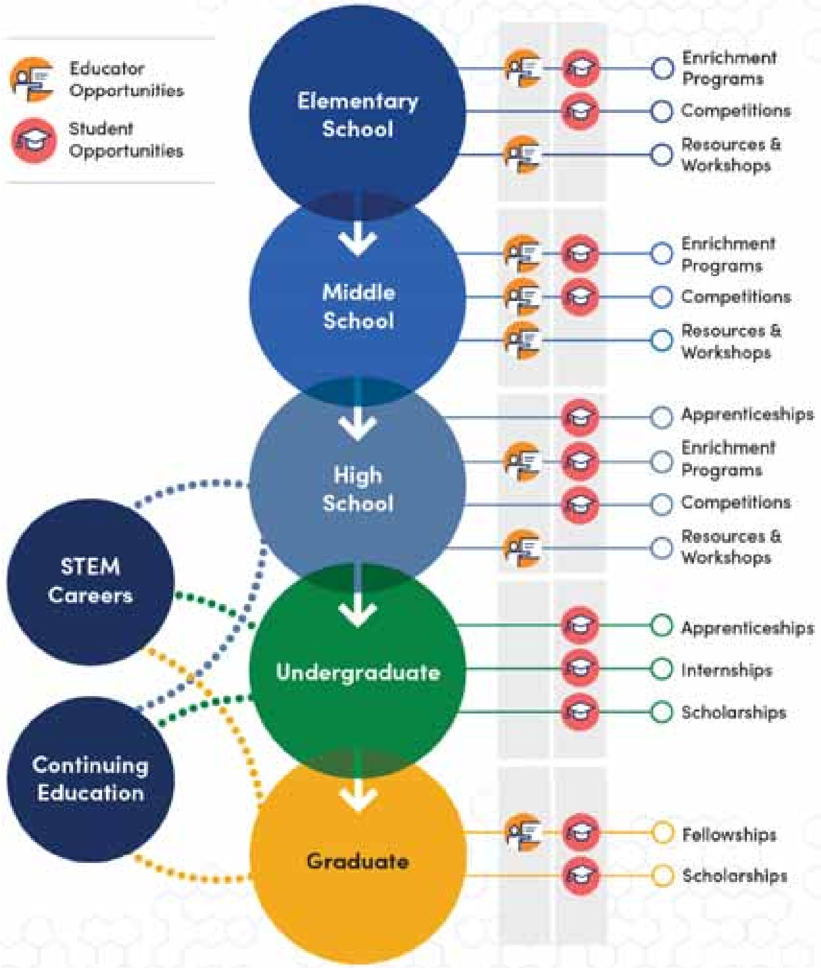
**Inspire, cultivate, and develop exceptional STEM talent** through a **continuum of opportunities** to enrich our current and future DoD workforce poised to tackle evolving defense technological challenges.

Distro A: approved for public release

# DoD STEM Programs and Reach

DoD STEM **engages** scientists and engineers at Defense laboratories and engineering centers, and Partner organizations to provide unique STEM learning experiences across the K-20 education continuum.

Opportunities include **educational programs, internships, scholarships**, and **career development for educators and students**.



Distro A: approved for public release

SMART
SCIENCE, MATHEMATICS, AND RESEARCH FOR TRANSFORMATION
PART OF THE NATIONAL DEFENSE EDUCATION PROGRAM
dodstem.us

SMART
SCIENCE, MATHEMATICS, AND RESEARCH FOR TRANSFORMATION
PART OF THE NATIONAL DEFENSE EDUCATION PROGRAM

# SMART Program Overview

- SMART funds scholarships across 24 STEM disciplines critical to national security and serves as a workforce development program for the DoD
  - Increases the flow of new, highly skilled technical talent into the DoD
  - Enhances the technical skills of the current civilian workforce
- Awards can be made to students pursuing a BS, MS, or PhD in a STEM discipline
- Scholars serve a 1-for-1 Civilian employment commitment at a DoD lab or facility upon graduation
- smartscholarship.org

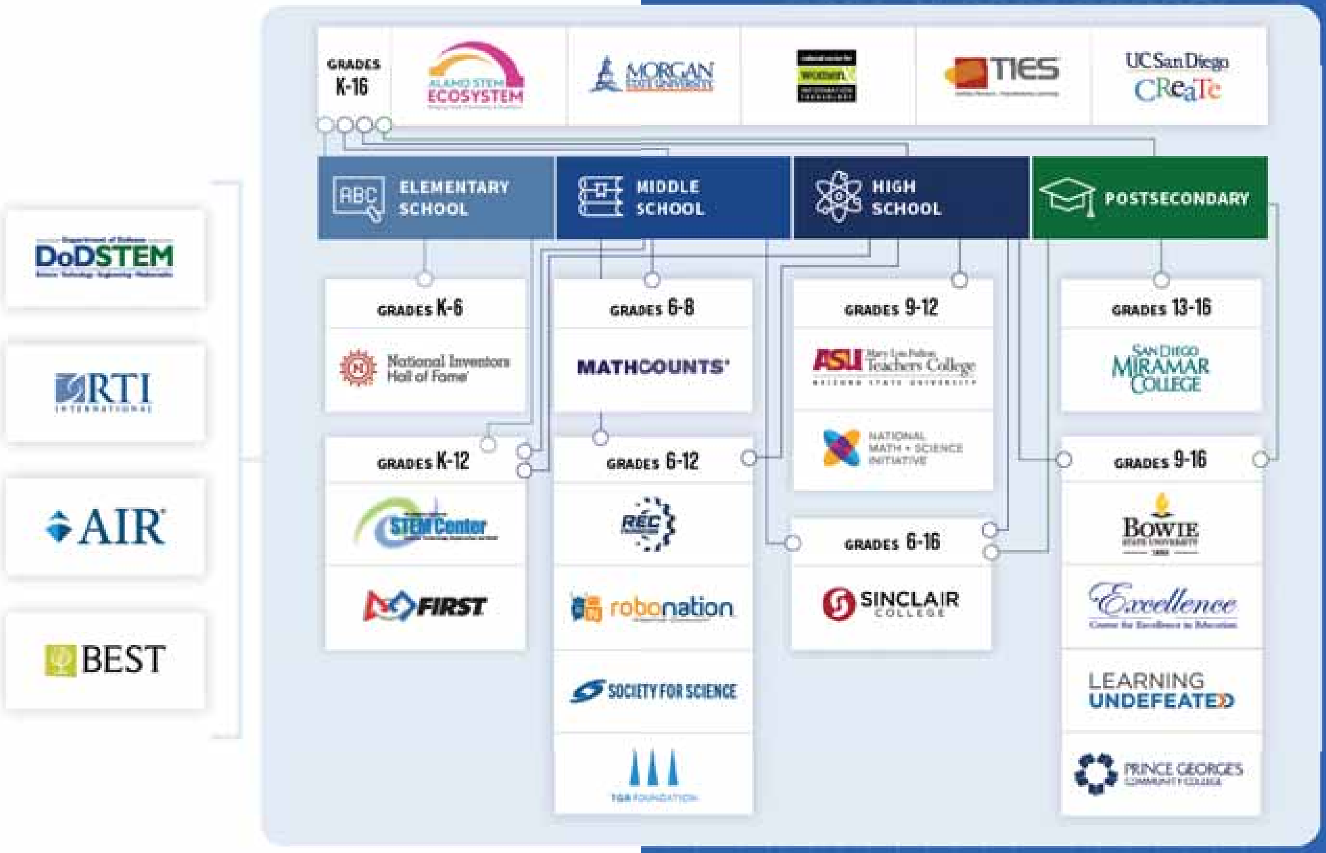
Distro A: approved for public release

# Defense Civilian Training Corps (DCTC): dctc.mil

- DCTC is a congressionally-mandated talent development program that **provides a multidisciplinary, active-learning curriculum** with summer internship projects at DoD organizations.
- Students are selected from **majors such as finance, engineering, sciences, business, and public policy** to join a DCTC cohort at host universities across the United States.
  - Pilot Universities: **North Carolina A&T, Purdue University, The University of Arizona and Virginia Tech**
- Curriculum includes **multidisciplinary capstone projects**.
- Upon graduation, **scholars join the DoD full time** with the support and accelerated **career advancement opportunities** necessary to achieve their professional ambitions

# Defense STEM Education Consortium (DSEC)

**DSEC is a collaborative partnership between academia, industry, not-for-profit organizations, and government** that aims to broaden STEM literacy and develop a diverse and agile future workforce to power the innovative defense infrastructure of the United States.



DoDSTEM
RTI International
AIR
BEST

GRADES K-16
ALAMO STEM ECOSYSTEM
MORGAN STATE UNIVERSITY
National Center for Women & Information Technology
TIES
UC San Diego CReaTe

ELEMENTARY SCHOOL
MIDDLE SCHOOL
HIGH SCHOOL
POSTSECONDARY

GRADES K-6
National Inventors Hall of Fame

GRADES K-12
STEM Center
FIRST

GRADES 6-8
MATHCOUNTS

GRADES 6-12
REC
robonation
SOCIETY FOR SCIENCE
TGR FOUNDATION

GRADES 9-12
ASU Mary Lou Fulton Teachers College Arizona State University
NATIONAL MATH + SCIENCE INITIATIVE

GRADES 6-16
SINCLAIR COLLEGE

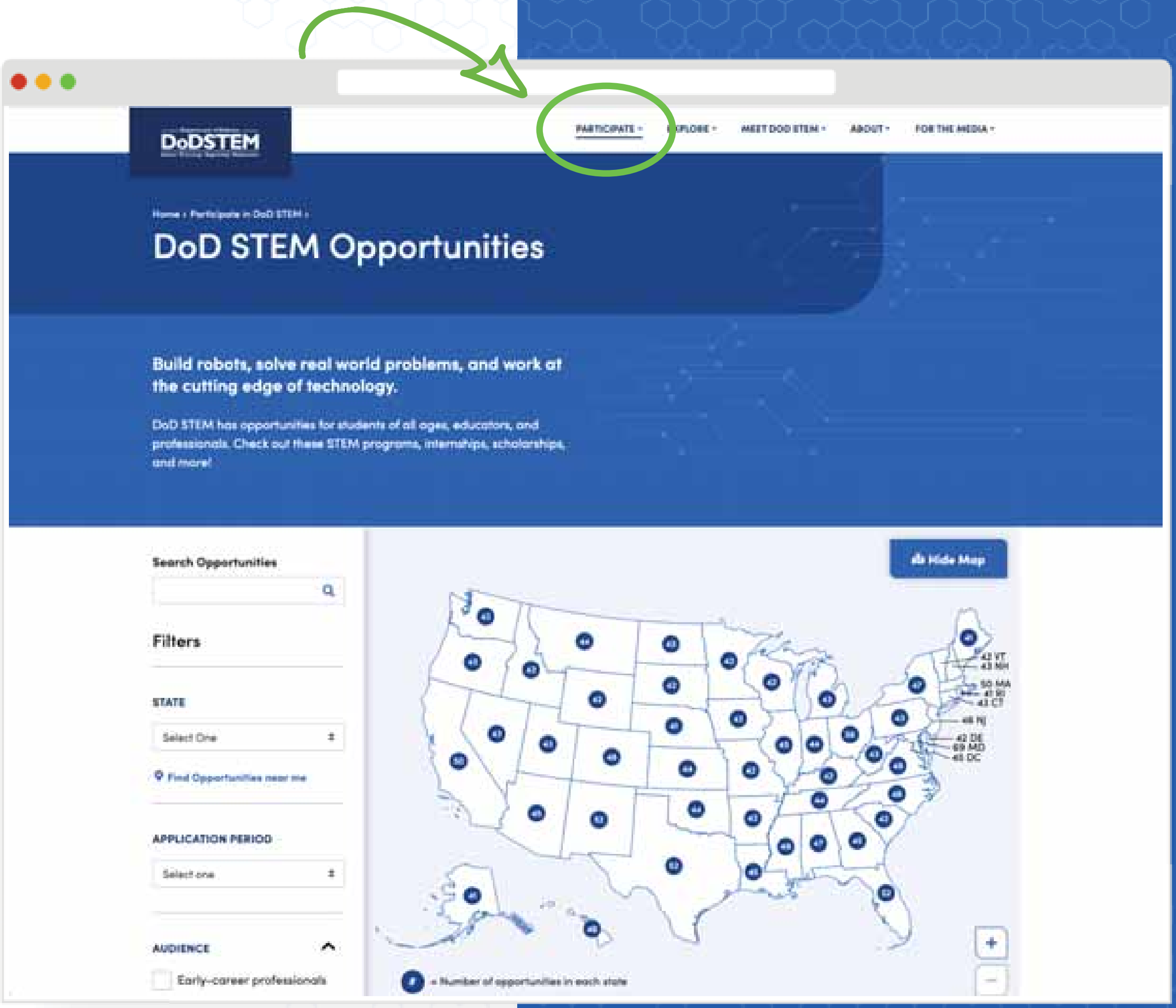
GRADES 13-16
SAN DIEGO MIRAMAR COLLEGE

GRADES 9-16
BOWIE STATE UNIVERSITY
Excellence
LEARNING UNDEFEATED
PRINCE GEORGE'S COMMUNITY COLLEGE

Distro A: approved for public release

# Participate in DoD STEM

dodstem.us/
participate/
opportunities



Home › Participate in DoD STEM ›

DoD STEM Opportunities

Build robots, solve real world problems, and work at the cutting edge of technology.

DoD STEM has opportunities for students of all ages, educators, and professionals. Check out these STEM programs, internships, scholarships, and more!

Search Opportunities

Filters

STATE

Select One

Find Opportunities near me

APPLICATION PERIOD

Select one

AUDIENCE

□ Early-career professionals

# Connect with DoD STEM

Inspiring the future

Science, Technology, Engineering and Mathematics, or STEM, is the gateway to a world of wonder. U.S. Department of Defense (DoD) STEM professionals work at the leading edge of our nation's most advanced technological breakthroughs. **STEM is our future.**

Meet DoD STEM

Participate in STEM

For Students

For Educators

DoD STEM supports a wide variety of activities including after-school programs, competitions, and internships for students and professional development and training for educators. Learn about upcoming STEM opportunities in your area or online.

View All STEM Opportunities

**dodstem.us**

DoDSTEM

@DoDSTEM

@DoDstem

@DoDstem

Distro A: approved for public release

Department of Defense

DoDSTEM

Science · Technology · Engineering · Mathematics

Distro A: approved for public release

# Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY$^{\text{TM}}$)

*Pioneering Mission-Focused Cyber-Spectrum Education for the DoD Workforce*

Chester “CJ” Maciag
Director, Cyber Technologies and Academic Outreach

ASD(CT), Integrated Sensing and Cyber
Office of the Undersecretary of Defense for Research and Engineering

Distribution A: Approved for Public Release

# VICEROY Vision, Mission, and Approach

## Vision

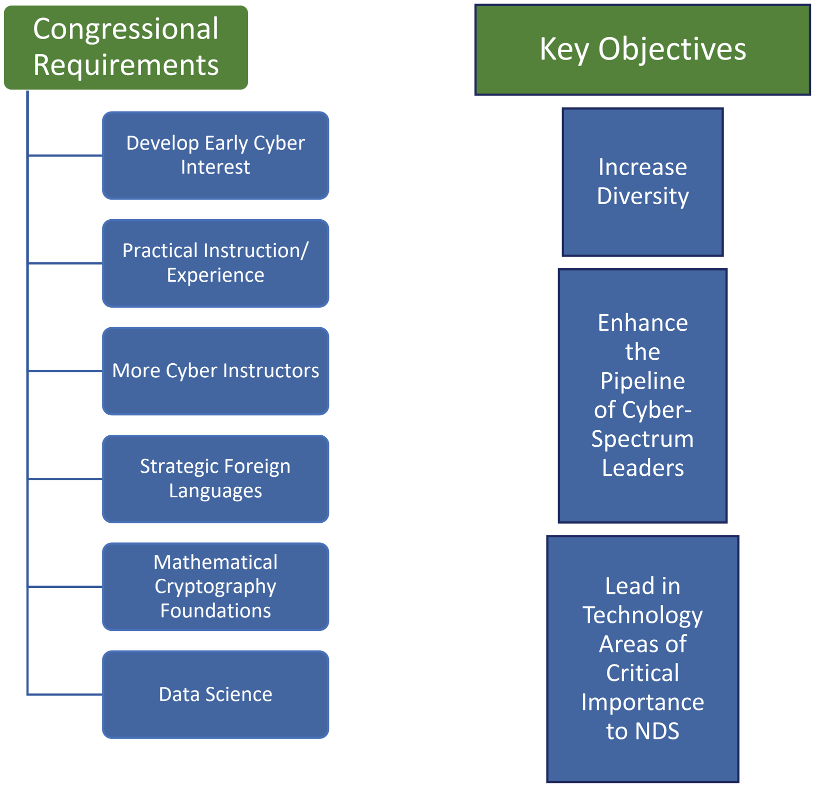
*Recognized by DoD as the leading mission-focused experiential cyber-spectrum operations education and internship pipeline producing job-ready leaders in military, civilian, and industrial base sectors.*

## Mission

Establish academic cyber institutes at institutions of higher learning, to develop foundational expertise in critical cyber operational skills for future military and civilian leaders of the Armed Forces and the Department of Defense, including such leaders of the reserve components.

## Approach

Augment traditional college curricula by providing hands-on, experiential learning and internship opportunities uniquely tailored to match the critical cyber-spectrum workforce demands of the Armed Services, Department of Defense, and our Defense Industrial Base partners.



Congressional Requirements

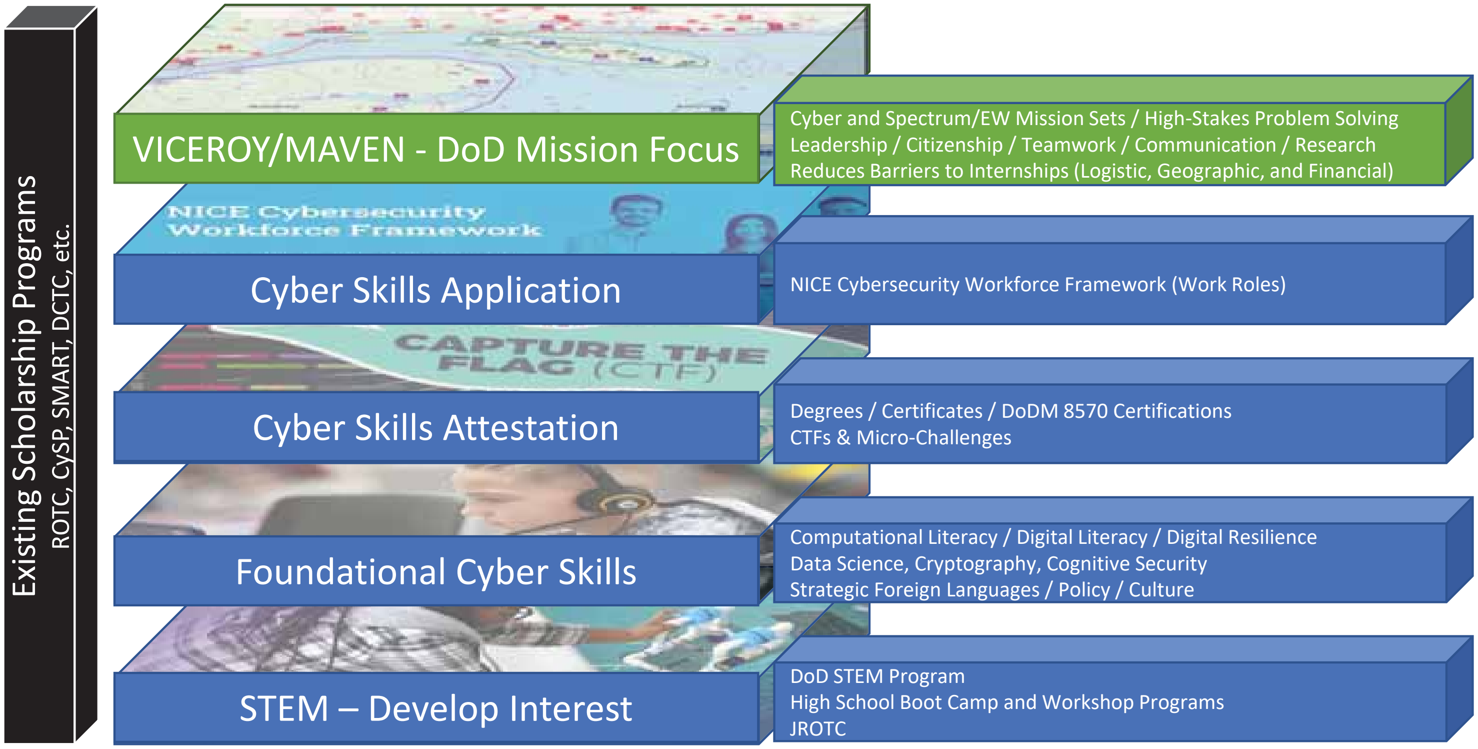
- Develop Early Cyber Interest
- Practical Instruction/ Experience
- More Cyber Instructors
- Strategic Foreign Languages
- Mathematical Cryptography Foundations
- Data Science

Key Objectives

- Increase Diversity
- Enhance the Pipeline of Cyber-Spectrum Leaders
- Lead in Technology Areas of Critical Importance to NDS

# How is VICEROY Different?

**Leveraging and building cyber and EMS programs to prepare students to support DoD missions**



Existing Scholarship Programs
ROTC, CySP, SMART, DCTC, etc.

VICEROY/MAVEN - DoD Mission Focus

Cyber and Spectrum/EW Mission Sets / High-Stakes Problem Solving
Leadership / Citizenship / Teamwork / Communication / Research
Reduces Barriers to Internships (Logistic, Geographic, and Financial)

Cyber Skills Application

NICE Cybersecurity Workforce Framework (Work Roles)

Cyber Skills Attestation

Degrees / Certificates / DoDM 8570 Certifications
CTFs & Micro-Challenges

Foundational Cyber Skills

Computational Literacy / Digital Literacy / Digital Resilience
Data Science, Cryptography, Cognitive Security
Strategic Foreign Languages / Policy / Culture

STEM – Develop Interest

DoD STEM Program
High School Boot Camp and Workshop Programs
JROTC

- DoD and National Security Problem Sets
- Mission-focused Education and Experiential Learning
- Cyber and Spectrum Curriculum
- Strategic Foreign Languages, Data Science/Crypto
- Degrees, Concentrations, and Industry Certifications
- Competitions and Skills Assessment

- Intro to DoD/Service-Specific Missions & Culture
- Cyber and Electromagnetic Spectrum (EMS) emphasis
- Hands-on Cyber and EMS Exercises;
- Blue Book® Mission Vulnerability Assessments
- IEEE Conference-style Paper
- Leadership, Citizenship, Teamwork

VICEROY leverages and aligns foundation of existing cyber programs and scholarships for mission success

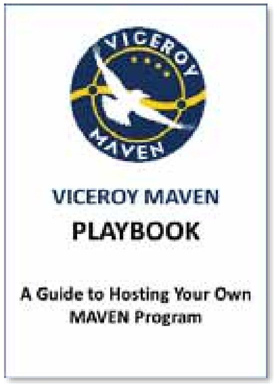
# Mapping the DCWS to VICEROY Activities

VICEROY-Unique Activities Denoted in GREEN

| | | | | | |
|---|---|---|---|---|---|
| *Education Pathway* | Secondary Schools | Undergrad & Graduate Education | Summer Experiential Internship | Follow-Up DoD Internships | DoD Employment |
| *VICEROY Activities* | **Develop early student interest** in challenging DoD and National Security problems sets<br>Enhance the pipeline of **cyber and spectrum students** at the secondary school level<br>Harness summer camps, JROTC, and **dual-enrollment** | **DoD Mission Focus -** Augments traditional college curricula and certifications with hands-on, research-based, operationally-focused experiential learning opportunities for ROTC and civilians<br>**Increases the number of cyber and spectrum instructors** at secondary and collegiate levels | MAVEN 8-week internship hones student competencies in **DoD leadership and culture, teamwork**, and oral and written **communications**<br>Financial assistance through stipends to overcome obstacles, **increase retention, and enhance geographic mobility** | **Provide exciting internship experiences** hosted by engaging and supportive mentors, leading to permanent employment within DoD<br>**Travel and housing stipends** to promote geographical mobility and Quality of Life to promote student satisfaction and success | **Internship Network** helps match students to employers for follow-on internships and permanent jobs<br>**Bridge Hiring Program** provides temporary hiring mechanism to ensure graduating student is retained while they are awaiting completion of final OPM hiring processes |
| *DCWS Pillars* | IDENTIFICATION & RECRUITMENT | RECRUITMENT & DEVELOPMENT | RECRUITMENT & DEVELOPMENT | DEVELOPMENT AND RETENTION | RETENTION |

# 2023 VICEROY MAVEN Summer Internship

- Pedigree and Focus
  - Leverages 20+ years of experience from running the Advanced Course in Engineering Cyber Security Bootcamp (ACE)
  - Leadership, community service, writing, public speaking, research, career day, capstone, bluing trips, and graduation dinner components
- When: 12 June - 4 August 2023 in Rome, NY
  - Standard 8-week program, with 10-week option available
  - 43 first-year interns / 6 graduate assistants (average intern GPA 3.57)
- What's New
  - Air Force / Space Force mission and electromagnetic spectrum (EMS) emphasis
  - Blue Book® cyber vulnerability assessment of a mission system
  - Hands-on cyber and EMS exercises; IEEE conference-style paper
- FY24 Plans - Expanding to Army and Navy in FY24
  - Engaging at Service HQ and organizational element levels



VICEROY MAVEN

PLAYBOOK

A Guide to Hosting Your Own MAVEN Program

# MAVEN Curriculum Elements

| Category | Description |
|---|---|
| 1. Service and DoD Careers | DoD stories of service, career fair |
| 2. Domains/Missions | Immerse in mission-mindset through mission and mission system lectures, Blue Books®, and capstone event |
| 3. Mission Systems | Satellites, UAS, Cyber-enabled Munitions, SCADA, mIoT |
| 4. Core Cyber | OS and Network Fundamentals, CIAAAA, OCO, DCO, AI/ML and cyber |
| 5. Core EMS | Signal generation, transmit/receive, offensive and defensive techniques |
| 6. Leadership and Teamwork | Writing, public speaking, Blue Book®, and research teams |
| 7. Assessment | Writing and speaking rubrics, peer assessment, pre- and post-test |

# National Competition

## Purpose

- Generate early-semester excitement in cyber/spectrum high-stakes problem solving
- Elevate student awareness and pursuit of VICEROY
- Create sense of community and pride among VICEROY post-secondary institutions

## When

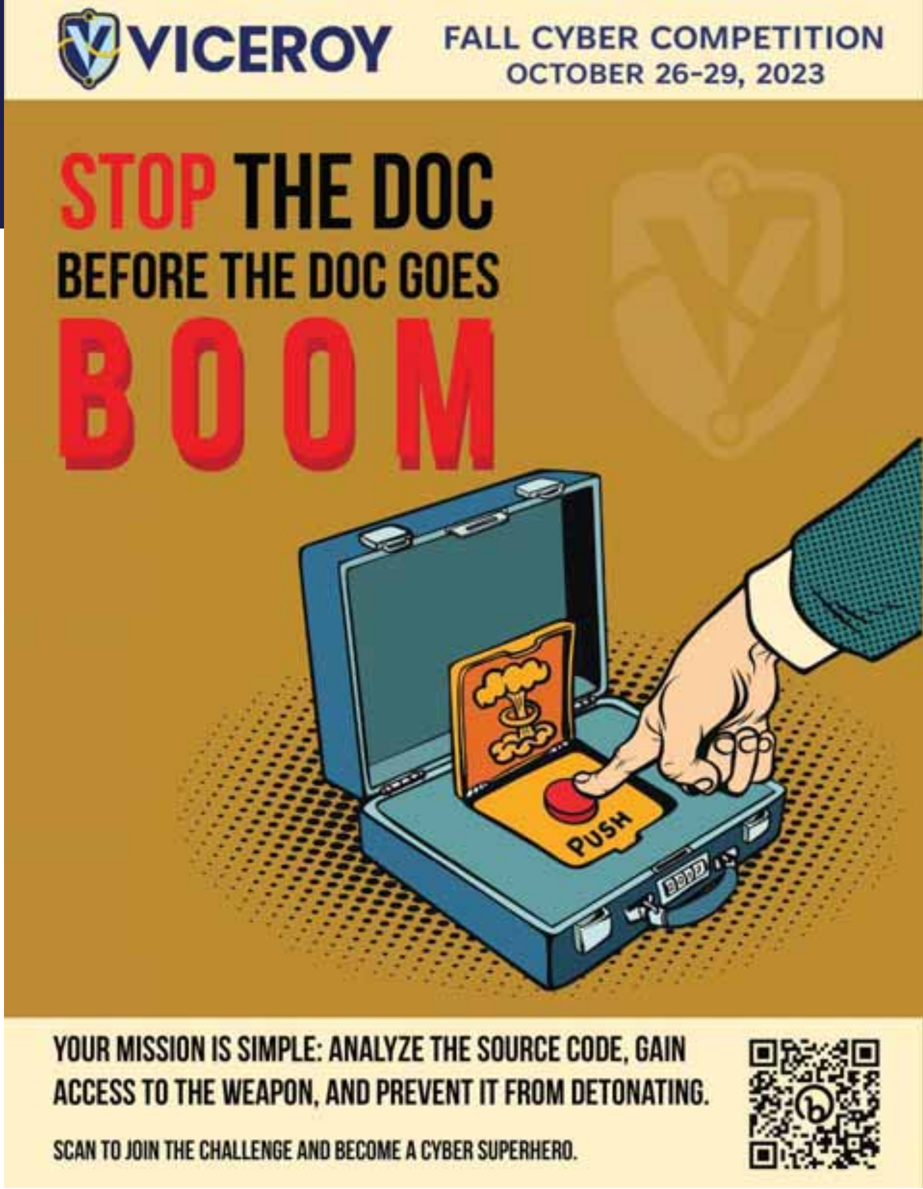
- October 26-29, 2023

## Format

- Online virtual competition
- Run by AFRL and GI Blue Edge Team

## Teams

- 20 teams registered for the competition
- Each team must have at least one VICEROY student
- Recommend 3-5 students per team



VICEROY

FALL CYBER COMPETITION
OCTOBER 26-29, 2023

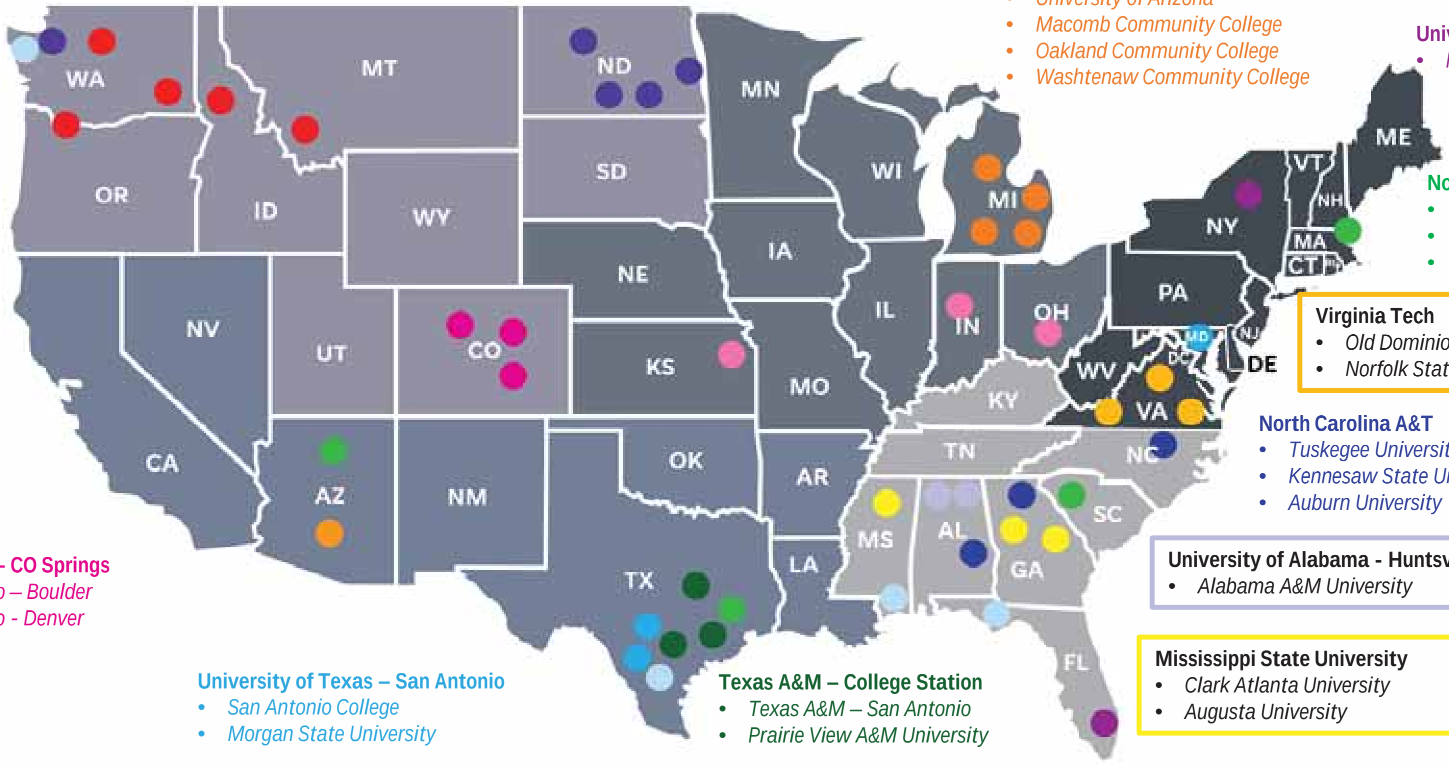
STOP THE DOC
BEFORE THE DOC GOES
BOOM

YOUR MISSION IS SIMPLE: ANALYZE THE SOURCE CODE, GAIN ACCESS TO THE WEAPON, AND PREVENT IT FROM DETONATING.

SCAN TO JOIN THE CHALLENGE AND BECOME A CYBER SUPERHERO.

# FY23 VICEROY Regional VIs and Partners

## Slate Blue - Operational Internship Sites with MOAs: Keyport, JBSA, Keesler, and Eglin



**North Dakota State University**
- *City University of Seattle*
- *Minot State University*
- *Bismarck State College*

**University of Kansas**
- *Ohio State University*
- *Purdue University Northwest*

**University of Detroit Mercy**
- *University of Arizona*
- *Macomb Community College*
- *Oakland Community College*
- *Washtenaw Community College*

**University at Albany**
- *Florida International University*

**Washington State University**
- *Central Washington University*
- *Columbia Basin College*
- *Montana State University*
- *University of Idaho*

**Northeastern University**
- *Northern Arizona University*
- *University of Houston*
- *University of South Carolina*

**Virginia Tech**
- *Old Dominion University*
- *Norfolk State University*

**North Carolina A&T**
- *Tuskegee University*
- *Kennesaw State University*
- *Auburn University*

**University of Alabama - Huntsville**
- *Alabama A&M University*

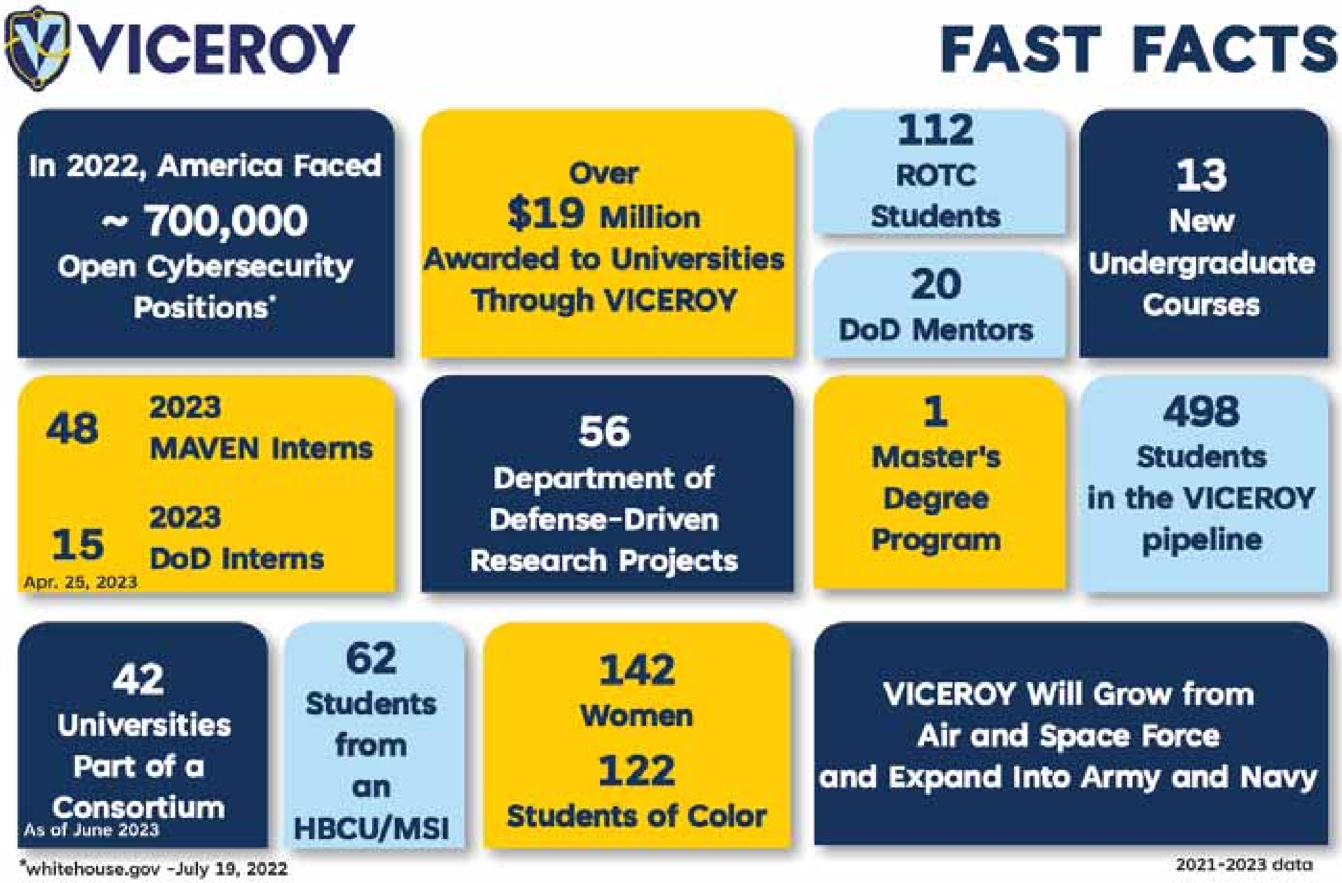
**University of Colorado – CO Springs**
- *University of Colorado – Boulder*
- *University of Colorado - Denver*

**University of Texas – San Antonio**
- *San Antonio College*
- *Morgan State University*

**Texas A&M – College Station**
- *Texas A&M – San Antonio*
- *Prairie View A&M University*

**Mississippi State University**
- *Clark Atlanta University*
- *Augusta University*

# By the numbers…
# Subset of our 30-month Accomplishments



VICEROY FAST FACTS

In 2022, America Faced ~ 700,000 Open Cybersecurity Positions*

Over $19 Million Awarded to Universities Through VICEROY

112 ROTC Students

20 DoD Mentors

13 New Undergraduate Courses

48 2023 MAVEN Interns

15 2023 DoD Interns

Apr. 25, 2023

56 Department of Defense-Driven Research Projects

1 Master's Degree Program

498 Students in the VICEROY pipeline

42 Universities Part of a Consortium

As of June 2023

62 Students from an HBCU/MSI

142 Women

122 Students of Color

VICEROY Will Grow from Air and Space Force and Expand Into Army and Navy

*whitehouse.gov -July 19, 2022

2021-2023 data

## Programs of Study

- 13 New Undergrad Courses
- 9 Seminars

## Academics

- Multitude of Cyber Certification Track Courses Developed and Awarded

## 18 DoD Participant Employers

- AF – Keesler, Fairchild, Eglin, JBSA, AFRL
- Army – Ft. Gordon, GVSC
- Navy – NUWC Keyport

VICEROY

# Thank You!

VICEROY MAVEN Flag Bearers at the 2023 Honor America Days at Ft. Stanwix, Rome NY

VICEROY Landing Page: https://adobe.ly/3pwEGaV

Mr. Chester “CJ” Maciag
Director, Cyber Technologies and Academic Outreach

ASD(CT), Integrated Sensing and Cyber
Office of the Undersecretary of Defense for Research and Engineering
Chester.j.Maciag.civ@mail.mil // (571) 969-0692

# TAB 1 – VICEROY Backup Information

# Wrap-up

- DoD faces challenges in recruiting top cyber and spectrum student talent
  - Students lack knowledge of uniquely challenging DoD problem sets and career rewards
  - Most post-secondary program curricula fail to prepare graduates for DoD mission success
  - Numerous talent pipeline barriers discourage students from pursuing DoD internships/employment
- USD(R&E) addressing these challenges through VICEROY program
  - Authorized by Section 1640 of the NDAA for 2019; Appropriations over FY20-23 totaling $40M
- VICEROY success to date:
  - 13 Virtual Institutes; 45 Academic institutions; Locations in all major U.S. regions
  - 498 VICEROY Students (112 ROTC, 122 female, 112 minority)
  - 55 DoD-relevant student projects; 13 new courses; 1 new M.S. in Cybersecurity Engineering
  - 18 Participating employers; 4 major internship centers via 3 MOAs and 1 EPA
  - MAVEN – Our premiere summer experiential internship (48 participants summer 2023)

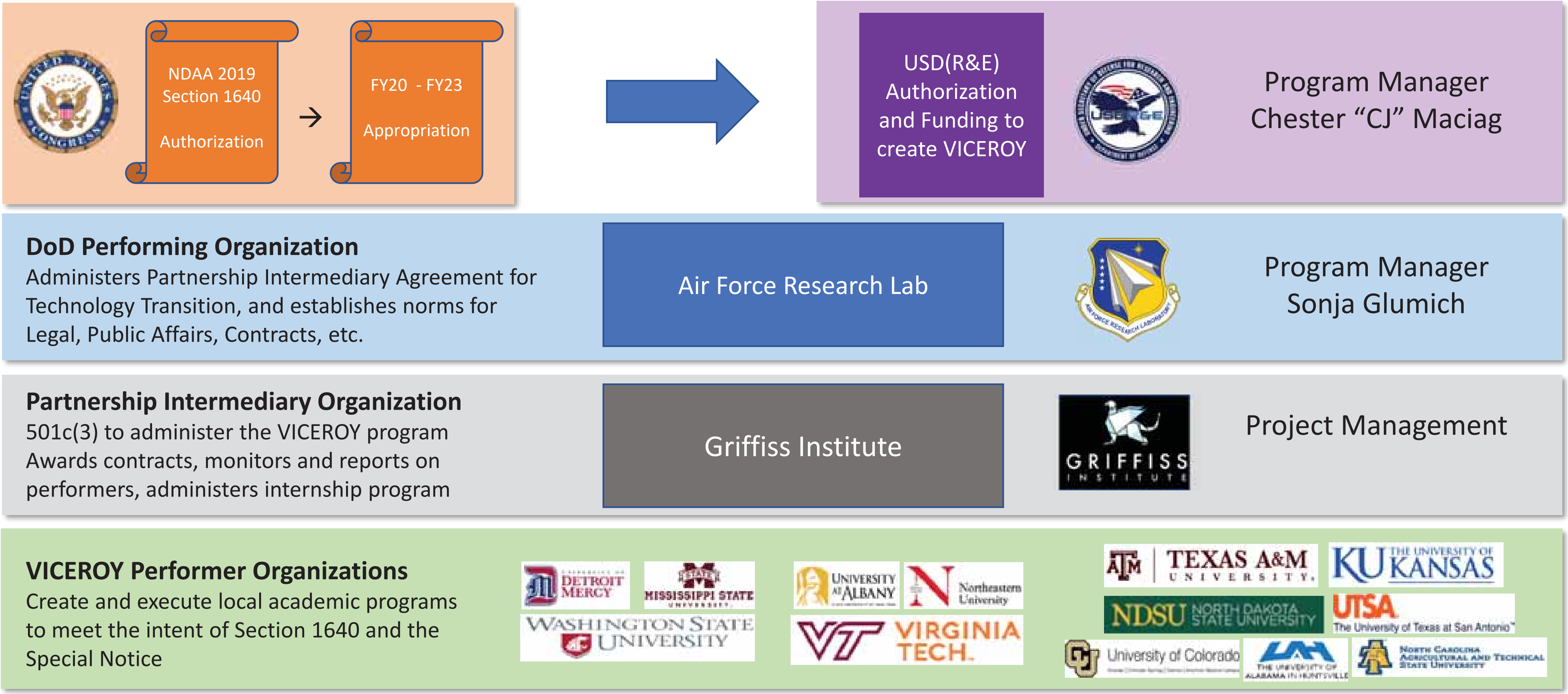
OSD Engaging Services/Components to Develop Long-Term Sustainable Execution Plan

# Section 1640 of the NDAA for FY2019

## SECTION 1640. PROGRAM TO ESTABLISH CYBER INSTITUTES AT INSTITUTIONS OF HIGHER LEARNING (2 of 2)

- ***SELECTED INSTITUTIONS OF HIGHER LEARNING**.*
  - *(1) IN GENERAL.—The Secretary of Defense shall select institutions of higher learning for purposes of the program established under subsection (a) from among institutions of higher learning that have a Reserve Officers' Training Corps program.*
  - *(2) CONSIDERATION OF SENIOR MILITARY COLLEGES.—In selecting institutions of higher learning under paragraph (1), the Secretary shall consider the senior military colleges with Reserve Officers' Training Corps programs.*
- ***ELEMENTS. Each institute established under the program authorized by subsection (a) shall include the following:***
  - *(1) Programs to provide future military and civilian leaders of the Armed Forces or the Department of Defense who possess **cyber operational expertise** from beginning through advanced skill levels. Such programs shall include **instruction and practical experiences** that lead to recognized certifications and degrees in the cyber field.*
  - *(2) Programs of targeted **strategic foreign language proficiency** training for such future leaders that— (A) are designed to significantly enhance critical cyber operational capabilities; and (B) are tailored to current and anticipated readiness requirements.*
  - *(3) Programs related to **mathematical foundations of cryptography** and courses in cryptographic theory and practice designed to complement and reinforce cyber education along with the strategic language programs critical to cyber operations.*
  - *(4) Programs related to **data science and courses in data science theory** and practice designed to complement and reinforce cyber education along with the strategic language programs critical to cyber operations.*
  - *(5) Programs designed to **develop early interest and cyber talent** through summer programs, dual enrollment opportunities for cyber, strategic language, data science, and cryptography related courses.*
  - *(6) Training and education programs to expand the **pool of qualified cyber instructors** necessary to support cyber education in regional school systems.*
- ***PARTNERSHIPS WITH DEPARTMENT OF DEFENSE AND THE ARMED FORCES.** Any institute established under the program authorized by subsection (a) may enter into a partnership with one or more components of the Armed Forces, active or reserve, or any agency of the Department of Defense to facilitate the development of critical cyber skills for students who may pursue a military career.*
- ***PARTNERSHIPS.** Any institute established under the program authorized by subsection (a) may enter into a partnership with one or more local educational agencies to facilitate the development of critical cyber skills.*
- ***SENIOR MILITARYCOLLEGES DEFINED.** The term ''senior military colleges'' has the meaning given such term in section 2111a(f) of title 10, United States Code.*

# VICEROY Organizational Relationships



NDAA 2019 Section 1640 Authorization → FY20 - FY23 Appropriation

USD(R&E) Authorization and Funding to create VICEROY

Program Manager Chester "CJ" Maciag

**DoD Performing Organization**
Administers Partnership Intermediary Agreement for Technology Transition, and establishes norms for Legal, Public Affairs, Contracts, etc.

Air Force Research Lab

Program Manager Sonja Glumich

**Partnership Intermediary Organization**
501c(3) to administer the VICEROY program
Awards contracts, monitors and reports on performers, administers internship program

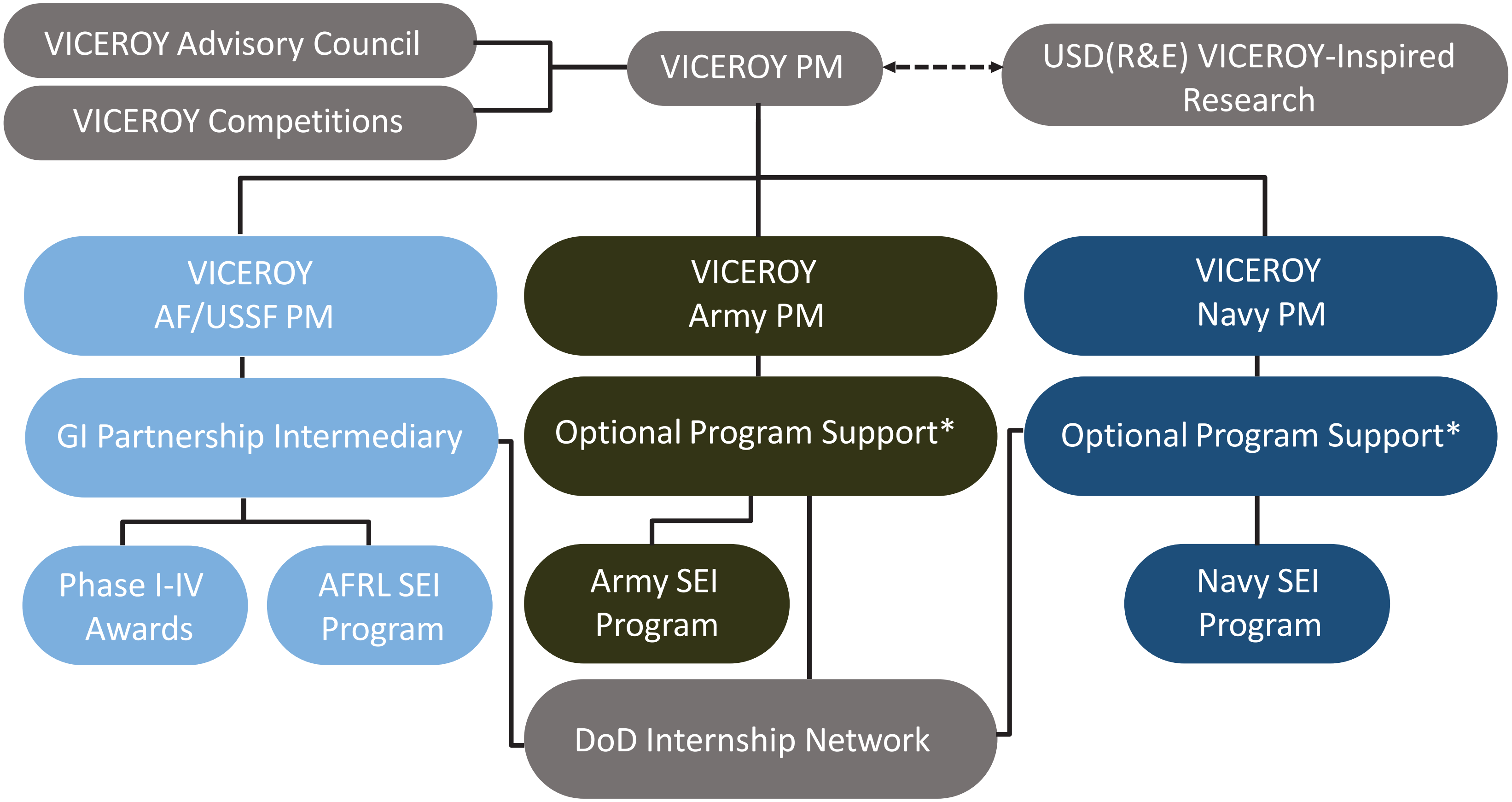
Griffiss Institute

Project Management

**VICEROY Performer Organizations**
Create and execute local academic programs to meet the intent of Section 1640 and the Special Notice

Detroit Mercy
Mississippi State University
Washington State University
University at Albany
Northeastern University
Virginia Tech
Texas A&M University
The University of Kansas
NDSU North Dakota State University
UTSA The University of Texas at San Antonio
University of Colorado
The University of Alabama in Huntsville
North Carolina Agricultural and Technical State University

# Program Partner Structure (MAVEN Expansion)



VICEROY Advisory Council

VICEROY Competitions

VICEROY PM

USD(R&E) VICEROY-Inspired Research

VICEROY AF/USSF PM

VICEROY Army PM

VICEROY Navy PM

GI Partnership Intermediary

Optional Program Support*

Optional Program Support*

Phase I-IV Awards

AFRL SEI Program

Army SEI Program

Navy SEI Program

DoD Internship Network

# VICEROY – Future Plans

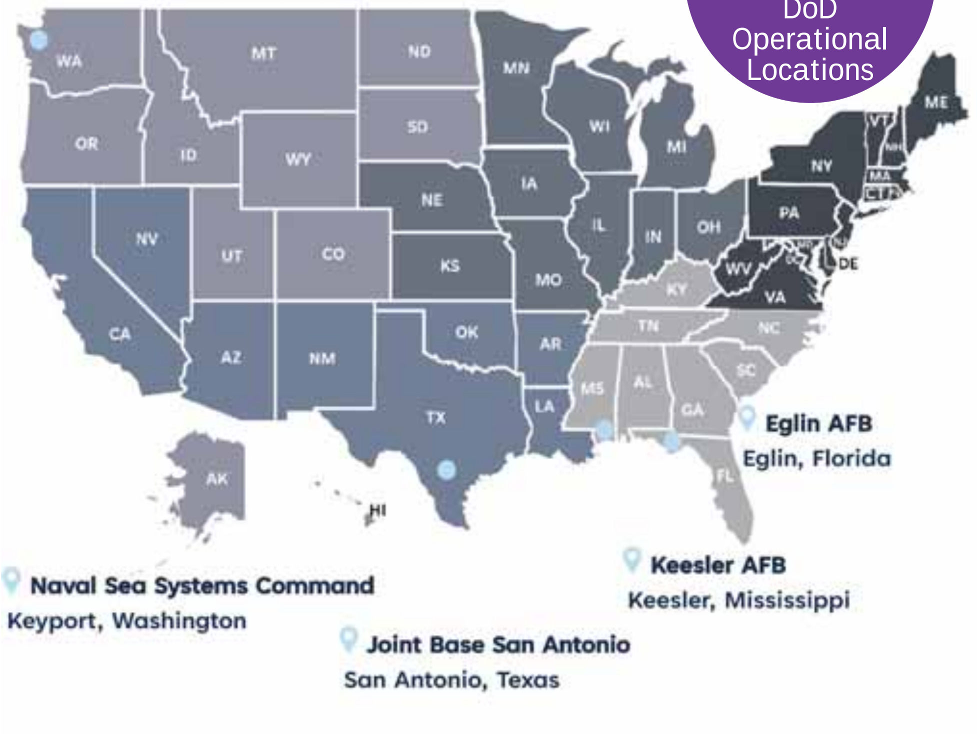
- Fall 2023 – Conduct national VICEROY mission-focused competition
- Fall 2023 – Partner with scholarship, retention, and excepted service programs
  - Engaging DCTC[1] Program through Virginia Tech and U of Arizona (already VICEROY consortium members)
- Spring 2024 – Expand number of internship host sites
  - Interest from NIWC-PAC, NRL, and STRATCOM, among others
- Summer 2024 - Expand MAVEN internship program to Army and Navy
  - Interest from NIWC-PAC, and ARL-Adelphi
- Ongoing – Identify VICEROY sustainment funding beyond FY24
  - Conducting discussions with Services and installations to identify cost-sharing strategy

1 – DCTC: Defense Civilian Training Corps

# Follow-up Summer Internship Host Site Locations

## (Post-MAVEN, or alternative to MAVEN)

**34**
Second Year Internships at DoD Operational Locations



Eglin AFB
Eglin, Florida

Keesler AFB
Keesler, Mississippi

Naval Sea Systems Command
Keyport, Washington

Joint Base San Antonio
San Antonio, Texas

**MOA**

Eglin, Florida

"The 96th Test Wing executes developmental test and evaluation enabling the warfighter to put weapons on target in all battlespace media while also providing support for all other Team Eglin missions as the installation host wing. Eglin deploys combat ready forces while delivering full spectrum support to the DoD's second largest test and training complex. Today, Eglin tests and evaluates non-nuclear munitions, electronic combat systems and navigation/guidance systems."

Click to learn more.

**MOA**

San Antonio, Texas

"The Air Force is the lead agency for Joint Base San Antonio, comprising three primary locations at JBSA-Fort Sam Houston, JBSA-Lackland and JBSA-Randolph plus 8 other operating locations and more than 200 mission partners. JBSA services more DOD students than any other installation, more active runways than any other installation, houses the DOD's largest hospital and only level one trauma center, supports more than 250,000 personnel."

Click to learn more.

**MOA**

Keesler, Mississippi

"Keesler trains more than 28,000 students annually with an average daily student load of more than 2,700. The 81st TRW is a lead Joint Training Installation, instructing not only Air Force, but Army, Navy, Marine Corps, Coast Guard and civilian federal agency personnel. Keesler's mission is enduring.
We provide a wide array of capabilities in over 160 career field specialty training courses from 8 operating locations in the continental United States. Our mission is not only to technically train warfighters, but to develop and inspire them."

Click to learn more.

**EPA**

Keyport, Washington

"Keyport provides technical leadership, engineering expertise, and unique facility complexes that serve to ensure sustainment of undersea warfare (USW) superiority for the United States. As one of two divisions of the Naval Undersea Warfare Center, Keyport's mission is focused on developing and applying advanced technical capabilities to test, evaluate, field, and maintain undersea warfare systems and related defense assets. These advanced technical capabilities directly support the full spectrum of Navy undersea programs."

Click to learn more.

# VICEROY Support to Interns – Breaking Down Barriers to Summer Employment

## Housing

- Housing for First Year Interns is provided nearby Griffiss Institute
- Housing for Follow-up DoD Host Site Interns is provided nearby each DoD host site

## Pay

- Graduate Assistants are paid $29/hr
- Follow-up DoD Host Site Interns are paid $24/hr
- First Year Interns are paid $22/hr

## Travel

- Interns that live greater than 50 miles from their placement site will receive travel reimbursement up to $1500 for airfare or mileage
- Daily transportation is provided to/from Griffiss Institute for interns in Rome, NY

## Quality of Life

- All travel and housing is facilitated by Griffiss Institute
- Interns can meet one another digitally before start dates to build rapport
- We ensure interns have a quality environment where they can thrive

# VICEROY Virtual Institutes

- Faculty-led, multi-institution, multi-year research endeavors that specifically target cyber and electromagnetic spectrum operations (EMSO) challenges of interest to the DoD

- Develop new or augment existing cyber coursework leading to specializations, degrees, or industry certifications

- Provide scholarships and stipends for student participation

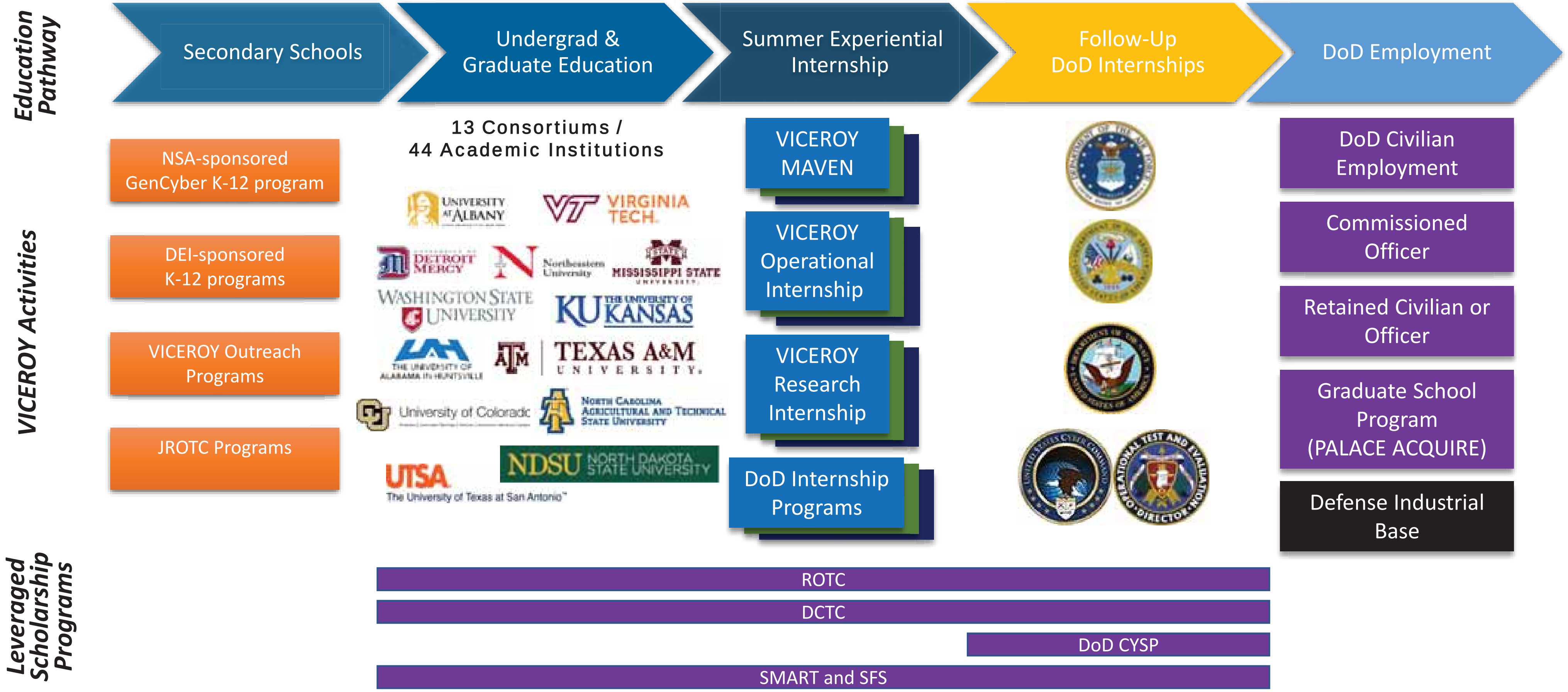
- Sponsor cyber research projects of interest to the DoD for VICEROY students

- Hold cyber seminars, workshops, and competitions

- Report progress and share lessons learned at the annual VICEROY Symposium

# Mapping the DCWS to VICEROY Activities

**Leveraged Scholarship Programs at Bottom**



*Education Pathway*

Secondary Schools → Undergrad & Graduate Education → Summer Experiential Internship → Follow-Up DoD Internships → DoD Employment

*VICEROY Activities*

NSA-sponsored GenCyber K-12 program

DEI-sponsored K-12 programs

VICEROY Outreach Programs

JROTC Programs

13 Consortiums / 44 Academic Institutions

VICEROY MAVEN

VICEROY Operational Internship

VICEROY Research Internship

DoD Internship Programs

DoD Civilian Employment

Commissioned Officer

Retained Civilian or Officer

Graduate School Program (PALACE ACQUIRE)

Defense Industrial Base

*Leveraged Scholarship Programs*

ROTC

DCTC

DoD CYSP

SMART and SFS

University at Albany
Virginia Tech
Detroit Mercy
Northeastern University
Mississippi State University
Washington State University
The University of Kansas
The University of Alabama in Huntsville
Texas A&M University
University of Colorado
North Carolina Agricultural and Technical State University
UTSA The University of Texas at San Antonio
NDSU North Dakota State University
Operational Test and Evaluation Director

# TAB 2 – MAVEN
# Student Background

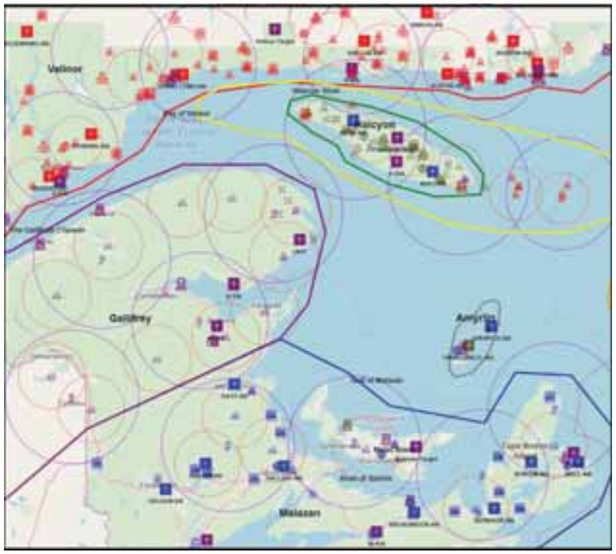
# MAVEN Internship Capstone

- **Mission Relevance:** Based closely on AF and USSF Unit Cyber Warfare Training culminating operational capstone challenge (CONCORD DAWN)

- **Concord Dawn Capstone**: Transmit the coordinates of a High Value Target to a UAV to enable target strike

- **Future VICEROY-Wide Activities:**
  - National VICEROY 44-school competition in Fall 2023
  - Custom capstone tailored to the new MAVEN curriculum
  - Alternate capstones focused on ground, surface, undersea, and space domains of Service partners

Partnership with AFRL/RI's *Blue Edge* competition development team



# What our VICEROY Interns are Saying…

"As a graduate of the 2022 VICEROY program, I was honored to have experienced the internship in its inaugural year. The mentorship and hands-on experience I received has proven invaluable as I continue my studies in the Computer Science field."

**Jacob Lebovich**
*1st Year – VICEROY, Intern - 2022*
*2nd Year – VICEROY, GA - 2023*

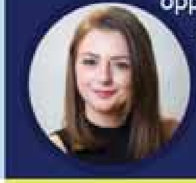
"Previously, my interests lay within artificial intelligence and data science, but VICEROY cultivated my passion for cybersecurity. I got to craft technical reports, learn new programmatic concepts, and perform research under a mentor. This program gave me lessons in leadership, an expansive network, and various core experiences."

**Aailya Jakir**
*1st Year – VICEROY - 2022*
*2nd Year – ACE - 2023*

"This internship, facilitated by VICEROY, has allowed me to not only demonstrate my knowledge and skills but also make a significant impact. Additionally, I have been offered an amazing chance to be a part of a select few to instruct and shape future cyber warriors for the Air Force, which I'm truly excited about."

**Justin Pettiss**
*1st Year – VICEROY - 2023*
*Keesler Air Force Base*
336 TRS/TRR

"I have thoroughly enjoyed the VICEROY summer internship. Wavelength is at a pivotal moment of innovation for creating Air Force software. It has been an awesome experience and I'm grateful to have been a part of this program. I hope many others get to pursue this opportunity as it has been a wonderful exposure. "



**Morgan Hardy**
*1st Year – VICEROY - 2023*
*Joint Base San Antonio*
*WAVELENGTH*

"The first year of VICEROY I saw as a transition from academia to the workforce, and this summer is the application of those skills we learned last summer in a real work environment. Overall, I feel this summer has adequately prepared me for future employment opportunities and I highly recommend this experience to those with interest in radar and the DoD."

**Morgan Jones**
*1st Year – VICEROY - 2022*
*2nd Year – VICEROY - 2023*
*Eglin Air Force Base- 350TH*

"My experience with Wavelength as a software development intern has been mind-opening, exciting, while being challenging. I work in a group of three, so we were able to learn and discover a lot from each other. Teamwork is an aspect that I enjoy doing during this internship, as we get along with each other well."

**Timothy Truong**
*1st Year – VICEROY - 2023*
*Joint Base San Antonio*
*WAVELENGTH*

"My experience this Summer as a VICEROY Intern for The Naval Undersea Warfare Center Division Keyport, has been incredible. I have fostered many connections in my short time at Keyport and I am eager to continue supplying the government with my growing cybersecurity knowledge."

**Benjamin Price**
*1st Year – VICEROY - 2023*
*Naval Undersea Warfare Center Division Keyport*

"During my VICEROY summer internship, I have had the ability to network and learn with my peers. Ultimately, I have garnered a valuable experience and have taken an important first step toward a future in the DoD."

**Ryan Silvus**
*1st Year – VICEROY - 2023*
*Joint Base San Antonio*
*WAVELENGTH*

My name is Turner Woodward, and I'm a student of the University of Detroit Mercy pursuing a degree in Computer Engineering with a minor in Computer Science. I am an ambitious life-long learner, and I spend most of my free time programming, gardening, or making CAD models to 3D print. The MAVEN program has challenged me to constantly improve my skills and build me into a CYBER professional, and I truly believe I would not be who I am today if not for the support from my fellow MAVENs. I feel this internship has been a transformative experience and my first steps to a long career in the DoD, and I am very thankful for the opportunity to visit the Pentagon.

**1st**

**Turner Woodward**

*1st Year VICEROY, Intern - 2023*

***University of Detroit Mercy***

*Computer Engineering*

My name is Guinevere Fish. I am studying computer science and will be a junior at Washington State University in the fall. I am involved in the cybersecurity club at WSU, the CyberCougs. The opportunity to participate in this internship has not only given me skills that I can bring back to utilize in the club at school but has also given me a look into what working in cybersecurity in the government might look like.

**2nd**

**Guinevere Fish**

*1st Year VICEROY, Intern - 2023*

***Washington State University***

*Computer Science*

I arrived at Viceroy midway through a career change. I earned a BA in English at Kalamazoo College, and an MA in Japanese at University of Wisconsin before moving to the University of Washington, where I focused on early modern Japanese literature and intellectual history. While working for a Japanese IT firm as a lead bilingual test engineer, I decided to shore up my foundations and began coursework for an AS in physics at Oakland Community College. OCC entered the VICEROY consortium just as I completed the degree, and, with their support, enabled me to think beyond the automotive industry. In the fall, I will begin the MS Vehicle Cyber Engineering program at the University of Detroit, Mercy.

**3rd**

**Benjamin Rosenberg**

*1st Year VICEROY, Intern - 2023*

***Oakland Community College***

*Computer Information Sciences*

VICEROY AFRL

Hi, my name is Yasmin Chambers. I am a rising senior at Mississippi State University, majoring in computer engineering with a minor in mathematics. I am in the U.S. Army Reserves, and recently contracted into the AROTC program at MSU. I enjoy fitness, nature, reading, and hackathons! The VICEROY program has given me the necessary tools to create my own solutions and further elevate the technologies that are present. I have gained diversified insight and seen the wide scope of cybersecurity and electromagnetic spectrum systems. I plan to use this knowledge to strengthen the military's cyber intelligence and use new technology to advance our armed forces' defense. I look forward to networking and experiencing the Pentagon.

**4th**

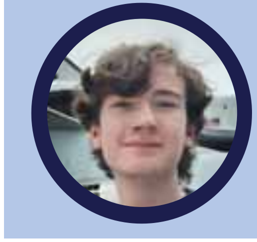
**Yasmin Chambers**

*1st Year VICEROY, Intern - 2023*

***Mississippi State University***

*Computer Engineering*

Hello, I'm Alex, a rising junior at Washington State University. At Washington State, I study Computer Science and participate in cybersecurity competitions with my team, the CyberCougs. Being able to come to the east coast, and work at the Air Force Research Lab in New York has been an amazing opportunity. Working with other interns to perform research has been fulfilling, and learning more about cybersecurity through the MAVEN program has been educational as well. I'm honored and excited to come to the Pentagon to learn more. Thank you!



**5th**

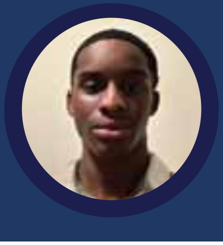
**Alexander Hagood**

*1st Year VICEROY, Intern - 2023*

***Washington State University***

*Computer Science*

My name is Elijah Gartrell, a rising Junior at Old Dominion University majoring in Cybersecurity with a double minor in French & International Relations. Currently residing in Northern Virginia, I enjoy family time, sports, and music. This summer at VICEROY, I worked on the Virtual Reality Information Flow Analysis project with mentor Sonja Glumich. This project was amazing and truly a great opportunity.



**6th**

**Elijah Gartrell**

*1st Year VICEROY, Intern - 2023*

***Old Dominion University***

*Cyber Security*

SECURE OUR WORLD

# INDIANA UNIVERSITY OF PENNSYLVANIA: NATIONAL CYBERSECURITY AWARENESS MONTH 2023

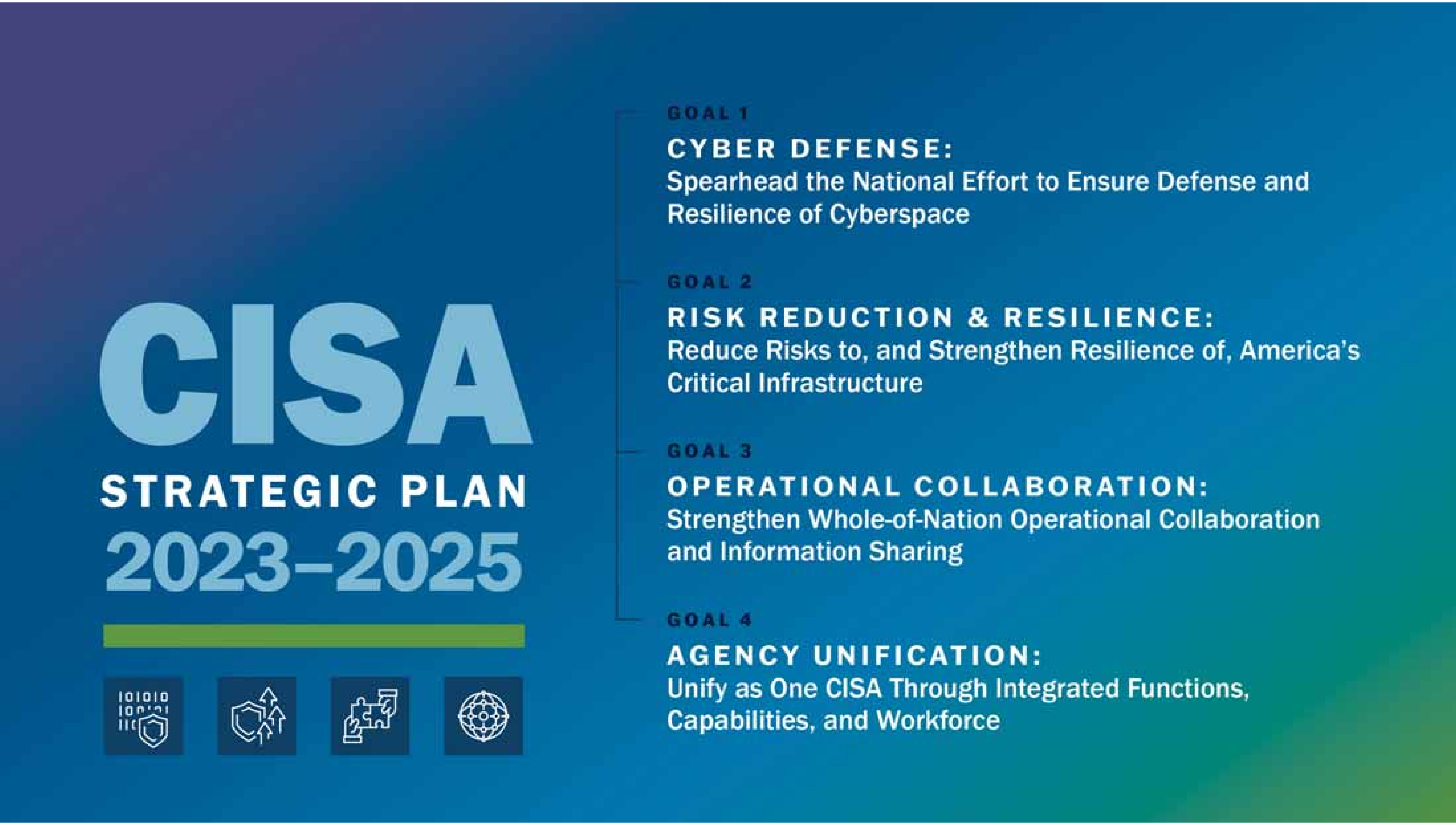
**Derek Mueller**
**Cybersecurity Advisor – State Coordinator Pennsylvania**
Region III (MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

# Cybersecurity Awareness Month

- Launched in 2004
- Co-managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA)
- Collaborative effort between government and industry to raise cybersecurity awareness
- Ensures that everyone has the resources they need to be safe and secure online.

SECURE OUR WORLD

# October is Cybersecurity Awareness Month



# CISA

## STRATEGIC PLAN 2023–2025

GOAL 1

**CYBER DEFENSE:**
Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

**RISK REDUCTION & RESILIENCE:**
Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure

GOAL 3

**OPERATIONAL COLLABORATION:**
Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

**AGENCY UNIFICATION:**
Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

# What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Wherever there is technology, there needs to be cybersecurity.

# Why is it Important?

- Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.
- For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

# Feelings Toward Cybersecurity

- **78%** of people consider staying secure online a priority
- **34%** noted they often feel overwhelmed by information and, as a result, minimize their online actions
- **46%** felt frustrated while staying secure online
- **39%** of users trying to keep safe felt information on how to stay secure online is confusing

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

# Our Online Behaviors

- **Only 33% of individuals create unique passwords for all accounts**
  - Only 18% of individuals have downloaded a password manager
- **43% of respondents have never heard of multifactor authentication (MFA)**
  - Out of the 57% of the participants who had heard about it:
    - 79% applied it at least once and 94% of them reporting that they were still using MFA
- **92% of respondents took action after a security training**
  - 58% say they are better at recognizing phishing
  - 45% started using strong and unique passwords
  - 40% started using MFA
  - 40% started regularly installing software updates

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

# Who – Cyber Threat Actors

Nation States

Hacktivists

Cyber Criminals

# How – Avenues for attack

- Social Engineering
- Vulnerability Exploitation
- Misconfigurations & Poor Security Practices
- Physical Access and Hands On Exploitation
- Phishing
- Insider Threat

SECURE OUR WORLD

# Action Steps

# 4 Easy Ways to Stay Safe Online

Use Strong Passwords and a Password Manager

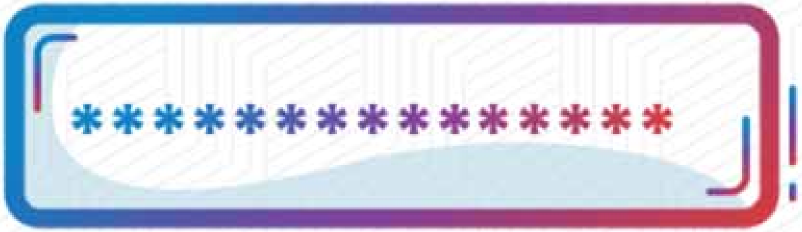
Turn on Multifactor Authentication

Recognize and Report Phishing Attacks

Update Your Software

# Use Strong Passwords

## CREATE STRONG PASSWORDS:



- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Complex**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces

# Use a Password Manager

## WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

# Turn on Multifactor Authentication

## WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  Fingerprint
  Facial recognition

# Turn on Multifactor Authentication

## WHERE SHOULD YOU USE MFA?

- **Email**
- **Accounts with financial information**
  Ex: Online store
- **Accounts with personal information**
  Ex: Social media

# Recognize and Report Phishing

## PHISHING RED FLAGS:

- **A tone that’s urgent or makes you scared**

*"Click this link immediately or your account will be closed"*

- **Bad spellings, bad grammar**

- **Requests to send personal info**

- **Sender email address doesn’t match the company it’s coming from**

Ex: Amazon.com vs. Amaz0n.com

- **An email you weren't expecting**

# Recognize and Report Phishing

## WHAT TO DO

### Do NOT

- Don't click any links
- Don't click any attachments
- Don't send personal info

### Do

- Verify
- Contact that person directly if it's someone you know
- Report it to your IT department or email/phone provider
- DELETE IT

# Update Your Software

## WHY?

- Updates ensure your devices and apps are protected from the latest threats

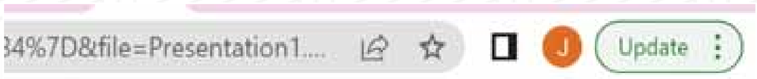
- Don't click "remind me later", it could leave you vulnerable to cyber threats

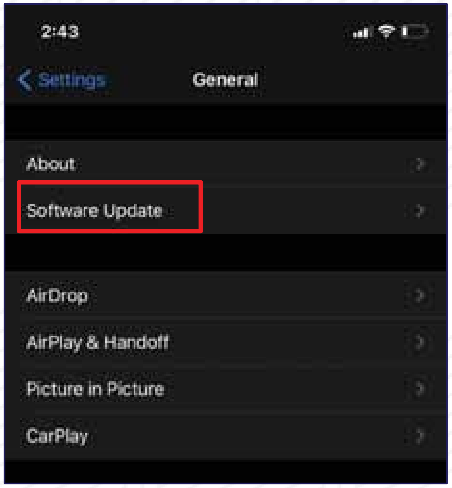
- Automatic updates are the easiest way to stay secure

# Update Your Software

## WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts

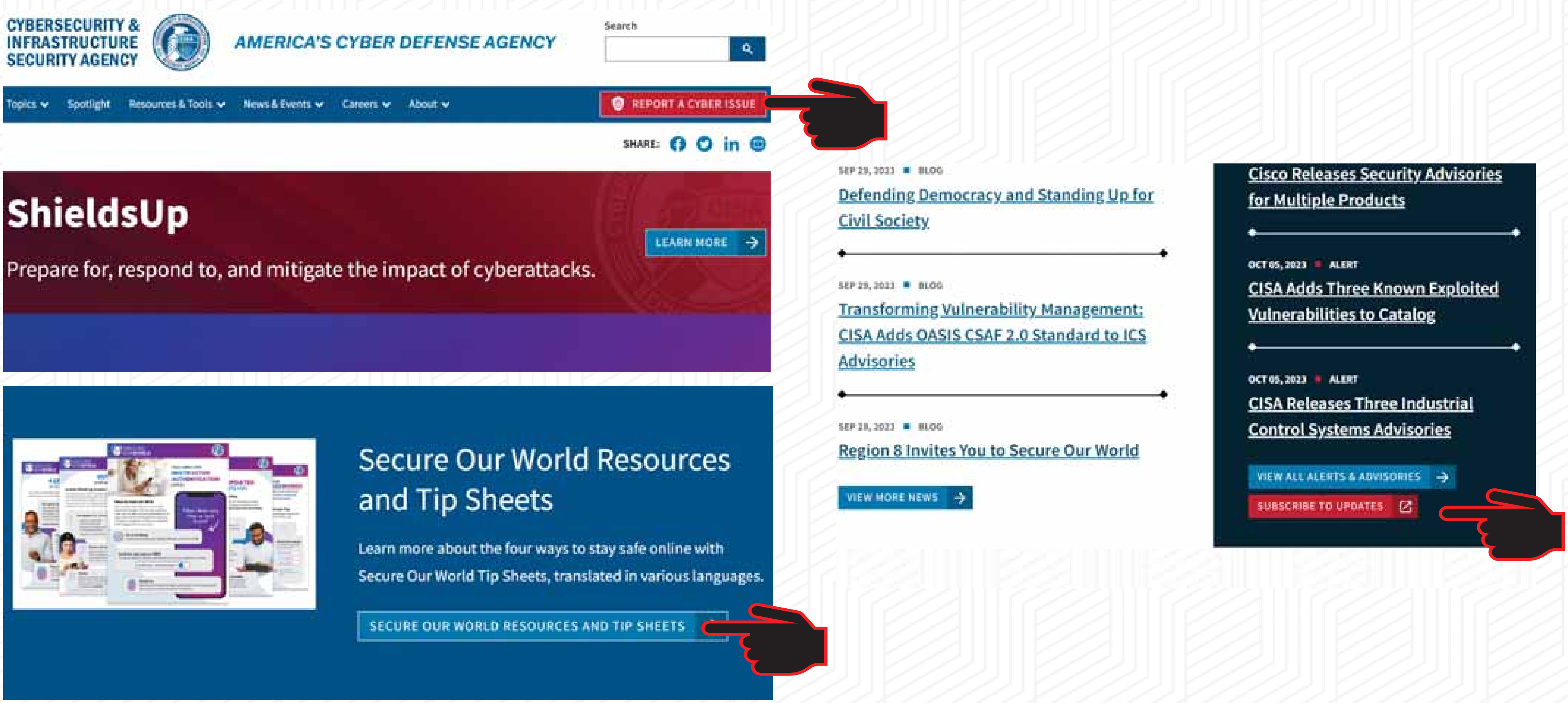




# Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online** and **learn about risks** like phishing and business email compromise.

# CISA Website – cisa.gov



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ⌄ Spotlight Resources & Tools ⌄ News & Events ⌄ Careers ⌄ About ⌄

REPORT A CYBER ISSUE

SHARE:

## ShieldsUp

Prepare for, respond to, and mitigate the impact of cyberattacks.

LEARN MORE →

## Secure Our World Resources and Tip Sheets

Learn more about the four ways to stay safe online with Secure Our World Tip Sheets, translated in various languages.

SECURE OUR WORLD RESOURCES AND TIP SHEETS

SEP 29, 2023 ■ BLOG

Defending Democracy and Standing Up for Civil Society

SEP 29, 2023 ■ BLOG

Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories

SEP 28, 2023 ■ BLOG

Region 8 Invites You to Secure Our World

VIEW MORE NEWS →

Cisco Releases Security Advisories for Multiple Products

OCT 05, 2023 ■ ALERT

CISA Adds Three Known Exploited Vulnerabilities to Catalog

OCT 05, 2023 ■ ALERT

CISA Releases Three Industrial Control Systems Advisories

VIEW ALL ALERTS & ADVISORIES →

SUBSCRIBE TO UPDATES

# Ways to Get Involved

### AT WORK

- Publicize resources and activities
  - Intranet
  - Website
  - Emails to employees/customers
- Promotions
  - Discounts
  - Giveaways
- Hold a contest
  - Phishing simulation
  - Poster contest

### AT HOME

- Share helpful tips and resources
  - Kids
  - Parents
  - Friends
- Hold a family “tech talk”
  - Discuss how each family member can protect their devices, accounts, and personal information.
- Create a culture of security in your family

# Ways to Get Involved Cont.

## IN YOUR COMMUNITY

- Volunteer to teach others in your community
- Reach out to
  - Your kid's school
  - A library/community center
  - Senior center
  - Place of worship

## ONLINE

- Join on the conversation on social media using
  - **#CybersecurityAwarenessMonth**
  - **#SecureOurWorld**

# What’s It Worth - Avg. Dark Web Price (USD)

Credit card details, account balance up to 5,000 ($120)

Credit card details, account balance up to 1,000 ($80)

Stolen online banking logins, minimum $2,000 on account ($65)

Cashapp verified account ($800)

Stolen PayPal account details, minimum $100 balances ($15)

50 Hacked PayPal account logins ($150)

Crypto.com verified account ($250)

Binance verified account ($260)

USA verified LocalBitcoins account ($120)

Utility bill templates ($25)

New York driver’s license ($70)

US driver’s license (avg.) ($150)

10 million USA email addresses ($120)

Netflix account, 1-year subscription ($25)

Uber hacked acct. ($15)

Uber driver hacked acct. ($35)

Hacked Facebook account ($45)

Hacked Instagram account ($40)

Hacked Twitter account ($25)

Hacked Gmail account ($65)

# Additional Resources

### CISA

- Report a Cyber Issue
- Secure by Design
- Cross-Sector Cybersecurity Performance Goals
- Cyber Resource Hub
- Cybersecurity Training & Exercises
- CISA YouTube Channel

### NCA

- Resources and Guides
- Videos and On-Demand Webinars

# Other Federal Reporting Resources

**FBI 24x7 CyWatch:** (855) 292-3937 or CyWatch@fbi.gov

**FBI Cyber Complaint Center:** www.ic3.gov

For individuals who are victims of an online/digital crime

**Federal Trade Commission –** reportfraud.ftc.gov

For individuals who are victims of bad business practices or taken advantage of by online companies

**Identity Theft Resources** – IdentityTheft.gov

For individuals who believe they may be victims of Identity Theft

For more information, visit **cisa.gov** or contact **central@cisa.dhs.gov**

**Derek Mueller**
**Cybersecurity Advisor – State Coordinator Pennsylvania**
Region III (MD, PA, DE, DC, VA, WV)
Derek.mueller@cisa.dhs.gov
Cybersecurity and Infrastructure Security Agency

# GROWING THE NEXT GENERATION OF CYBER TALENT

Star Hardison,

Governance Program Manager

Workforce Innovation Directorate, DoD CIO

November 2023

# AGENDA

- Mission Statement
- DoD CWF Strategy Implementation Plan
- Cultivating Tomorrow’s Talent Pool
- What is the DoD Cyber Scholarship Program?
- DoD 8140 Qualification Model Example
- Questions

# MISSION STATEMENT

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

**The Department of Defense** is one of the Nation's largest employers with approximately:

- 1.3 million active-duty service members
- 750,000 National Guard and Reserve service members
- 750,000 civilian personnel
- 600,000 contractors

**Growing Our Talent:**

To remain the strongest fighting force in the world, we must **recruit** and **retain** the best of America.

That means **we must** continue:

- Building pathways of opportunity for all qualified Americans.
- Deepening the Department's partnerships with America's best universities.
- Continuing to invest in training and education and create programs that focus on science, technology, engineering, and math.
- Providing exceptional opportunities for service and professional development for our total force.

# DoD CYBER WORKFORCE STRATEGY IMPLEMENTATION PLAN

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

## Cyber Workforce Strategy

- Aims to provide the tools, resources, policies and programs that enable the Department's cyber workforce stakeholders to **identify, recruit, develop** and **retain** a more agile and effective cyber workforce.

## Implementation Plan

- Sets the foundation for how the Department will execute the 22 objective and 38 initiatives aligned with the 4 overarching goals in the CWF Strategy.

Identification

Recruitment

Development

Retention

GOAL 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.

GOAL 2: Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements.

GOAL 3: Facilitate a cultural shift to optimize Department-wide personnel management activities.

GOAL 4: Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

# CULTIVATING TOMORROW’S TALENT POOL

DOD CYBER WORKFORCE STRATEGY

2023-2027

**CWF Strategy Goal 4:**

- Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

**Objective 4.3:**

- Enhance collaboration with academia to cultivate a talent pipeline and support important areas of research.

DOD CYBER WORKFORCE STRATEGY IMPLEMENTATION PLAN

2023-2027

**Initiative 4.3.1:**

- Establish a centralized program office to manage cyber-focused student and employee developmental programs across the Department.

**Initiative 4.3.2:**

- Ensure NCAE-C curriculum aligns with Department-wide cyber standard.

**Initiative 4.3.3:**

- Increase return on investment of scholarship programs and effectively track participation to customize recruitment and outreach efforts.

# WHAT IS THE DoD CYBER SCHOLARSHIP PROGRAM?

01100011 01111001 01100010 01100101 01110010 00100000 01110111

## The DoD Cyber Scholarship Program (DoD CySP)

(Formerly the Information Assurance Scholarship Program) is designed to encourage the recruitment of the nation's top cyber talent and the retention of DoD personnel who have skills necessary to meet DoD's cyber requirements and help secure our nation against the threats of information systems and networks.

### Grants awarded for scholarships and capacity building to NCAE-Cs:

**Scholarships**

*Recruitment*: Targets students who are not current DoD or Federal employees and who are enrolled at designated CAEs; may be undergraduate or graduate students

*Retention:* Targets Military and Civilian DoD personnel for Associates or Graduate (Certificates, Masters, and PhD programs)

### NCAE-Cs

National Centers of Academic Excellence in Cybersecurity (NCAE-C)

National Centers of Academic Excellence in Cyber Defense (CAE-CD)

National Centers of Academic Excellence in Cyber Defense Research (CAE-R)

National Centers of Academic Excellence in Cyber Operations (CAE-CO**)**

# DoD 8140 QUALIFICATION MODEL EXAMPLE

| (621) Software Developer | | | | |
|---|---|---|---|---|
| | | **Basic** | **Intermediate** | **Advanced** |
| **Foundational Qualification Options** | **Education** | Associate degree or higher from an accredited college or university | Bachelor degree or higher from an accredited college or university | Bachelor degree or higher from an accredited college or university |
| | | ***OR*** | ***OR*** | ***OR*** |
| | **Training** | Offerings listed in DoD 8140 Training Repository | Offerings listed in DoD 8140 Training Repository | Offerings listed in DoD 8140 Training Repository |
| | | ***OR*** | ***OR*** | ***OR*** |
| | **Personnel Certification** | GSEC | CSSLP | CISSP-ISSAP |
| **Foundational Qualification Alternative** | **Experience** | Conditional Alternative | Conditional Alternative | Conditional Alternative |
| **Residential Qualification** | **On-the-Job Qualification** | Always Required | Always Required | Always Required |
| | **Environment-Specific Requirements** | Component Discretion | Component Discretion | Component Discretion |
| **Annual Maintenance** | **Continuous Professional Development** | Minimum of 20 hours annually or what is required to maintain certification; whichever is greater. | Minimum of 20 hours annually or what is required to maintain certification; whichever is greater. | Minimum of 20 hours annually or what is required to maintain certification; whichever is greater. |

# Survey on Cyber Education Requirements

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

**Sponsor:** Institute for Defense Analyses (IDA) (on behalf of the DoD)

**Purpose:** To gather perspectives on how to best educate the DoD's cyber workforce to protect the Nation from future cyber threats (findings will be included in a report requested by Congress).

**Survey Question Focus:**

- Student capacity in cyber programs of study
- Educator staffing levels
- Cyber education preferences and requirements
- Perceptions of future cyber threats
- The need for a National Cyber Academy

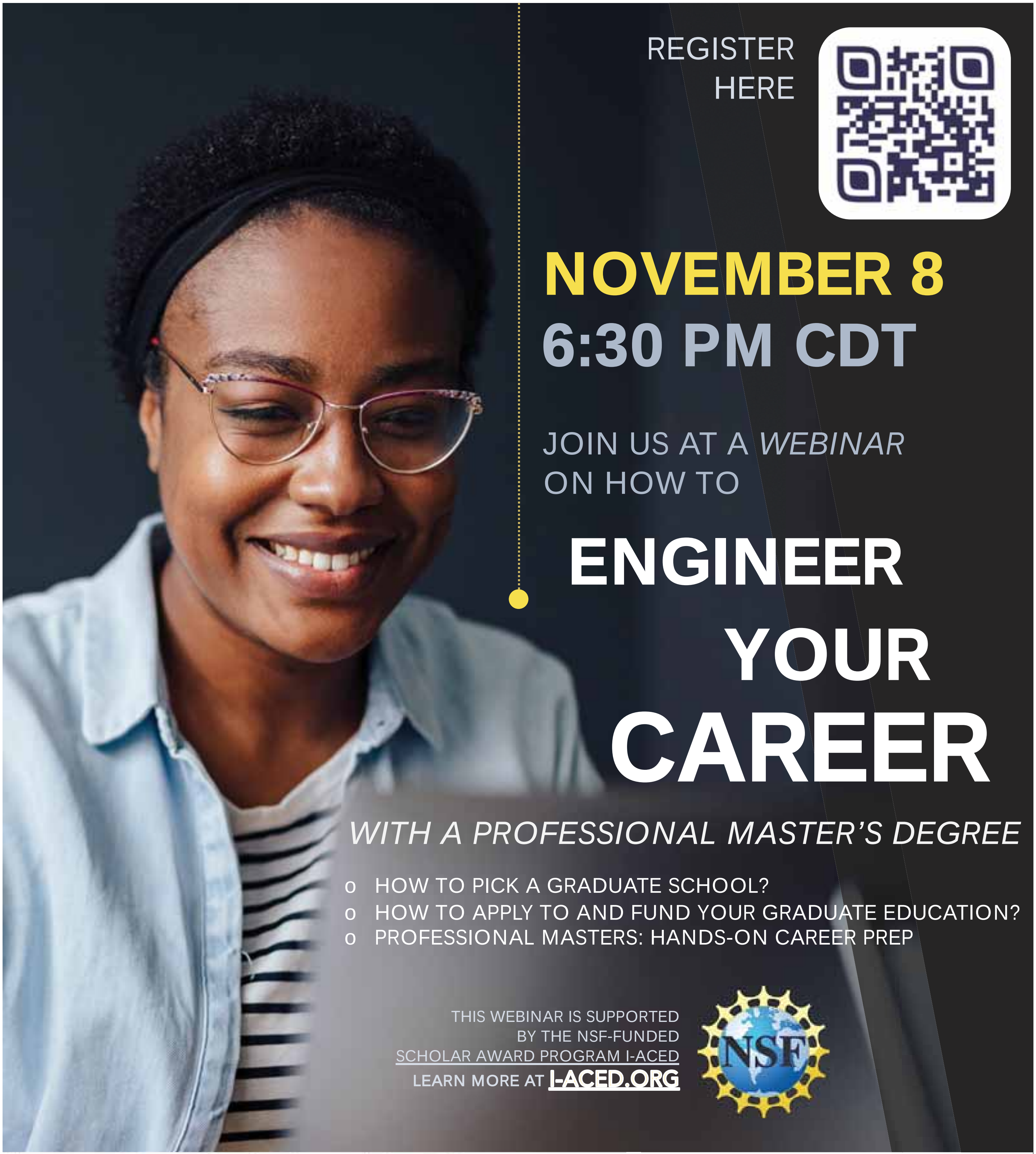
**SHARE YOUR THOUGHTS ON CYBER EDUCATION BY TAKING A BRIEF SURVEY**

(visit the URL or Scan the QR Code below )

https://idaorg.gov1.qualtrics.com/jfe/form/SV_251iRbIdGNIdmUC

# QUESTIONS

SCAN TO VIEW THE CYBER WORKFORCE STRATEGY



REGISTER<br>HERE

## NOVEMBER 8
## 6:30 PM CDT

JOIN US AT A *WEBINAR* ON HOW TO

# ENGINEER YOUR CAREER

*WITH A PROFESSIONAL MASTER'S DEGREE*

- HOW TO PICK A GRADUATE SCHOOL?
- HOW TO APPLY TO AND FUND YOUR GRADUATE EDUCATION?
- PROFESSIONAL MASTERS: HANDS-ON CAREER PREP

THIS WEBINAR IS SUPPORTED
BY THE NSF-FUNDED
SCHOLAR AWARD PROGRAM I-ACED
LEARN MORE AT **I-ACED.ORG**

NSF

## I-ACED

IMPROVING ACCESS TO CAREER &
EDUCATIONAL DEVELOPMENT

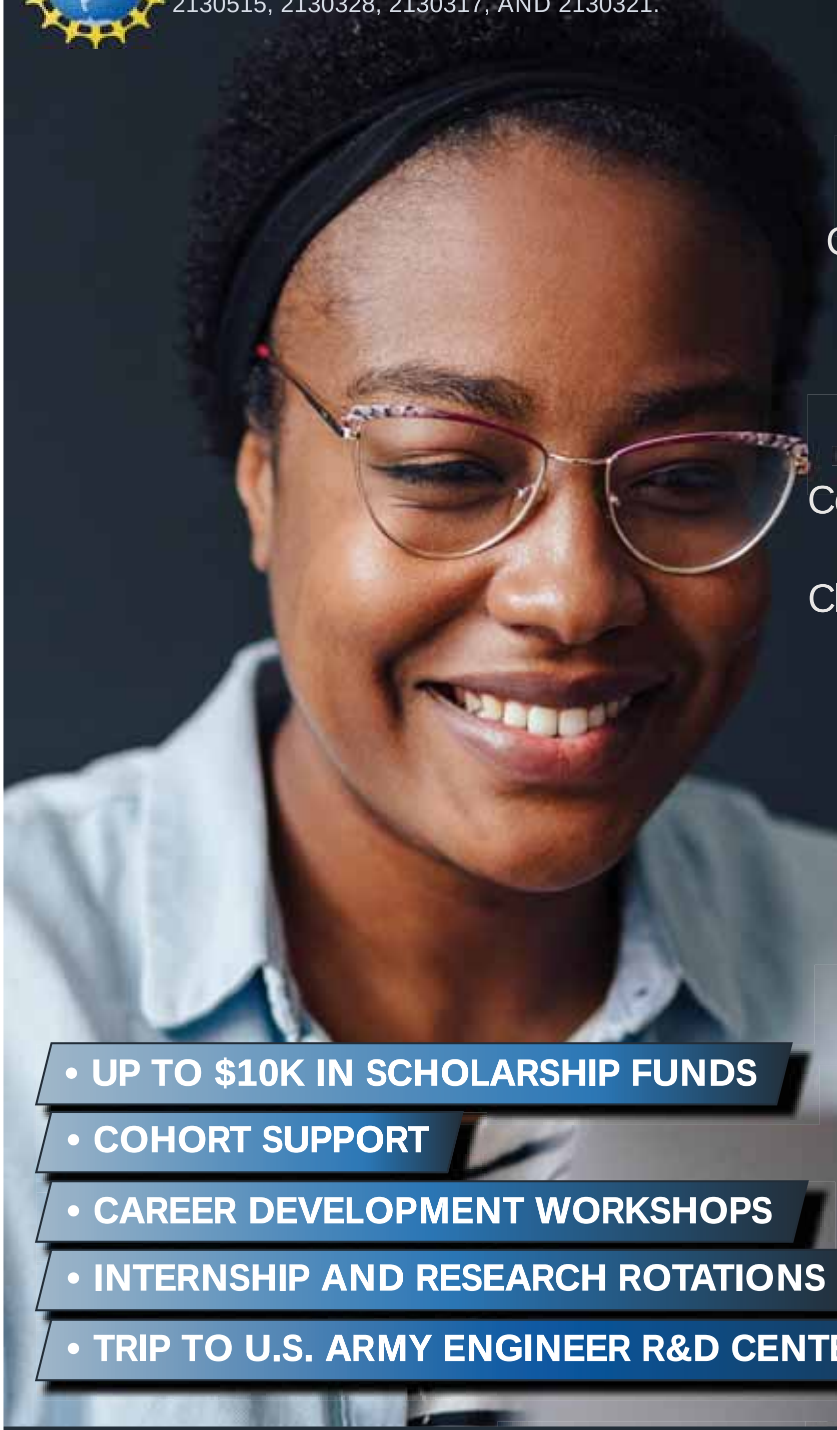
- Up To $10k In Scholarship Funds
- Cohort Support And Career Development Workshops
- Tour Around U.S. Army Engineer R&D Center
- Internship And Research Rotations

JSU JACKSON STATE UNIVERSITY · PRAIRIE VIEW A&M UNIVERSITY · RICE · TSU TEXAS SOUTHERN UNIVERSITY · ERDC ENGINEER RESEARCH & DEVELOPMENT CENTER

# I-ACED

## IMPROVING ACCESS TO CAREER & EDUCATIONAL DEVELOPMENT

THIS PROGRAM IS SUPPORTED BY THE NATIONAL SCIENCE FOUNDATION AWARDS 2130515, 2130328, 2130317, AND 2130321.



*I-ACED IS A NEEDS-BASED SCHOLAR AWARD PROGRAM OFFERED AT*

### JACKSON STATE UNIVERSITY

Computer Science | Computational & Data Enabled Science & Engineering | Coastal Engineering

### PRAIRIE VIEW A&M UNIVERSITY

Computer Science | Mechanical Engineering | Electrical & Computer Engineering | Chemical Engineering | Civil & Environmental Engineering

### RICE UNIVERSITY

Data Science | Computational & Applied Mathematics | Industrial Engineering | Bioengineering | Chemical Engineering

### TEXAS SOUTHERN UNIVERSITY

Computer Science | Mathematics | Environmental Toxicology | Transportation Planning & Management

- UP TO $10K IN SCHOLARSHIP FUNDS
- COHORT SUPPORT
- CAREER DEVELOPMENT WORKSHOPS
- INTERNSHIP AND RESEARCH ROTATIONS
- TRIP TO U.S. ARMY ENGINEER R&D CENTER (ERDC)

**LEARN MORE AT I-ACED.ORG**

JSU JACKSON STATE UNIVERSITY | PRAIRIE VIEW A&M UNIVERSITY | RICE | TSU TEXAS SOUTHERN UNIVERSITY | ERDC ENGINEER RESEARCH & DEVELOPMENT CENTER

*High-Performance Computing*

# INTERNSHIP

*Program (HIP)*

**You can harness high performance computing resources to solve our most critical Department of Defense mission challenges.**

## INTERNSHIP

### Eligibility Requirements

- U.S. Citizens that are 18 years old at time of application
- Majoring in STEM discipline
- Full-time student or recent graduate (undergraduate, graduate, or post-doc)
- Minimum cumulative GPA 3.0 or higher (4.0 scale)

### Funding

Monthly stipend, dislocation allowance, housing allowance, & professional travel.

### Internship Location

Locations vary but are typically in Mississippi, Maryland, Ohio, & California. Some opportunities are remote.

### Final Reporting

Research paper and oral report.

## CALL FOR INTERNS

FY24

The **Department of Defense's (DoD) High Performance Computing Modernization Program (HPCMP) High-Performance Computing Internship Program (HIP)** develops the skills of future computational scientists and offers an opportunity for prospective DoD employees to experience defense-related research and development.

The HIP provides undergraduate and graduate students, majoring in science, technology, engineering, and mathematics (STEM) areas, internship opportunities to gain exposure to and experience with high-end computing (HEC) by working under the mentorship of scientists and engineers at DoD facilities across the nation.

Interns will be paired with DoD mentors for a 10-week on-site research experience.

## FACTS

Applications:

**November 2023 to March 2024**

https://www.zintellect.com

## Program Benefits

* Learn from and collaborate with scientists and engineers at DoD facilities across the nation.
* Contribute to significant Research, Development, Test, Evaluation & Acquisitions Engineering activities.
* Develop critical skills and establish long-term connections.
* Receive financial support including a stipend and travel allowances.
* Gain a competitive advantage and improve long-term career opportunities.

DoD HPC

*Have a question? Email us at*

**HIP@hpc.mil**

*Faculty Immersion*

# EXPERIENCE

*(FIX)*

**You can harness high performance computing resources to solve our most critical Department of Defense mission challenges**

FY24

The Faculty Immersion Experience seeks to provide research experiences for university faculty while strengthening collaboration, enhancing research capabilities, and encouraging broader university-level participation in high-end computing (HEC)

- Selected faculty members collaborate directly with researchers at DoD laboratories on projects that leverage HPCMP resources.
- Participants are encouraged to have collaborative summer research with students during their appointment.
- Stipend is based on faculty position (i.e., assistant, associate, full professor).

## Award Benefit

- Appointments are for 10 weeks in the summer term
- Stipend, round-trip domestic travel to laboratory and housing allowance are included
- Labs provide training seminars and professional development opportunities

## Eligibility

- U.S. Citizen
- Must work full-time at an accredited, degree-granting, post-secondary US institution (includes community college). Adjunct or visiting faculty are ineligible
- Must work in an area of physics, chemistry, non-medical biology, engineering, environmental sciences, geology or geosciences, mathematics, materials sciences, or computer or computational sciences

## FACTS

Applications:

**November 2023 to March 2024**

https://www.zintellect.com

## Program Benefits

* Learn from and collaborate with scientists and engineers at DoD facilities across the nation.
* Contribute to significant Research, Development, Test, Evaluation & Acquisitions Engineering activities.
* Develop critical skills and establish long-term connections.
* Receive financial support including a stipend and travel allowances.
* Gain a competitive advantage and improve long-term career

*Have a question? Email us at*

**HIP@hpc.mil**