

```
mirror_mod = modifier_ob.  
set mirror object to mirror.  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
  
print("please select exactly  
  
-- OPERATOR CLASSES ----  
  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
  
context):  
context.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

DAF CISO's Small Business Cybersecurity Resources Lollapalooza



Jan 30, 2024

Website

The Blue Cyber Education Series for Small Businesses [webpage](#)



Daily Office Hours

We have daily office hours for answering/researching your questions about Small Business cybersecurity and data protection!



DAF CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

U.S. Small Business Cybersecurity Boot Camp on November 28. Register [HERE](#)



EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING WEBINAR

[Click here for the registration link and agenda](#) for the Small Business Every-Tuesday Small Business Cybersecurity Ask-Me-Anything*

SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS	+
SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS	+
SMALL BUSINESS CYBERSECURITY MEMOS	+
CYBERSECURITY-AS-A-SERVICE SUPPORT AGENCIES (BLUE CYBER IS #4)	+
DCMA DIBCAC PRESENTATIONS	+
NSA DIB DEFENSE SERVICES	+
DAU DEFENSE ACQUISITION UNIVERSITY SMALL BIZ CYBER RESOURCES	+
NCA NATIONAL CYBERSECURITY ALLIANCE "CYBERSECURE MY BUSINESS" RESOURCES	+
NIST SMALL BUSINESS CORNER CYBERSECURITY RESOURCES	+
CISA SMALL BUSINESS RESOURCES	+
PHISHING PROTECTION STRATEGIES	+
DC3 DCISE DIB SERVICES	+

DAF CISO'S BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on www.sbir.gov/events

Daily Open Office Hours sign-up [LINK](#)

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/ Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Events

All FREE and PUBLIC
www.sbir.gov/events

40 Presentations
Vides and PowerPoints

SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS	+
SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS	-
FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL BUSINESS	
DDO CYBERSECURITY INCIDENT REPORTING	
GET YOUR SP8S ON DOCUMENTING COMPLIANCE WITH NIST SP 800-171	
CAN I GIVE MY CONTRACTOR CUI?	
DAF FAST TRACK ATO INFORMATION	
PROTECTING OF COMMON TYPES OF DOD CUI	
SMALL BUSINESS CYBERSECURITY RESOURCES	
SMALL BUSINESS NEEDS BIG CYBERSECURITY	
THREAT BRIEFING FOR SMALL BUSINESSES	
WHERE TO BEGIN WITH NIST SP 800-171	
DDO CLOUD COMPUTING	
HACKERS ARE WATCHING YOU	
HARDENING WINDOWS FOR NIST SP 800-171	
QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES	
DEMISTIFYING NIST ZERO TRUST ARCHITECTURE FOR SMALL BUSINESS	
SMALL BUSINESS ZERO TRUST STEPS - VERIFY EVERY TIME	
CMMC LEVEL 1 AND FAR 52-204-21: BASIC CYBER HYGIENE	
DCMA DIBCAC PRESENTATION NIST SP 800-171 CONFIGURATION MANAGEMENT	
DCMA DIBCAC PRESENTATION NIST SP 800-171 POLICY PROCEDURES OVERVIEW	
DCMA DIBCAC PRESENTATION ON NIST SP 800-171 ENCRYPTION REQUIREMENTS	
THE IMPORTANCE OF DIB SMALL BUSINESS CYBERSECURITY	
SAFEGUARDING FEDERAL CONTRACT INFORMATION (FCI)	
CYBER SUPPLY CHAIN RISK MANAGEMENT PRIMER	
CISA TO THE RESCUE! CISA RESOURCES	
COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW	
17 WAYS TO BE MORE CYBER SECURE TODAY!	
DCMA DIBCAC CYBERSECURITY AUDIT COMMON DEFICIENCIES	
COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW ZERO TRUST	
DDO MENTOR/PROTEGE PROGRAM	
SMALL BUSINESS CYBERSECURITY MEMOS	+



PR Proposed Rule

Cybersecurity Maturity Model Certification (CMMC) Program

A Proposed Rule by the [Defense Department](#) on 12/26/2023



This document has a comment period that ends in 41 days (02/26/2024)

SUBMIT A FORMAL COMMENT

48 comments received. [View posted comments](#)

PUBLISHED DOCUMENT

Start Printed Page 89058

AGENCY:

Office of the Department of Defense Chief Information Officer (CIO),
Department of Defense (DoD).

ACTION:

Proposed rule.

SUMMARY:

DOCUMENT DETAILS

Printed version:
[PDF](#)

Publication Date:
12/26/2023

Agencies:
[Department of Defense](#)
[Office of the Secretary](#)

Dates:
Comments must be received by
February 26, 2024.

Comments Close:
02/26/2024

<https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>

Poll



**How many employees
do you have in your
small business or
academic/research
institution?**

```
mirror_mod = modifier_ob.  
#set mirror object to mirror_  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
#selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
-- OPERATOR CLASSES ----  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
context):  
context.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

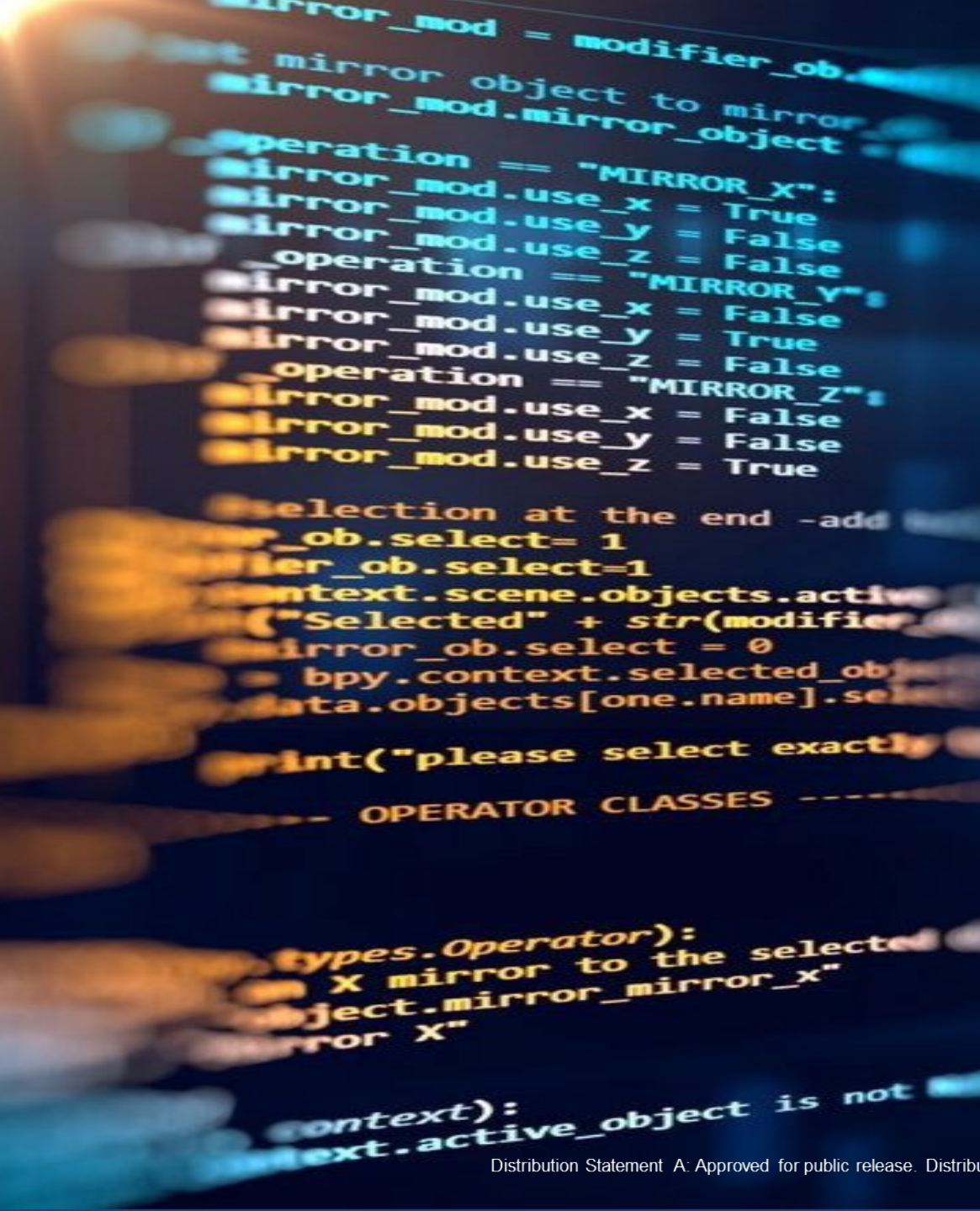
*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

Kick Off DAF CISO Mr. Aaron Bishop



Jan 30, 2024

BLUE CYBER EDUCATION SERIES



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

United South and Eastern Tribes - USET

Rebecca Naragon



Jan 30, 2024
BLUE CYBER EDUCATION SERIES

[Video at https://youtu.be/FqMYGtUi7PU](https://youtu.be/FqMYGtUi7PU)

[8 minutes](#)

```
mirror_mod = modifier_ob.  
set mirror object to mirror.  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
-- OPERATOR CLASSES ----  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
context):  
context.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

Defense Acquisition University

Ken Carkhuff



Jan 30, 2024

BLUE CYBER EDUCATION SERIES

DAU



DAU SMALL BUSINESS ASSISTANCE FOR BLUE CYBER LOLLAPALOOZA ON 30 JAN 2024

Distribution Statement A: Approved for public release: distribution is unlimited.

LEARNING OPTIONS

- Classroom
- Online
- Certification Training
- Credentials
- Continuous Learning
- 547 Courses
- 50,000 Learning Assets

DAU Virtual Campus

The screenshot displays the DAU Virtual Campus user interface. At the top left is the DAU logo. A navigation bar includes links for Home, Learning, Connect, Reports, and Help Desk. A search bar is located in the top right corner. The main content area features a personalized dashboard for a user named Abel. It includes a profile section with 13 completions and 5 hours of learning. Below this are sections for 'Your Subjects' (with an 'Add' button), 'Your Language(s)', and 'Your Playlists' (with 0 created, 0 followers, and 0 followed, and a 'Create New Playlist' button). A 'Transcript View' section shows 0 past due, 3 due soon, and 2 assigned/no due date items. A prominent orange banner indicates 'DUE SOON' for 'Unauthorized Disclosure of Classified'. To the right, a banner welcomes the user to the new Learner Home and prompts them to add subjects. Below this is a 'Continue Learning' section with four course cards: 'Annual OSD RIM Training', 'Unauthorized Disclosure of', 'OPSEC Awareness', and 'DAU Mandatory Training Guide'. Each card shows the course title, status (Registered), and a 'Launch' button.

<https://dau.csod.com/>

DAU Quick Links



Updated DAWIA requirements, certification training and elective learning options

- **[DAWIA Certification](#)**: Streamlined certification framework and functional area-based training
- **[Defense Acquisition Credentials](#)**: Training programs tailored to job functions and skills
- **[DAU Courses](#)**: Training courses designed specifically for Defense acquisition professionals and available in-person and online
- **[Commercial Training](#)**: Access to online training resources from leading providers such as Coursera, LinkedIn Learning and more



Acquisition tools and resources to improve job performance and build skills

- **[Tools](#)**: Resources and job aids help complete tasks
- **[Library](#)**: Research and information resources from DoD and commercial sources
- **[Events](#)**: Opportunities to hear directly from leaders, experts and practitioners while earning CLPs. Watch live or on-demand
- **[DAU Media](#)**: Access videos and podcasts on a wide variety of topics and interest areas, including the TEDxDAU video collection
- **[Community Hub](#)**: Knowledge sharing and collaboration around specific interests



Acquisition consulting, tailored training and workshops for individuals and teams

- **[Acquisition Consulting](#)**: Customized services to help overcome specific challenges and solve complex problems
- **[Executive Coaching](#)**: One-on-one support to help leaders effectively manage high-performing teams
- **[Workshops](#)**: Sessions designed around specific issues, requirements, or program objectives

DOING BUSINESS WITH THE DOD

Developing a Business Relationship with Department of Defense

It typically takes at least 24 months of planning before a government contractor wins their first contract. Plan to invest significant time and resources identifying potential opportunities, marketing to potential clients, developing proposals, winning and performing your first DoD contract while complying with DoD rules.



Small Business

Other than Small Business

All Things Small Business Podcast

Mindfully designed 30 minute conversations that connect our listeners to real-life issues impacting our small business community. Interview topics range from:

- Industry marketing strategies
- Business development & growth strategies
- True grit of being a small business owner
- Influence of socioeconomic programs

Did You Know?



People Employed by Small Business (Source: Census Bureau)



Small Businesses Represent 96% of Employer Firms in High-Patenting Manufacturing Industries (Source: SBA Office of Advocacy)



24% of All Patents in the Top 100 Emerging Clusters Belong to Small Business Firms (Source: SBA Office of Advocacy)



46.8% of Private Sector Firms Employ Less than 50 Employees (Source: Census Bureau)

Download the SBA Office of Advocacy FAQs

Industry Resources

Learn more about Small Business Programs, Government Procurements, Collaboration and more by using the resource links below.

Business

Using Resources from the Department of Defense

Making it

SMALL BUSINESS COURSES

- Recommended courses:
 - CON 0040 Market Research
 - CON 0090 Strategies for Contracting with Service-Disabled Veteran-Owned Small Businesses (SDVOSBs)
 - CLM 059 Fundamentals of Small Business for the Acquisition Workforce
 - CLC 045 Partnering
 - CLC 059 Management of Subcontracting Compliance
- To access course information: <https://icatalog.dau.edu/>

SMALL BUSINESS COURSES

SBP 1010 - Introduction to Small Business Programs, Part A
SBP 2010 - Intermediate Small Business Programs, Part A



Upon successful completion - you will be able to:

- Describe the importance of small business to the industrial base
- Apply the appropriate small business programs and initiatives to support the decision-making process
- Summarize the various small business systems necessary for expanding small business opportunities
- Demonstrate key SBP activities during market research
- Advise the acquisition team of small business elements of the solicitation
- Demonstrate SBP activities during the evaluation and the source selection process
- Determine methods for addressing post-award small business issues

<https://www.dau.edu/training/career-development/contracting/blog/DAU-Deploys-SBP-1010---Introduction-to-Small-Business-Programs,-Part-A>

<https://www.dau.edu/training/career-development/contracting/blog/DAU-Deploys-SBP-2010---Intermediate-Small-Business-Programs-Part-A/>

SMALL BUSINESS COURSES

- CAC or DAU account required (<https://www.dau.edu/faq/p/New-DAU-Account>)
- All SBP VILT classes are now available for self-registration by DoD employees in the virtual campus.
- FAI will be offering DAU equivalent SBP VILT courses starting in Mar 2024. <https://fai.gov>
- Students enroll and disenroll themselves
 - Registration closes 10 days prior to the start of the class
 - https://dau.csod.com/catalog/CustomPage.aspx?id=221000349&tab_page_id=221000349

DAU SMALL BUSINESS MEDIA PAGE



13:30
CONTRACTING CONVERSATIONS
CSBP 001 - Small Business Professional Credential
JIM WILLIAMS JIM VALLEY



05:10
All Things Small Business: SBP 202V (2020V)...



AbilityOne PROGRAM ★
AbilityOne: Development and Determination of the Fair Market Price - AbilityOne Series - AbilityOne Development and...



DAU
Welcome to the Small Business Series Adversarial Foreign Investments
Access speaker slides and other information ->
<https://www.dau.edu/report/Small-Business-Series-Adversarial-Foreign-Investments-15-Dec-2022>
Mics: Audio will be muted throughout the session
Recording: This session will be recorded and posted on the event page
01:54:52
Questions: Please submit questions via chat.
Small Business Series - Adversarial Foreign Investments
Dial in (Audio only) 1-571-403-8146 Phone Conference ID: 669 862 5729



01:54:15
Summer Small Business Pricing Series
Public Vouchers and Real-time Labor Evaluations -...



DAU
Welcome to the Spring Small Business Series The 2023 DoD Small Business Strategy
Access speaker slides and other information ->
01:50:25
Small Business Series - The 2023 DoD Small Business Strategy
Mics: Audio will be muted throughout the session
Recording: This session will be recorded and posted on the event page
Questions: Please submit questions via chat.
Dial in (Audio only) 1-571-403-8146 Phone Conference ID: 669 862 5729

<https://media.dau.edu/channel/Small%2BBusiness/62965391>

DAU CYBERSECURITY MEDIA PAGE

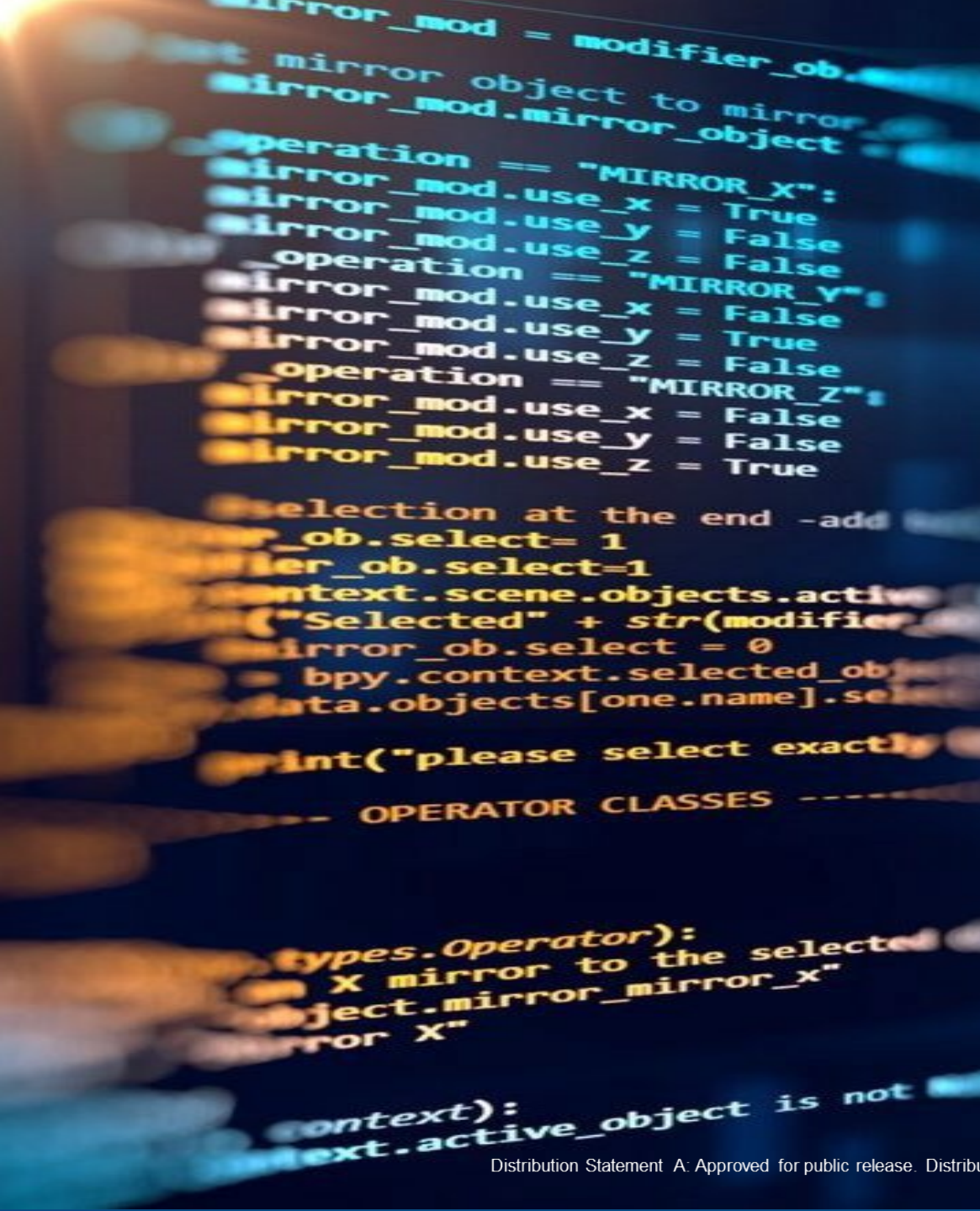
⇒ CYBER - DAU WEB EVENTS



⇒ CYBER COURSES AND WORKSHOPS



<https://media.dau.edu/channel/CyberSecurity/62925431>



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

Cybersecurity and Infrastructure Security Agency

JD Henry



Jan 30, 2024

BLUE CYBER EDUCATION SERIES



CISA

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

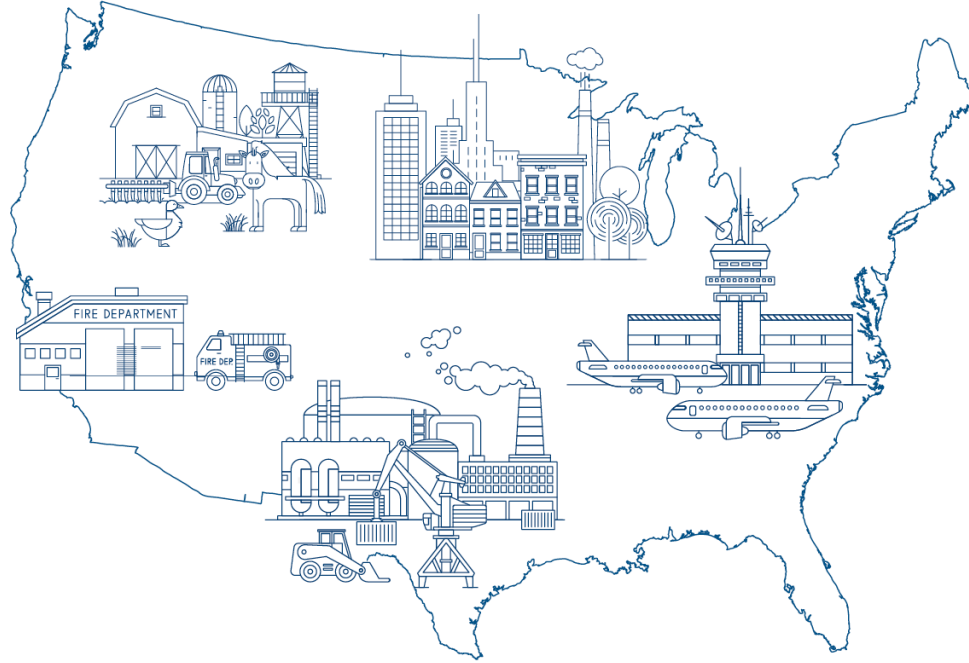
Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.





Integrated Operations



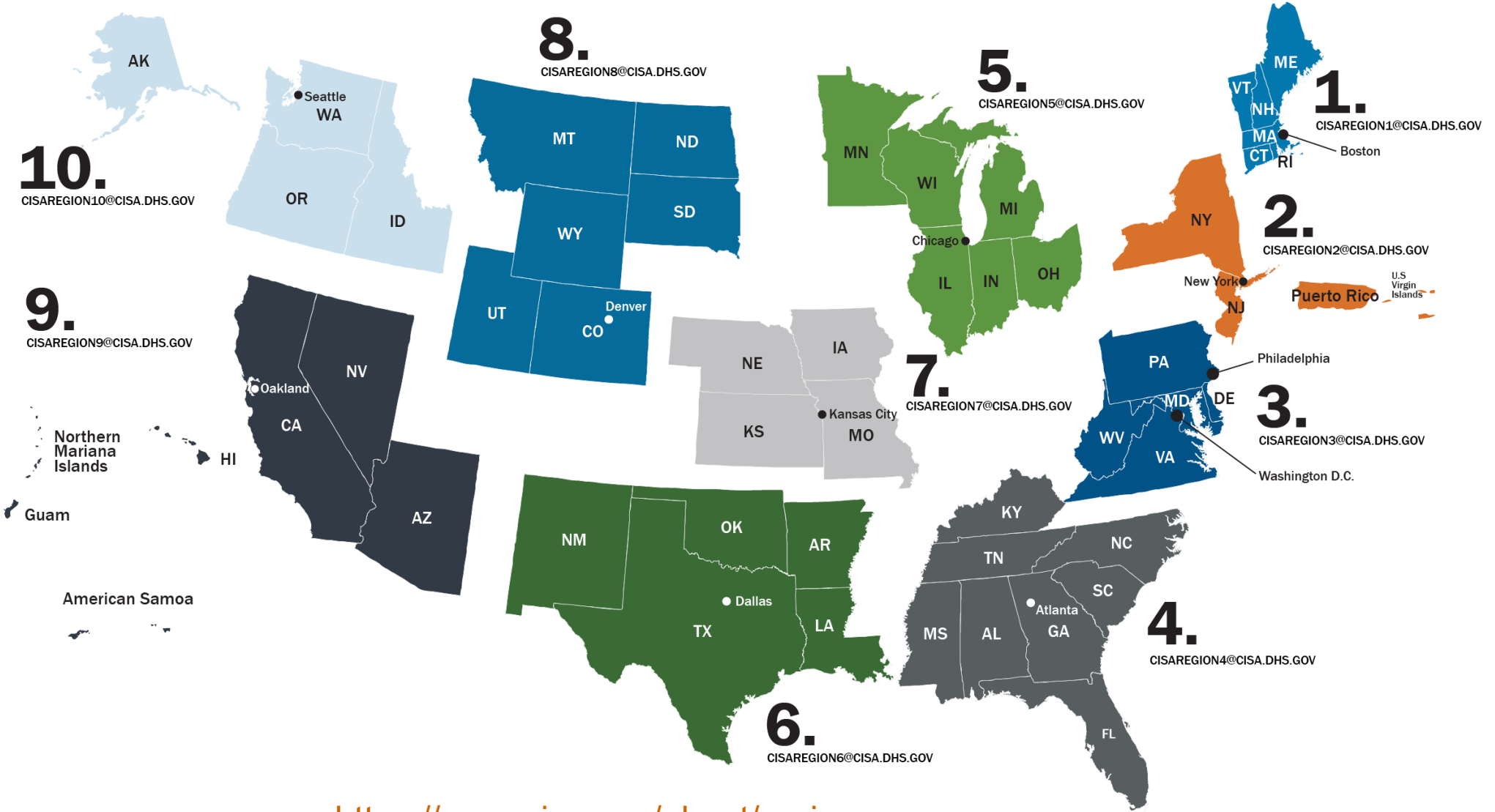
HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- ▶ Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- ▶ Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

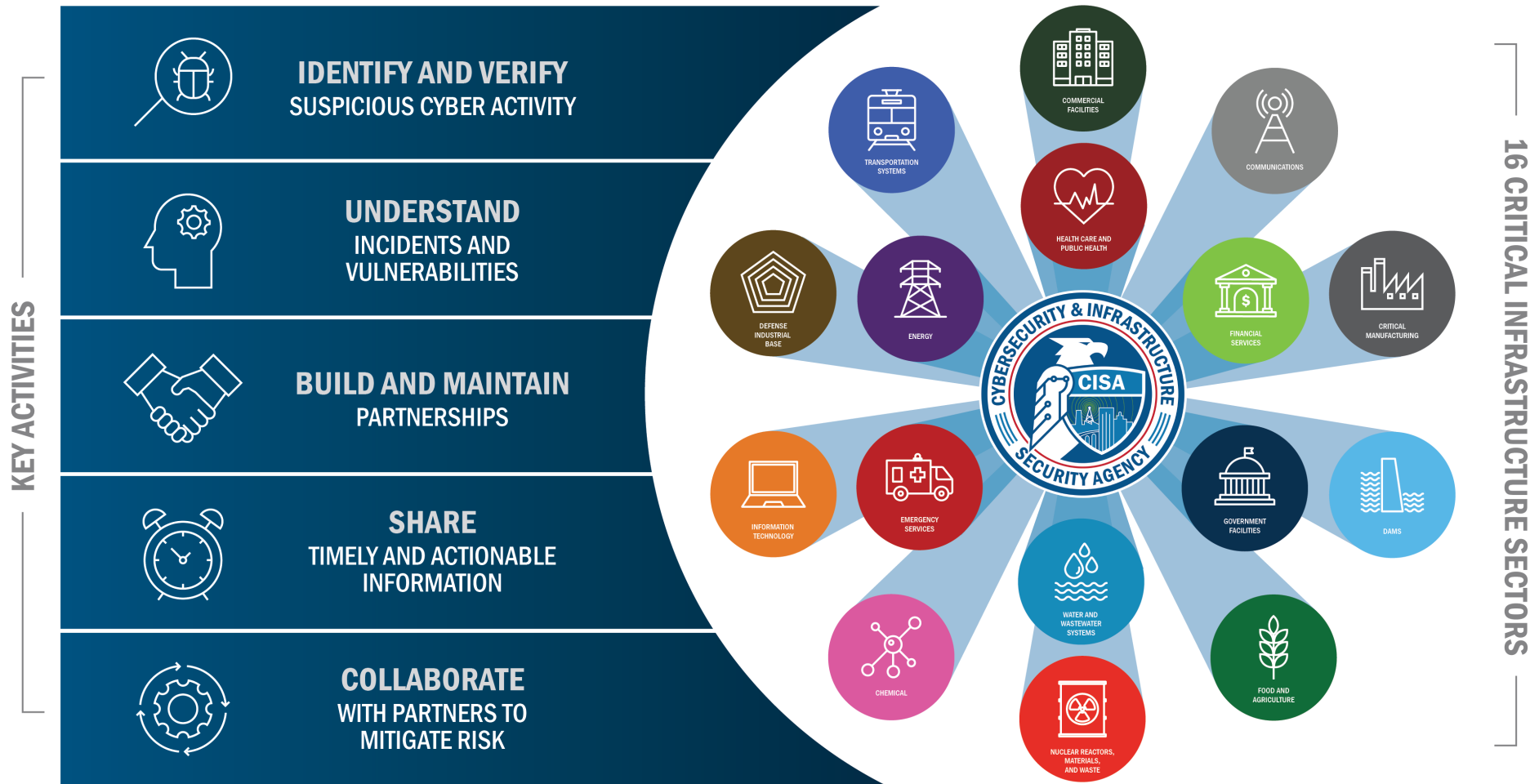
CISA enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



Serving Critical Infrastructure



TODAY'S CYBER THREAT LANDSCAPE



Cyber Threats of Today*

* Not an exhaustive list!

TLP: CLEAR

Ransomware

- Double/Multi-extortion (Lockbit Conti, Hive, Vice Society, etc.)

Malware

- IT and OT specific malware

Denial of Service

- Cyber criminals, Hacktivists (KillNet / Aviation Sector)

Threats to External Dependencies

- 3rd party vendors, service providers, infrastructure providers
- Supply chain compromise

Advanced Persistent Threats (APTs)

- Highly sophisticated with substantial financial backing
- Various motivations (political, economic, etc.)



CISA SERVICES & RESOURCES



Cybersecurity Services

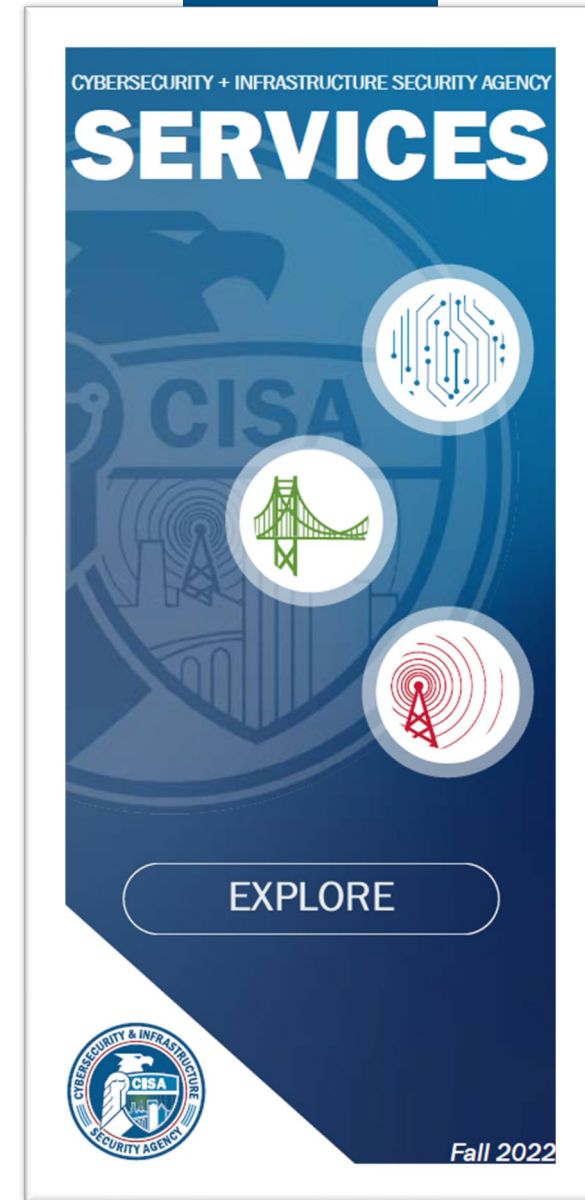
- **CISA Cybersecurity Services & Assessments**
 - Cyber Hygiene Vulnerability Scanning
 - Cybersecurity Performance Goals (CPG)
 - Cybersecurity Assessments
 - Tabletop Exercises (TTX)
 - Training
 - & more

For more information on these services and more, please visit

<https://www.cisa.gov/topics/cyber-threats-and-advisories>

or

<https://www.cisa.gov/cyber-resource-hub>



Cyber Hygiene Vulnerability Scanning

GOAL:

Reduce exposure to threats by taking a proactive approach to identifying and mitigating attack vectors

- Hosts with no vulnerabilities detected are rescanned every 7 days
- Hosts with low-severity vulnerabilities are rescanned every 6 days
- Hosts with medium-severity vulnerabilities are rescanned every 4 days
- Hosts with high-severity vulnerabilities are rescanned every 24 hours
- Hosts with critical-severity vulnerabilities are rescanned every 12 hours



Email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.



Cybersecurity Performance Goals (CPGs)

- What are the CPGs?
 - A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
 - Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).
- How should organizations use the CPGs?
 - Inform strategy decisions and resource investment.

The CPG's Address:

- Account Security
- Device Security
- Data Security
- Governance and Training, Vulnerability Management,
- Supply Chain/Third Party, Response and Recovery
- Other (network segmentation, email, etc,)

The most current version of the CPGs is located at:

<https://www.cisa.gov/cpg>



Where to Find Them

- The most current version of the CPGs is located at: <https://www.cisa.gov/cpg>
- Here you can find:



The core list of CPGs



CPG Checklist



Spreadsheet of all text content



Link to our GitHub discussion page



The screenshot shows the CISA website header with navigation links for CYBERSECURITY, INFRASTRUCTURE SECURITY, EMERGENCY COMMUNICATIONS, NATIONAL RISK MANAGEMENT, ABOUT CISA, and MEDIA. Below the header is a section titled 'CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS' featuring a blue banner with the text 'CYBERSECURITY PERFORMANCE GOALS'. Below the banner is a paragraph of text:

In July 2021, President Biden signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. This memorandum required CISA, in coordination with the National Institute of Standards and Technology (NIST) and the interagency community, to develop baseline cybersecurity performance goals that are consistent across all critical infrastructure sectors. These voluntary cross-sector Cybersecurity Performance Goals (CPGs) are intended to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts.

The CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. The goals were informed by existing cybersecurity frameworks and guidance, as well as the real-world threats and adversary tactics, techniques, and procedures (TTPs) observed by CISA and its government and industry partners. By implementing these goals, owners and operators will not only reduce risks to critical infrastructure operations, but also to the American people.

Cybersecurity Performance Goals

Approximate Cost/Impact/Complexity ratings to inform investment planning.

Mapping to NIST CSF Subcategory

8.1 Network Segmentation	PR.AC-5, PR.PT-4, DE.CM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
<p>COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: HIGH</p> <p>TTP OR RISK ADDRESSED: Network Service Discovery (T1046) Trusted Relationship (T1199) Network Connection Enumeration (ICS T0840) Network Sniffing (T1040, ICS T0842)</p> <p>RECOMMENDED ACTION: All connections to the OT network are denied by default unless explicitly allowed (e.g. by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.</p>		<p>DATE:</p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>	<p>DATE:</p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>	

MITRE ATT&CK TTPs addressed by the Goal

How organizations can demonstrate the effective implementation the security practice, based on input from CISA's collaborative stakeholder process. These Actions will be updated regularly as new threats and defenses arise.



Cyber Information Sharing

Information sharing is the key to preventing a wide-spread cyber-attack. CISA develops partnerships to rapidly share critical information about cyber incidents.

Cybersecurity Alerts & Advisories

- Offers the latest cybersecurity news, advisories, alerts, tools, and resources.
- Found at:

<https://www.cisa.gov/news-events/cybersecurity-advisories>



CYBERSECURITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023

Alert Code: AA23-144a



J.D. Henry
January 29, 2024

Reducing Risk of Known Exploited Vulnerabilities



CISA's Known Exploited Vulnerabilities Catalog

The following sections detail the criteria behind each of the three thresholds for KEV catalog updates, which are:

- The vulnerability has an **assigned Common Vulnerabilities and Exposures (CVE) ID**.
- There is reliable evidence that the vulnerability **has been actively exploited** in the wild.
- There is a **clear remediation action** for the vulnerability, such as a vendor-provided update.

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



<https://www.cisa.gov/stopransomware>

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE CISA.GOV



Getting Ahead of the Ransomware Epidemic:

CISA's Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs



STOP RANSOMWARE

UPDATED

Ransomware

#STOPRANSOMWARE

GUIDE

HAVE YOU BEEN HIT BY RANSOMWARE?

LEARN MORE



Protection and Response



Services



Public Safety



Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Ransomware Vulnerability Warning Pilot (RVWP)

- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), signed into law in March 2022, required CISA to establish the RVWP
- CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including
 - CISA's Cyber Hygiene Vulnerability Scanning service
 - Administrative Subpoena Authority
- CISA Regional staff members, located throughout the country, make notifications and may provide resources to mitigate the vulnerability.



Ransomware Vulnerability Warning Pilot (RVWP)

- In 2023, CISA conducted more than 1,700 notifications to various organizations about open vulnerabilities on their networks that are specifically exploited by ransomware actors
- If you receive a notification, you can verify the identity of the CISA personnel through CISA Central: Central@cisa.gov or (888) 282-0870.



2023 Pre-Ransomware Notifications

In 2023, CISA conducted more than 1200 pre-ransomware notifications to include:

7
U.S. Water and Wastewater
Sector Entities

37
U.S. Transportation System
Sector and Energy Sector
Entities

39
U.S. Emergency Services
Sector Entities

274
U.S. and Int'l K-12 School
Districts & Institutes of
Higher Education

154
U.S. Healthcare
Organizations

94
U.S. State, Local, Tribal, and
Territorial Governments

Driven by the cybersecurity research community, infrastructure providers, and cyber threat intelligence companies about potential early-stage ransomware activity.



<https://www.cisa.gov/secure-our-world>

- CISA's cybersecurity awareness program to provide small businesses, communities and individuals with the guidance and tools they need to protect themselves online.

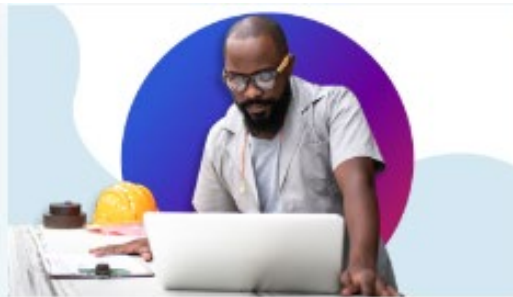
The program emphasizes four simple steps:

- Use strong passwords and a password manager.
- Turn on multifactor authentication.
- Recognize and report phishing.
- Update software.



Secure Yourself & Your Family

Quick steps we can all take to greatly increase our safety and protect our money, identity, data and more.



Secure Your Business

Prevent malicious threats that could cause hassle, financial losses or even business closure. Protect your business, employees and customers!



Secure Your Products

Adopt Secure by Design practices for your products that reasonably protect against malicious actors and put customer safety first.



Cyber Incident Reporting

When to Report:

If there is a suspected or confirmed cyber attack or incident that:

- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

REPORTING CYBER ATTACKS

- Contact CISA at central@cisa.gov or 888-282-0870
- FBI Field Office: <http://www.fbi.gov/contact-us/field> or the FBI's 24-7 Cyber Watch at 855-292-3937 or by e-mail at cywatch@fbi.gov
- State reporting laws & requirements
- Regulatory Authorities



“If You See Something, Say Something”

TLP: CLEAR

Protect your every day.

RECOGNIZE THE SIGNS OF TERRORISM-RELATED SUSPICIOUS ACTIVITY

EXPRESSED OR IMPLIED THREAT
Communicating a spoken or written threat to commit a crime that could harm or kill people or damage a facility, infrastructure, or secured site

OBSERVATION/SURVEILLANCE
A prolonged or unusual interest in facilities, buildings, or infrastructure beyond casual or professional interest, in a suspicious manner

PHOTOGRAPHY
Taking pictures or videos of persons, facilities, buildings, or infrastructure in a covert manner, such as taking photos or video of security-related equipment or personnel, infrequently used access points, or the structure of a building

THEFT/LOSS/DIVERSION
Stealing or diverting items—such as equipment, uniforms, or badges—that belong to a facility or secured site

TESTING OR PROBING OF SECURITY
Challenging or testing a facility's security or IT systems to assess the strength or weakness of the target

AVIATION ACTIVITY
Operating or interfering with the operation of an aircraft that poses a threat of harm to people and property

BREACH/ATTEMPTED INTRUSION
Unauthorized people trying to enter a restricted area or impersonating authorized personnel

MISREPRESENTATION
Presenting false information or misleading documents to conceal possible illegal activity

ELICITING INFORMATION
Questioning personnel beyond mere curiosity about an event, facility, or operations

ACQUISITION OF EXPERTISE
Gaining skills or knowledge on a specific topic, such as facility security, military tactics, or flying an aircraft

CYBERATTACK
Disrupting or compromising an organization's information technology systems

RECRUITING/FINANCING
Funding suspicious or criminal activity or recruiting people to participate in criminal or terrorist activity

SABOTAGE/TAMPERING/VANDALISM
Damaging or destroying part of a facility, infrastructure, or secured site

MATERIALS ACQUISITION/STORAGE
Acquisition and/or storage of unusual materials such as cell phones, radio controllers, or toxic materials

WEAPONS COLLECTION/STORAGE
Collection or discovery of unusual amounts of weapons including explosives, chemicals, or other destructive materials

SECTOR-SPECIFIC INCIDENT
Actions which raise concern to specific sectors, (e.g., power plant) with regard to their personnel, facilities, systems, or functions

The above activities should only be reported if they are conducted in a manner that would arouse suspicion of terrorism.

If you **see** something, **say** something
REPORT SUSPICIOUS ACTIVITY TO LOCAL AUTHORITIES OR CALL 9-1-1 IN CASE OF EMERGENCY

dhs.gov/SeeSay

"If You See Something, Say Something®" is a national campaign that raises public awareness of the signs of terrorism and terrorism-related crime, and how to report suspicious activity to state and local law enforcement.

To become a partner, send an email to:
seesay@hq.dhs.gov

For more information visit:
www.dhs.gov/see-something-say-something



J.D. Henry
January 29, 2024

Questions?

Central@CISA.GOV
888-282-0870

Or

<https://www.cisa.gov/about/regions>

Or



All CISA services and resources can be found by visiting
www.CISA.gov





For more information, visit [CISA.gov](https://www.cisa.gov) or contact central@cisa.dhs.gov

```
mirror_mod = modifier_ob.  
#set mirror object to mirror_  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
#selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
-- OPERATOR CLASSES ----  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
context):  
context.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

Project Spectrum.io

Derrick Davis



Jan 30, 2024

BLUE CYBER EDUCATION SERIES



PROJECT SPECTRUM

Supporting Resilience in Cybersecurity and Developing the DIB Cloud Environment

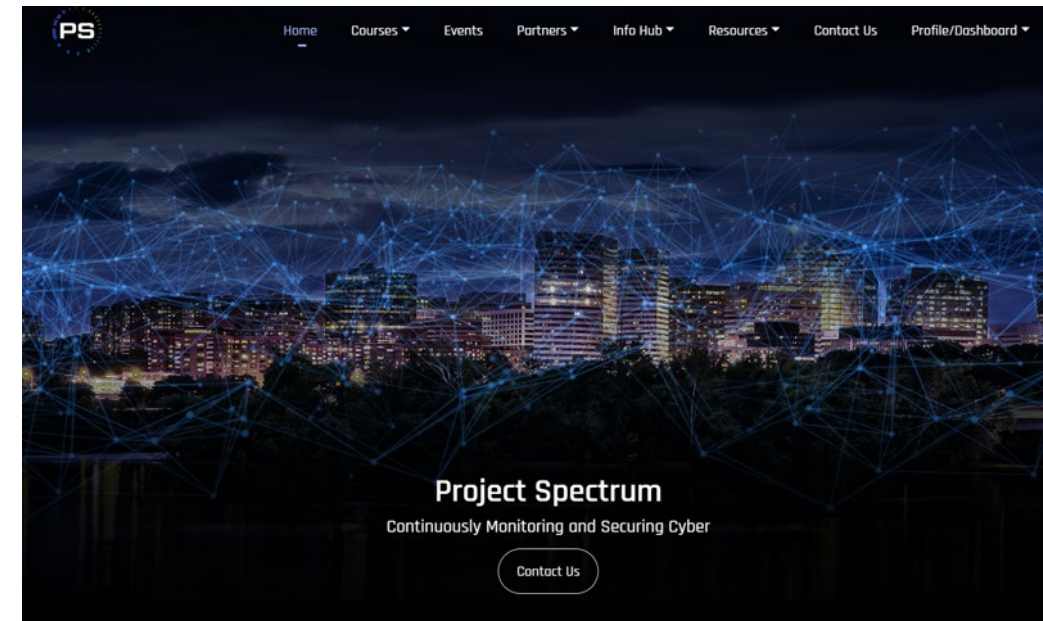
Derrick Davis

1/29/2024

CYBERSECURITY FOR SMALL BUSINESSES AND THE DIB



- Project Spectrum is a DoD-supported initiative through the Office of Small Business Programs (OSBP)
- PS provides a comprehensive, cost-effective platform of cybersecurity information, resources, tools, and training
- The PS mission is to improve the cybersecurity readiness, resilience, and compliance of small/medium-sized businesses and all DIB companies



Why Project Spectrum?



- Small businesses comprise more than 70% of the DIB
- 25% of DoD prime contracts are awarded to small businesses
- Nearly 43% of all cyberattacks target small- and medium-sized businesses

(Statistics as of August 2023)

The numbers definitively show that small businesses within the DIB are the most targeted. Project Spectrum's no-cost security services help level the playing field.



WHY SMALL BUSINESSES ARE TARGETED



Access to sensitive government information



Intellectual property



Connection with larger defense contractors



Focused on production and meeting deadlines, not 'extraneous' activities like cybersecurity



Limited cybersecurity resources due to funding; ill-prepared to handle cyberattacks



The Government 'Mandate'

Via FAR's clauses 252.204-21 and 252.204-7012, the Federal Government requires businesses to properly protect both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

FCI is sensitive, but not classified, information that is provided by or generated for the Government under a contract. FCI is a subset of CUI.

CUI is a broad category of sensitive information, while unclassified, that requires safeguarding and the dissemination of security controls pursuant to federal laws, regulations and policies.

Examples of FCI

- Contract information
- Organizational charts
- Process documentation
- Contract performance reports
- RFP or RFI responses

Examples of CUI

- Proprietary Business Information (PBI)
- Unclassified Controlled Technical Information (UCTI)
- Sensitive but Unclassified (SBU)
- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES)

CMMC Model



CMMC Level 1 is considered as **“Foundational”** for basic data safeguarding for businesses that only handle FCI data.

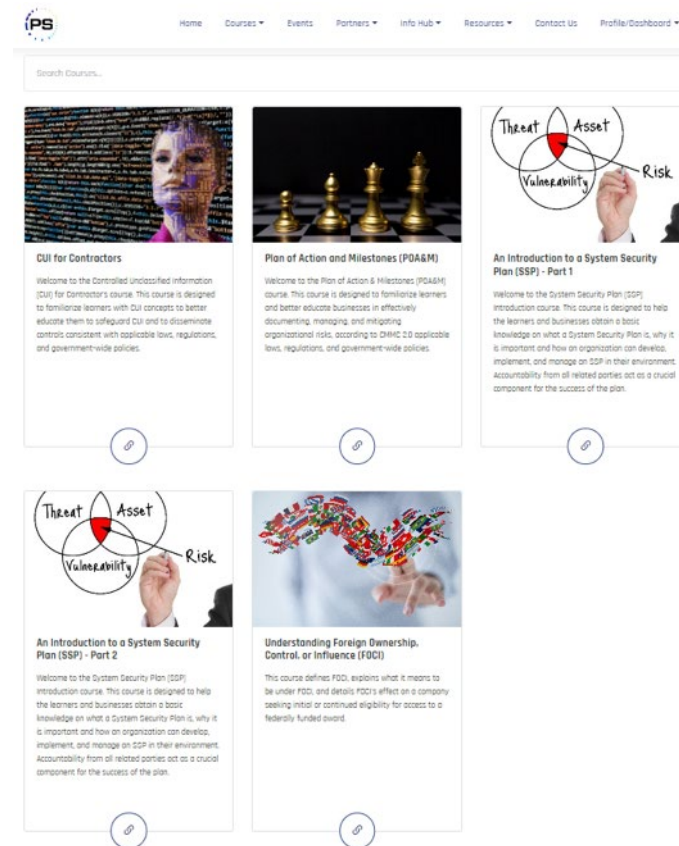
CMMC Level 2 is considered as **“Advanced”** for enhancing data safeguarding for businesses that handle CUI “prioritized” and “non-prioritized” data acquisitions.

CMMC Level 3 is considered as **“Expert”** for high capacity in safeguarding CUI data that carries the highest priority for DoD programs.

	<i>Model</i>		<i>Assessments</i>
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	<i>CUI, highest priority programs</i>	Triennial Gov't-led
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	<i>CUI, prioritized acquisitions</i>	Triennial Third-Party
		<i>CUI, non-prioritized acquisitions</i>	
LEVEL 1 Foundational	17 practices	<i>FCI, not critical to national security</i>	Annual Self-Assessment

Project Spectrum has developed a robust cybersecurity training program built upon a proprietary Learning Management System:

- Full Scope Training courses focused on: CUI for Contractors, Plan of Actions & Milestones, CMMC Level 1, and Systems Security Plan Fundamentals
- 26 'micro-courses' that provide training on core CMMC controls
- DIY tools enabling companies to conduct self-assessments against NIST and CMMC standards





Developing the DIB's Secure Cloud Environment

Project Spectrum is leading the way in developing the DIB's Secure Cloud Environment to ensure the protection of the DIB's cyber-based assets.

Why do we need a Secure Cloud Environment for the DIB?

- Small businesses in the DIB are limited in their ability to meet increasing cybersecurity requirements for the protection of Department of Defense (DoD) information and operations.
- The problem is especially critical for small disadvantaged businesses that do not have the expertise or resources to meet the stringent DoD security controls along with emerging monitoring and mitigation requirements.
- A solution that only stores DoD data in such a secure, managed cloud does not need to meet the DoD requirements for on-premise security and safe storage and development of DoD technical data.

Secure Cloud Deployment Expectations



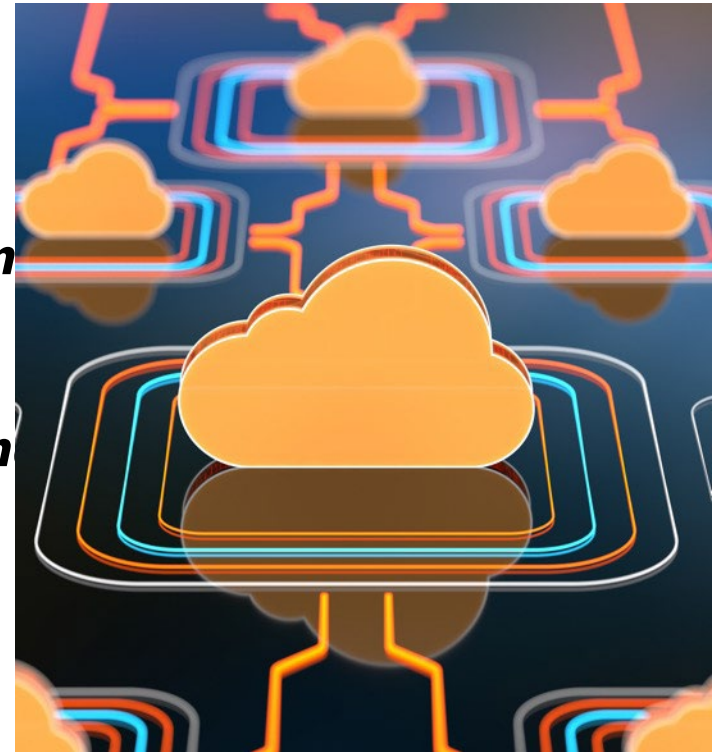
- We will provide a secure hosting environment that supports thin-client services to enable small business DIB companies to meet most DoD cybersecurity and emerging FOCI requirements as defined by statute.
- Our cloud architecture provides secure storage, processing, and transmission of controlled unclassified information through a virtual desktop technology.
- The solution supports CMMC / NIST 800-171 compliance and due diligence standards.
- The solution is cloud-agnostic and can be deployed on local servers (for OCONUS-based companies) and commercial cloud offerings such as AWS (for CONUS-based companies).
- The solution uses Infrastructure-as-Code for automated easy deployment.
- The solution provides secure clean-up when the environment is not used.

The Secure Cloud Environment Pilot Mechanics



Our DIB pilot will include 50 small businesses. As part of the pilot, we will collect the following metrics for evaluation:

- ***Usability of the platform (subjective metrics on ease of use)***
- ***System Performance metrics (including latency of access, uptime of the infrastructure)***
- ***Compliance metrics (including number of reported incidents and number of cyber-attacks on the infrastructure)***
- ***Cost incurred per small business for using the infrastructure***
- ***Tool requirements per participating small business***





Deployment Timelines and Challenges

- The Secure Cloud Environment will be ready for pilot deployment and testing in the next six months on a cohort of 50 small businesses chosen from Mentor-Protégé Program and rapid innovation fund participants that are part of project Spectrum.
- The small businesses in the pilot cohort will be uniformly chosen from the OCONUS and CONUS-based companies.
- The usability and security will be assessed using the deployment.
- Cost estimate for the pilot will be approximately \$10M.
 - *The government will cover the cost of the pilot at not cost to the participants. At scale, there will be a low-cost offering covered by the government and a subscription-based model paid for by users.*
- Challenges
 - *Liability associated with data storage belongs to pilot participants.*
 - *Ongoing cost to deploy and scale the secure cloud to CMMC level 2.0 companies*



HOW TO CONNECT WITH PROJECT SPECTRUM

- Visit <https://projectspectrum.io> and register for your FREE account
 - Begin your self-assessment to establish your baseline
 - Access the PS comprehensive suite of tools, training, and resources
- Email the PS Outreach and Cyber Advisory teams
 - Contact outreach@projectspectrum.io
- Follow PS on social media
 - LinkedIn, Twitter, and YouTube
- Check the PS calendar of events on our website for upcoming presentations, webinars, etc.

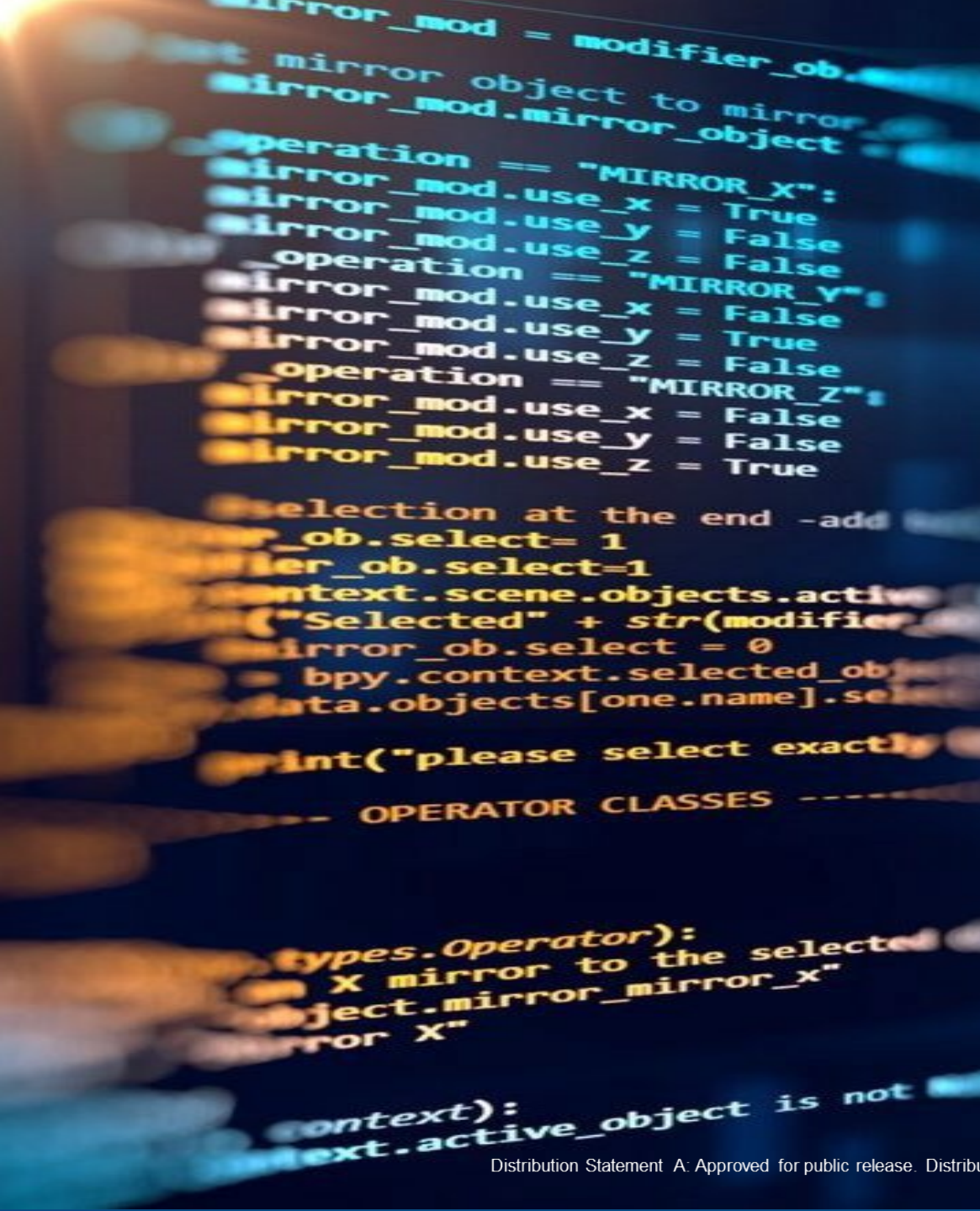




PROJECT SPECTRUM

**Thank you for your
time and attention**

Project Spectrum Briefing



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

DoD Cyber Crime Center DCISE

Scott Taylor



Jan 30, 2024

BLUE CYBER EDUCATION SERIES

DoD Cyber Crime Center

A Federal Cyber Center

DCISE 101





UNCLASSIFIED

DoD Cyber Crime Center (DC3)

A Federal Cyber Center

■ Cyber Forensics Lab (CFL)

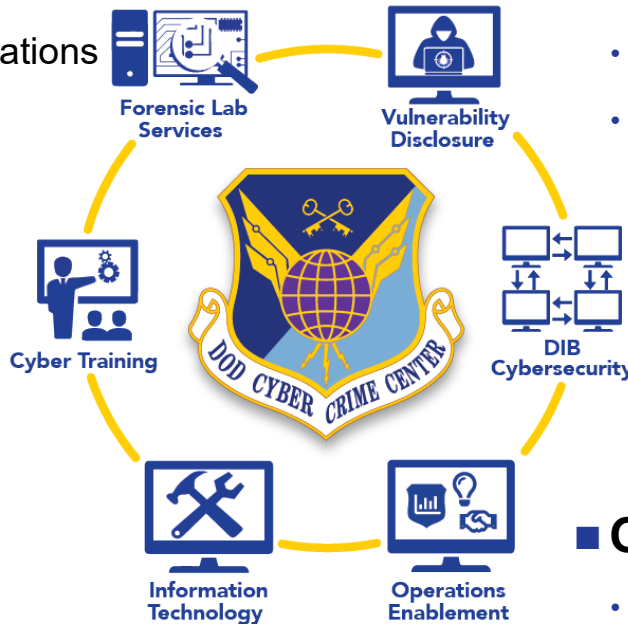
- Nationally accredited lab with exquisite digital forensics
- Support range of military operations and classifications
- Federated forensics and DC3 Pacific

■ Cyber Training Academy (CTA)

- In-residence, online, and mobile training teams
- Intermediate and advanced cyber courses
- LE/CI, Cyber Mission Forces, and International

■ Information Technology (XT)

- R&D of software and systems solutions
- Electronic Malware Submission, DC3 Advanced Carver
- Federated approach to standards, tagging, information sharing



■ Vulnerability Disclosure Program (VDP)

- Crowdsourced vulnerabilities on DoD systems
- 5,000 white-hat researchers from 45 countries
- Strong partnership with USCYBERCOM/JFHQ-DoDIN

■ Industrial Base Collaboration (DCISE)

- Cybersecurity partnership with 1,000+ CDCs
- Voluntary/mandatory DIB incident repository
- Expanded cybersecurity offerings

■ Operations Enablement (OED)

- Sharply focused technical/cyber intelligence analysis
- Counter FIE threats to DoD, USG, and DIB
- DoD solutions integrator in support of LE/CI/Cyber

Strategy and Partner Engagements (XE):

Deliberate partnerships to enable action - share insights - efficiently reduce risk

UNCLASSIFIED



Operational Element of DoD's DIB CS Program

Designated as the single DoD focal point for receiving all cyber incident reports affecting DIB unclassified info/networks

Voluntary reporting responsive to the DIB CS Framework Agreement

- A public-private partnership enabling:
 - Analytic support and forensic malware analysis for the DIB
 - Increased USG and industry understanding of cyber threat (analytic products, semi-annual technical exchanges, etc.)
 - Enhanced protection of unclassified defense information
 - Confidentiality of shared information

Mandatory reporting responsive to:

- DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*
- DFARS Clause 252.239-7010, *Cloud Computing Services*
- 32 CFR Part 236, *DIB Cyber Security Activities*, and others



DoD's DIB Cybersecurity (CS) Program

A public-private cybersecurity partnership established by DoD CIO and executed by DC3:

- Provides a collaborative environment for sharing unclassified and classified cyber threat information
- Offers analyst-to-analyst exchanges, mitigation, remediation strategies, Cybersecurity-as-a-Service
- Provides analytic support and forensic malware analysis to DIB Partners
- Protects confidentiality of shared information
- Increases US Government and industry understanding of cyber threats
- Enables companies to better protect unclassified defense information on company networks or information systems



Mission: Enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems



Participation

- DIB CS Participants are CDCs*:
 - Large, mid, and small-sized defense contractors
 - Sole source providers, market competitors, joint-development partners, supply chain vendors
 - Manufacturers of weapon systems, platforms, and critical parts
 - Federally Funded Research and Development Centers (FFRDCs)
 - Commercial Solution and Service Providers
 - University Affiliated Research Centers



* - pending update to CFR 32 pt. 236, anticipated in CY 2024



Info Sharing & Collaboration



DIB NETWORK

Online incident reporting and access to DCISE threat products (NIPR & SIPR instances)



DIB TECHNICAL WEB/TELECONFERENCES

DIB Partners and DCISE Analysts address current adversary techniques and trends



A2A AND B2B MEETINGS

Tailored to Partner capabilities, threats, and dynamic cybersecurity considerations



TECHEX AND RPEX/VIPEX

Interactive forums for deep technical discussion on a wide variety of cyber threat related topics



CYBERSECURITY as a SERVICE (CSaaS)

No cost cybersecurity services to identify gaps in cyber resiliency and provide technological capabilities



PRODUCTS

Cyber threat products, warnings, and notices to strengthen cybersecurity

■ Analysis of nation-state Advanced Persistent Threat (APT) DIB cyber events since February 2008

- Performed ~ 79,000 hours of no-cost forensics and malware analysis
- Published ~ 15,000 cyber reports
- Shared ~ 610,000 actionable, non-attributional indicators
- Informed by multiple USG data streams (USIC, LE, CI, and industry cyber threat reporting)



Cyber Threat Information Sharing

- **DIBNet-Unclassified (DIBNet-U):** Unclassified PKI-protected web portal used by the DIB to report cyber activity, and includes new participant application process, document libraries, and cyber threat collaboration tools
- **Classified Cyber Threat Products:** Dissemination of classified Secret level cyber threat information incorporate multiple methods to include: Technical Exchanges (TechEx), Regional Partner Exchanges (RPEX), Analyst to Analyst (A2A) Engagements, Distribution via Classified Media, DC3/DCISE SIPR Intelink, Secure Phone & Fax.





DCISE CTI Products

- **DCISE Produces 12 different products ranging from indicator-based to strategic cyber threat analyses**
 - **Threat Information Product (TIP)**
 - Derived from USG reporting; includes relevant IOCs to DIB/CDCs and narrative context
 - **Customer Response Form (CRF) Rollup/Supplement**
 - CRF Rollup – Derived from DIB reporting; includes relevant IOCs to DIB/CDCs and narrative context
 - CRF Supplement – Produced when additional amplifying data becomes available after initially reported in CRF Rollup (i.e. malware samples)
 - **Cyber Targeting Analysis Report (CTAR)**
 - In-depth risk analysis product detailing adversarial cyber targeting of US DoD technology/platforms/systems
 - **Threat Activity Report (TAR)**
 - In-depth analysis of cyber threat actors' TTPs against DIB targets
 - **DCISE Notifications**
 - Alerts, Warnings, Advisories, TIPPERS, Cyber Incident Notifications (CINs)
 - Vehicles to notify DIB Partners of varying levels of cyber threats (critical through situational)
 - **Weekly Indicator Round-Up (WIR)**
 - Roundup of DCISE IOCs released in DCISE products for the given week
 - **Cyber Threat Round-Up**
 - Compilation of relevant cyber news articles, posted to DIBNET splash page
 - **Slick Sheets (on varying topics)**



DCISE Expanded Offerings: Cyber Resilience Analysis (CRA)

- Interview-based analysis of organization's current CS resilience posture
- Collection of 300 questions in 10 security domains
- Questions mapped to CMMC, NIST 800-171, NIST Cybersecurity Framework domains, and the Cybersecurity Framework Profile for Ransomware Risk Management
- Facilitated analysis over 6–8 hours in person or virtually
- Final report highlights strengths and weaknesses
- Partners who have repeated CRAs have seen a 90% increase in compliance for underperforming domains





DCISE Expanded Offerings

Cybersecurity as a Service

DCISE³

- Compares DIB Partner firewall logs to DIB, USG, and commercial threat feeds
- Individual dashboards for DIB Partners
- Anonymized aggregated dashboards for DCISE analysts
- Auto-blocking feature supported on compatible firewalls
- Identified previously unknown vulnerable corporate assets
- Enabled proactive tipping to DIB Partners for instances of IOT vulnerabilities, SolarWinds compromises, Fortigate vulnerabilities, Confluence 0-days, ProxyShell targeting, malicious scanning activity
- Proved 80% uniqueness in DCISE indicators

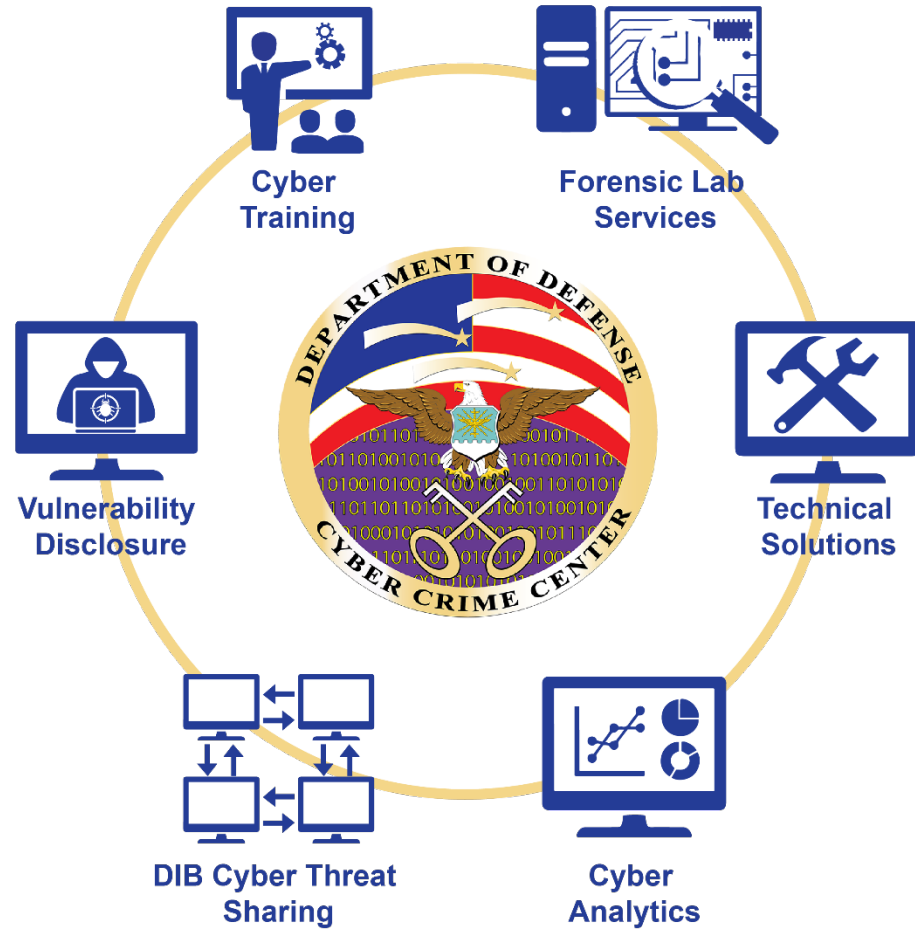
Adversary Emulation

- A form of penetration testing
- Leverages adversarial tactics, techniques, and procedures
- Test of DIB Partner security controls and policies against the most likely adversary to target them

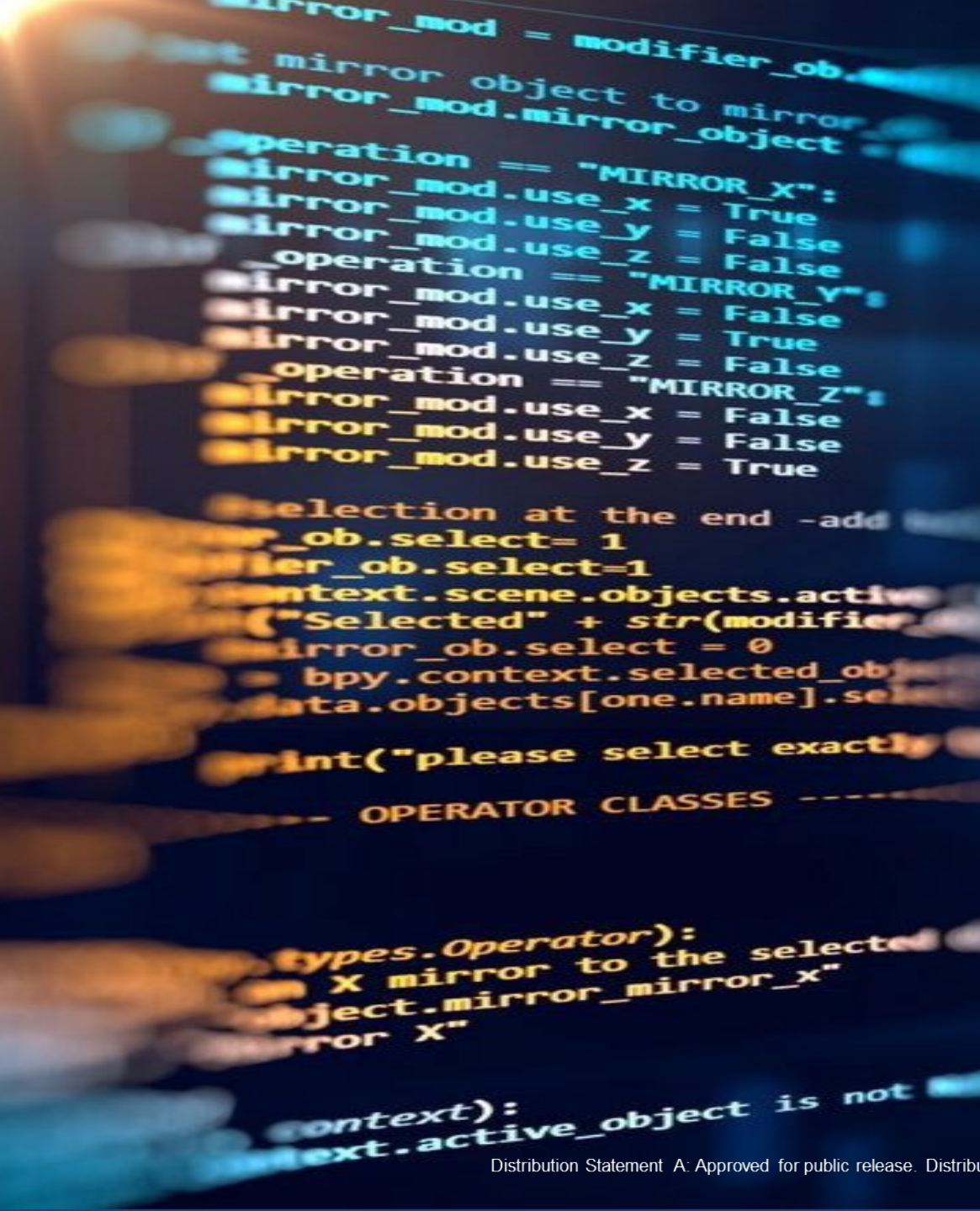




Questions?



dc3.dcise@us.af.mil
DCISE Hotline: (410) 981-0104
Toll Free: (877) 838-2174
Web: www.dc3.mil
on Twitter @DC3DCISE



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

NIST National Manufacturing Extension Partnership

Jyoti Malhotra



Jan 30, 2024

BLUE CYBER EDUCATION SERIES

The MEP National Network:

The Go-To Experts for Advancing U.S. Manufacturing: Cybersecurity

Dr. Jyoti Malhotra, Ph.D, National Programs Division



<https://www.nist.gov/mep/mep-national-network>



A unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

Our mission is to strengthen and empower U.S. manufacturers.



Delivering Value


As a public-private partnership, the Program delivers a high return on investment to taxpayers. **For every one dollar of federal investment** in FY 2022, the MEP National Network generated **\$35.80 in new sales growth** and **\$40.50 in new client investment**. This translates into more than **\$5.6 billion in new sales**. During this same time, **for every \$1,353 of federal investment**, the Network **created or retained one manufacturing job**.


A HIGH RETURN ON INVESTMENT TO TAXPAYERS

For Every One Dollar of Federal Investment

\$35.80
in New Sales
Growth 

\$40.50
in New Client
Investment 

This Translates into
More Than **\$5.6**
BILLION
in New Sales 

For Every **\$1,353** 
of Federal Investment the
Network Creates or Retains
One Manufacturing Job



FY22 Impact Survey Results

Over **116,700 JOBS** Created or Retained

**\$18.8
BILLION**
in New and
Retained Sales



**\$6.4
BILLION**



in Total Investment in
U.S. Manufacturing

**\$2.5
BILLION**
in Cost
Savings





Partnering to Drive a National Program

Over
1,450



Manufacturing
Experts



85.9

Net Promoter
Score

More than

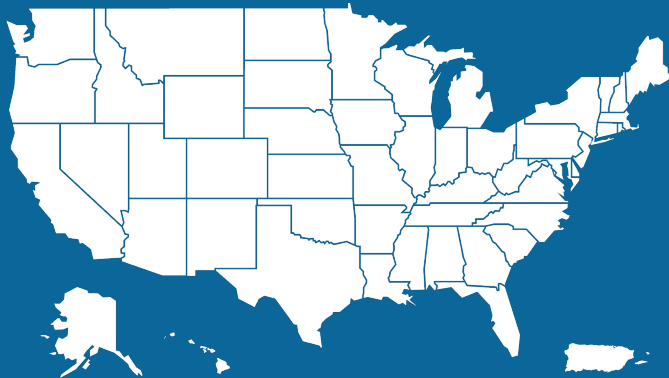
2,200



Partners

**NATIONAL
NETWORK**

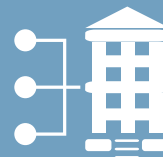
One Center in
Every State and
Puerto Rico



Approximately

430

Service
Locations





Our Partners



Economic
development
organizations



Federal agencies
& laboratories



Industry leaders
& think tanks



Manufacturing
USA Institutes



State & local
government



Universities,
community colleges
& technical schools



Trade associations
& other partners



Technical & Business Solution Examples





Cybersecurity Risk Management and Resilience

DID YOU KNOW?

Manufacturing is now the **most targeted** industry for cybersecurity attacks.¹

90%

of surveyed manufacturing executives identify **information technology (IT) and operational technology (OT) security** as a top spend area.²

\$105K

Average **cost of a data breach** for small businesses³

277 DAYS

Average **time to identify and contain** a data breach¹

In one study, about **1 out of 5 breaches** were the **result of supply chain compromises**. These breaches took an average of 26 days longer to identify and contain and were 2.5% more expensive.¹



Every MEP Center Can Provide Cybersecurity Services





- Awareness and training
- Basic cyber hygiene
- Business Continuity Planning
- Cyber Workforce development
- Digital Transformation / Industry 4.0
- Compliance with DOD cybersecurity requirements (DFARS/CMMC)
- Cyber integration into standards (e.g. AS 9100)
- Reduce cyber insurance costs
- Recover from a ransomware attack





Strengthening the Defense Supply Chain, By Helping SMMs:



-  Implement basic cyber hygiene requirements
-  Follow NIST SP 800-171
-  Conduct NIST SP 800-171 self-assessment
-  Transition to compliance with the CMMC program



Cybersecurity as a Way of Doing Business



Our appetite for
advanced technology
is rapidly exceeding our
ability to protect it.





HOW THE MEP NATIONAL NETWORK™ HELPS



MEP of Louisiana (MEPOL) helped *Haydel's Game Calls*, a 12-employee, nationally recognized leader in the manufacture of quality game calls with a “blow wet” feature that sets them apart, by conducting a cybersecurity assessment and training to make sure that its sensitive and highly competitive data and processes would be secure.⁹



New Hampshire MEP (NH MEP) helped *JMK, Inc.*, which designs, manufactures, and distributes commercial EMI/RFI powerline filters and suppression devices for commercial, military, and medical applications, engage Mainstay Technologies and performed a gap analysis for compliance to NIST 800-171. This included an action plan and milestones to achievement. The company, which had already experienced a data breach, was able to move forward with training, hardware installation, and procedures to enhance security.¹⁰



Manufacturing Works in Wyoming, helped **L&H Industrial**, a leader in technology innovations, custom manufacturing, and services for heavy industrial machinery used in mining, oil and gas, railways, and other industries stay on track to continue to do business with the DOD. This included linking them with 4th State Communications to document and solidify their internal cyber standards in order to complete a NIST 800-171 assessment and submit a new system security plan.¹¹



South Dakota Manufacturing and Technology Solutions helped **Rensberger Technologies**, a manufacturer with about 15 employees who create custom precision components for aerospace, defense, and medical equipment, achieve its AS9100 certification, complete a cybersecurity compliance assessment, and develop a system security plan, along with an action plan and milestones, enabling the company to retain its customers.¹²

Need Some Guidance?

The MEP National Network™ has the resources to help you safeguard your information, your systems, your employees, and your product. Contact your local MEP Center for assistance.



Visit: <https://www.nist.gov/mep/mep-national-network>



Call: 1-800-MEP-4MFG



Connect with Us

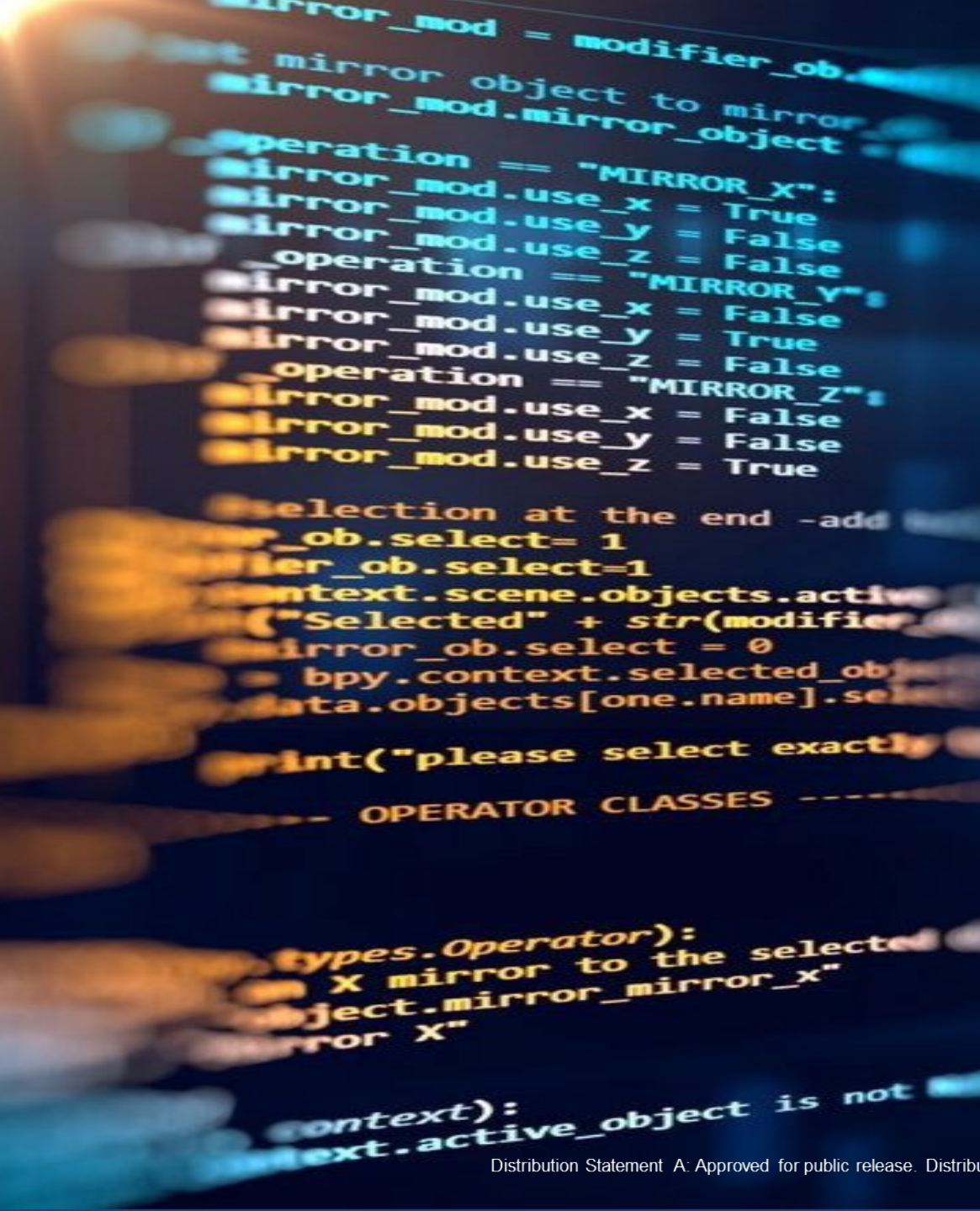


Visit Our Blog

www.nist.gov/blogs/manufacturing-innovation-blog

Visit Our Website

www.nist.gov/mep



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

National Cybersecurity Alliance

Cliff Steinhauer



Jan 30, 2024
BLUE CYBER EDUCATION SERIES



**NATIONAL
CYBERSECURITY
ALLIANCE**

Small Business Cybersecurity Resources

Cliff Steinhauer
Director, Information Security & Engagement

We empower a more secure, interconnected world.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.



HBCU
Career
Program



NATIONAL CYBERSECURITY ALLIANCE

For Your Business

Resources



<https://staysafeonline.org/programs/cybersecure-my-business/>

Contact Max McKenna max@staysafeonline.org

01

Hands-on Activities

02

Instructor Led

03

Modular Design

04

Industry Partnerships

05

Implementation and Follow-up



SMB Resources

<https://staysafeonline.org/resources/cybersecurity-for-business/>

Think Intelligent About Artificial Intelligence

April 27, 2023 = 4 min read

Stay Secure While You Work From Home

March 10, 2023 = 4 min read

Detect Incidents

December 1, 2022 = 2 min read

4 Simple Steps to Better Protect Your Company from Cyberattacks

October 31, 2022 = 9 min read

Advancing collective risk management efforts in the financial sector

October 26, 2022 = 12 min read

Small Business Quick Wins

November 16, 2022 = 9 min read

6 Ways to Help Employees be Privacy Aware

October 13, 2022 = 6 min read

Gaining 360-Degree SecOps View to Trounce Cyber Threats with Cyber Fusion

October 12, 2022 = 9 min read

The Security Culture Connection

October 20, 2022 = 6 min read



Breaking down the NIST Framework

1. **Identifying** and understanding which business assets (“digital crown jewels”) others want
2. Learning how to **protect** those assets
3. **Detecting** when something has gone wrong
4. **Responding** quickly to minimize impact and implement an action plan
5. Learning what resources are needed to **recover** after a breach

01	Identify
----	-----------------

02	Protect
----	----------------

03	Detect
----	---------------

04	Respond
----	----------------

05	Recover
----	----------------



SMB Resources

<https://staysafeonline.org/programs/cybersecure-my-business/>

Identify

Assess the cybersecurity risks to your organization.

[Learn more](#)

Protect

Implement a cybersecurity plan for your business, protect your customers and train your employees to guard against cyber threats.

[Learn more](#)

Detect

Awareness of key threats will enable you to employ practices and behaviors that limit your company's risk.

[Learn more](#)

Respond

If your business has been victimized by a cyberattack, notify the appropriate authorities, work to recoup your losses and ensure attackers are brought to justice.

[Learn more](#)

Recover

The final step of making your business more cybersecure is the recovery efforts that follow response to a cyber incident.

[Learn more](#)

Small Business Cybersecurity Webinars

[Learn more](#)



Small Business Quick Wins

<https://staysafeonline.org/resources/small-business-quick-wins/>

Easy Steps for:

- Copier/Printer/Fax Security
- Email Security
- File Sharing
- Mobile Devices
- Point-of-sale systems
- Routers
- Social networks
- Software
- Third-party vendors
- USBs
- Websites
- Wi-Fi

Security Vendor Checklist

<https://staysafeonline.org/resources/vendor-security-checklist/>

20+ Questions to ask when choosing a security vendor, including:

- Does your company have a written controls plan that contains the administrative, technical and physical safeguards you use to collect, process, protect, store, transmit, dispose or otherwise handle our data (e.g., Information Security Plan)?
- Does the system or application that will be storing our company data provide access control mechanisms (e.g., unique user IDs, password standards, role-based access)? Please elaborate.
- How will you help me comply with all applicable privacy and security laws for my business?

On-Demand Webinars

https://www.youtube.com/playlist?list=PL7QHbjPSF0r41qjGuao_PA7Pp0haO9yNo

46 videos to help your business understand and mitigate cyber risk

Keeping Your Business Intelligent About AI
Thursday, May 23
Open TV, 13:00 PT

▶ PLAY ALL

CyberSecure My Business™
StaySafeOnline.org
46 videos 732 views Last updated on Jun 22, 2023

⋮ ↻ ⋮

▶ Play all **↻ Shuffle**

- Keeping Your Business Intelligent About AI**
StaySafeOnline.org • 492 views • 8 months ago
50:10
- Secure Your Business: Getting Started**
StaySafeOnline.org • 329 views • 1 year ago
55:06
 - Check your settings – not an expert
 - Don't hand over sensitive information
 - Patch your systems
 - Don't click on untrusted links
 - Don't click on email links
- Scam Alert! How to Avoid Online Scams and Fraud**
StaySafeOnline.org • 2.5K views • 1 year ago
1:00:16
- Understanding the Evolution of Ransomware for Small & Medium Sized Businesses**
StaySafeOnline.org • 247 views • 2 years ago
9:47
- Proactive Measures for Ransomware**
StaySafeOnline.org • 324 views • 2 years ago
4:27
- Resources to Help You Defend Against Ransomware**
StaySafeOnline.org • 224 views • 2 years ago
4:56

Resources For Your Employees

Security Awareness Training Videos

<https://staysafeonline.org/resources/security-awareness-episodes/>



8 episodes

Passwords

Data Handling

Computer Theft

Phishing and Ransomware

Removable Media

Vishing

Internet Downloads

Wi-fi

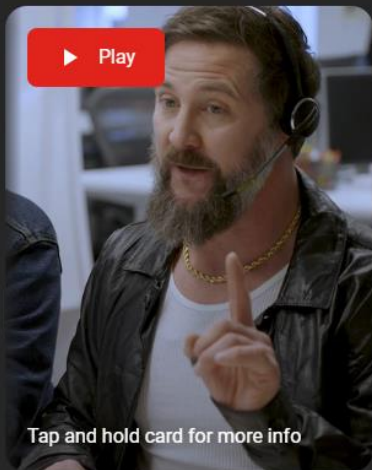
Downloadable from

<https://staysafeonline.org/resources/security-awareness-episodes/>

Kubikle Series

Kubikleseries.com

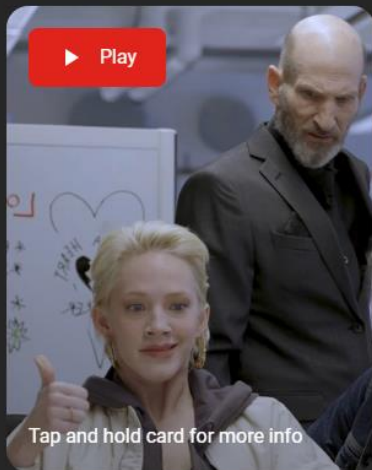
EPISODE 3



Romance

ROMANCE SCAMS

EPISODE 4



Copy Copy

PHISHING

EPISODE 5



Smooth Operator

VISHING

12 episodes

Humor and entertainment focused Netflix style short series (each video is 2-5 minutes)

Free Toolkits

<https://staysafeonline.org/resources/online-safety-privacy-basics/>



Anti-Cyberbullying Toolkit

Updated: June 1, 2023

[READ MORE](#)



Online Romance Scams Toolkit

Updated: June 1, 2023

[READ MORE](#)



Vacation and Travel Security Tips

Updated: June 16, 2023

[READ MORE](#)



Teach Others How to Stay Safe Online



Safe Online Holiday Shopping

Updated: June 1, 2023

Tip sheets
Infographics
Social media posts and graphics
On-demand webinars

Online Safety Basics

<https://staysafeonline.org/resources/online-safety-privacy-basics/>

Avoid Search Engine Ad
Malware!

February 9, 2023 = 2 min

True Love or Candy-Coated
Con: Identifying Romance
Scams

January 30, 2023 = 0 min

Online Romance and
Dating Scams

January 27, 2023 = 5 min

Public Computers and Wi-
Fi

January 19, 2023 = 4 min

What Is Data Privacy?

December 21, 2022 = 6 min

What to Do if Your
Password Manager Is
Breached

January 19, 2023 = 7 min

Securing Your Home
Network

December 20, 2022 = 3 min

How to Be an Online
Privacy Snob

December 20, 2022 = 6 min

Dongles, Sticks, Drives,
and Keys: What to Know
About Removable Media

December 20, 2022 = 7 min

Top tips on

- Passwords
- MFA
- Software Updates
- Phishing

Additional resources on

- Remote work
- Security on the go
- Securing your home network
- And much more!

Additional Resources

Non-Profit Cyber Resources: <https://nonprofitcyber.org/nonprofit-cyber-solutions-index/>

NIST Small Business Cybersecurity Corner: <https://www.nist.gov/itl/smallbusinesscyber>

Order free publications from the FTC: <https://www.bulkorder.ftc.gov/>

CISA Small business resources: <https://www.cisa.gov/audiences/small-and-medium->

businesses

Stay safe online.



**NATIONAL
CYBERSECURITY
ALLIANCE**

Website

StaySafeOnline.org

Twitter

[@staysafeonline](https://twitter.com/staysafeonline)

Facebook

[/staysafeonline](https://www.facebook.com/staysafeonline)

LinkedIn

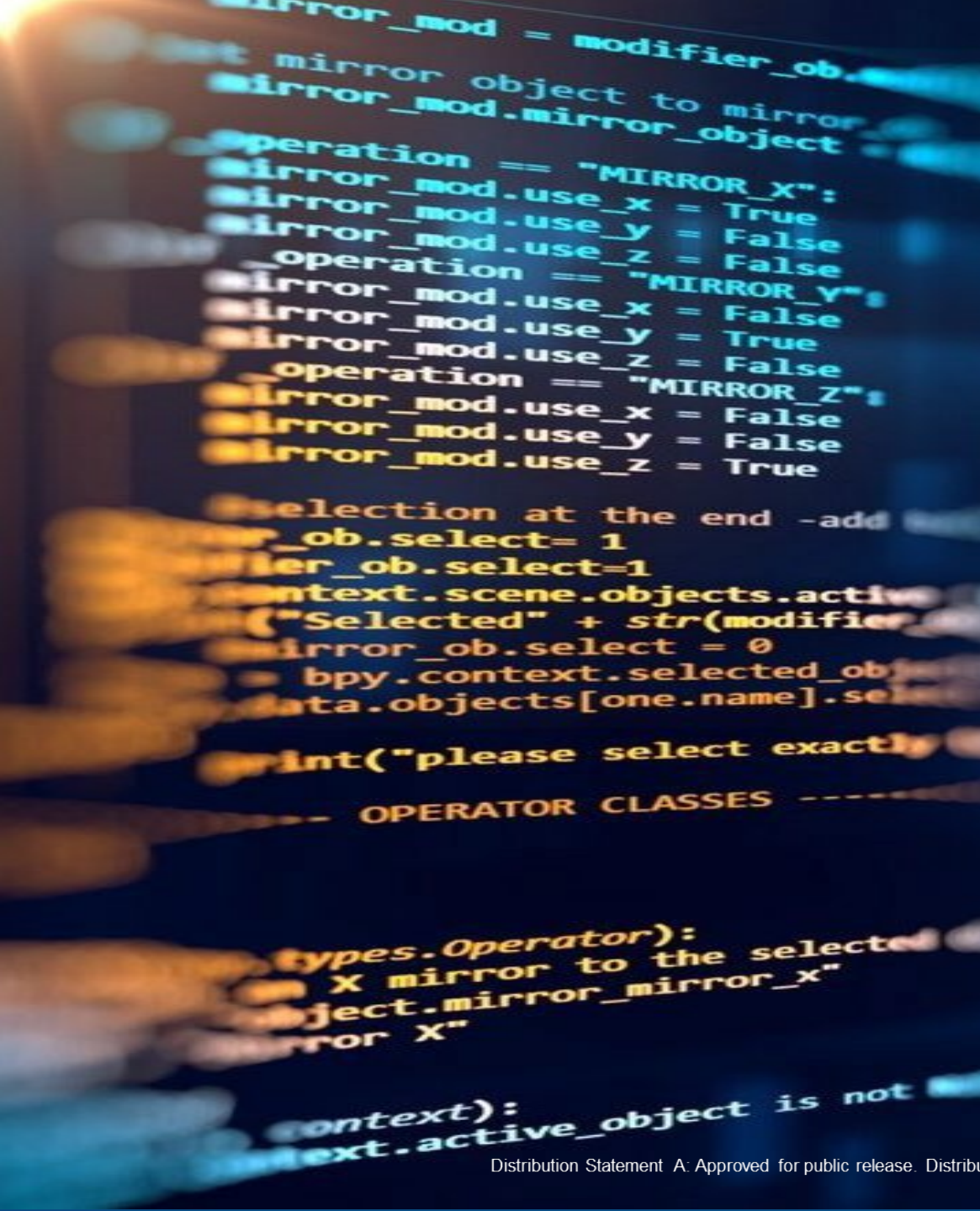
[/national-cyber-security-alliance](https://www.linkedin.com/company/national-cyber-security-alliance)

Instagram

[natlcybersecurityalliance](https://www.instagram.com/natlcybersecurityalliance)

Email

info@staysafeonline.org



AN OFFERING IN THE BLUE CYBER SERIES

*DAF CISO's
Small Business Cybersecurity Resources
Lollapalooza*

**New Mexico
APEX Accelerator Elythia McAnarney**

See Part 2 of this deck



Jan 30, 2024

BLUE CYBER EDUCATION SERIES