AN OFFERING IN THE BLUE CYBER SERIES:

# DOD Cybersecurity Incident Reporting

Version March 2024

#2 in the Blue Cyber Education Series

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-2004, 25 Jun 2021.

# Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contains many FARS and DFARS, some are listed some are referenced and you have to look them up.  These are not all, but some key security requirements.

What is a DFARS?  The Defense Federal Acquisition Regulation Supplement (DFARS) contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.

DFARS Clause 252.239-7010 Cloud Computing Services

FAR Clause 252.204-21 Basic Safeguarding of Covered Contractor Information Systems

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS  Clause 252.204-7008 Compliance with safeguarding covered defense information controls

DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements.

DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement

# DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information

# What if there is a potential breach?

Don't panic. Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize contractors acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.

Contact DoD immediately. Bad news does not get any better with time. These attacks threaten America's national security and put service members' lives at risk. DoD has to respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities. Contractors should report any potential breaches to DoD within 72 hours of discovery of any incident.

Be helpful and transparent. Contractors must also cooperate with DoD to respond to security incidents. Contractors should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review their networks to identify compromised computers, services, data and user accounts and identify specific covered defense information that may have been lost or compromised.

# What to Report to the Federal Government

*DHS Definition:* A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

*DFARS 7012 Definition* "Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

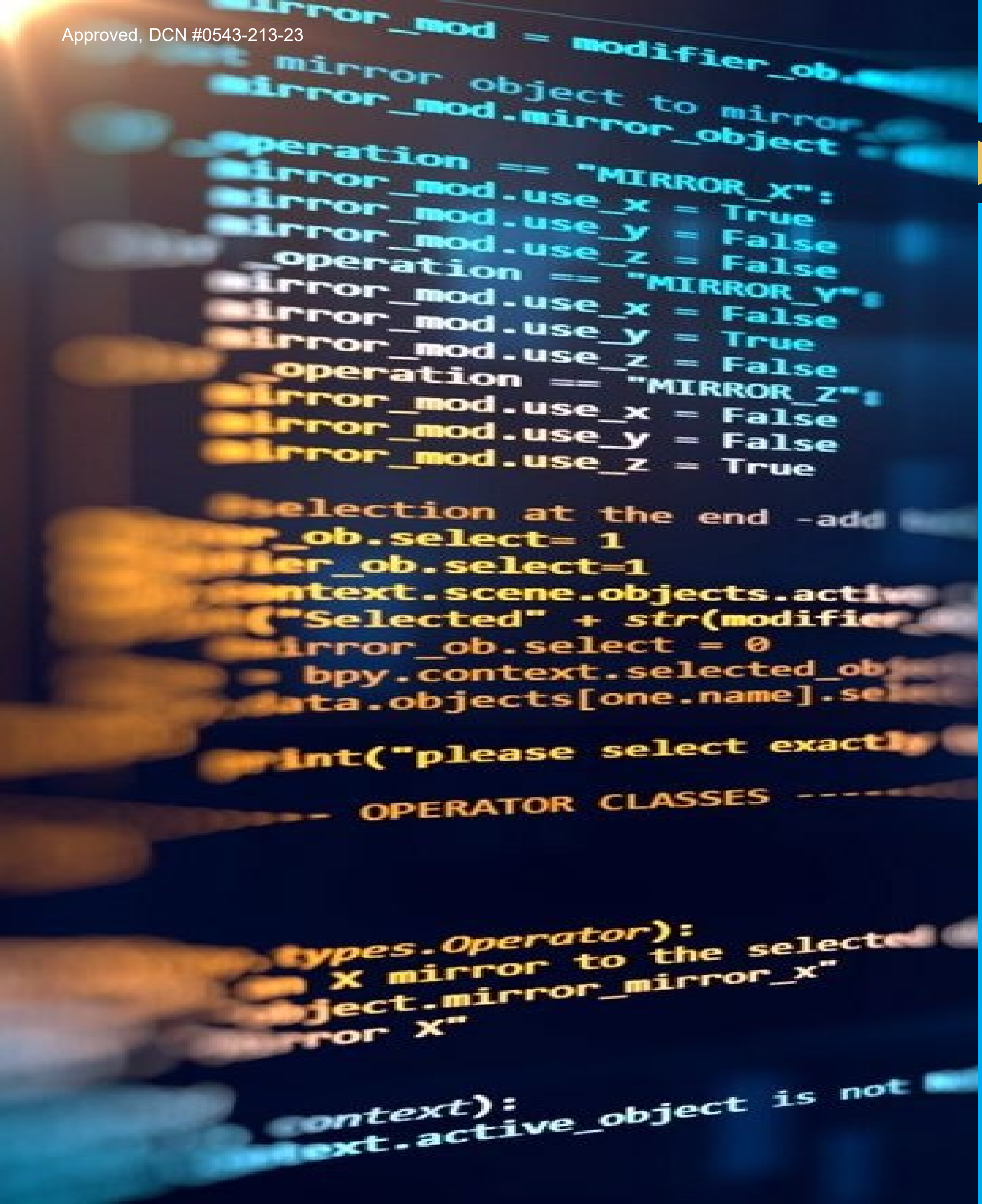
# Where to report cyber incidents/malware

To report cyber incidents that affect covered defense information Or that affect the contractor’s ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at https://dibnet.dod.mil/dibnet/ via an incident collection form (ICF).

If discovered and isolated in connection with a reported cyber incident, the contractor/ subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3). Also, https://dibnet.dod.mil/dibnet/

If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor

Approved, DCN #0543-213-23



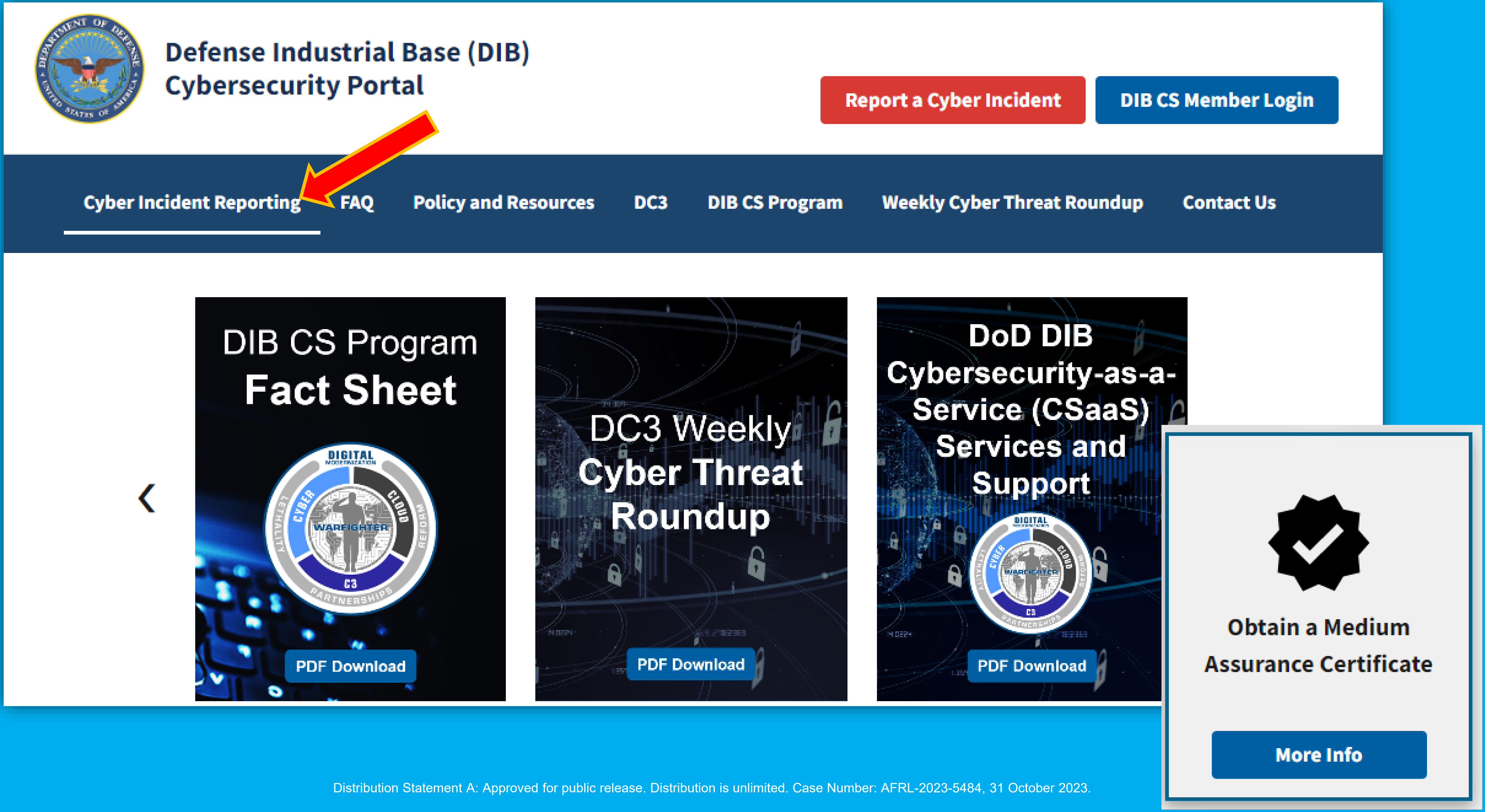
```
irror_mod = modifier_ob.
 mirror object to mirror
irror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

context):
ext.active_object is not
```

## AN OFFERING IN THE BLUE CYBER SERIES

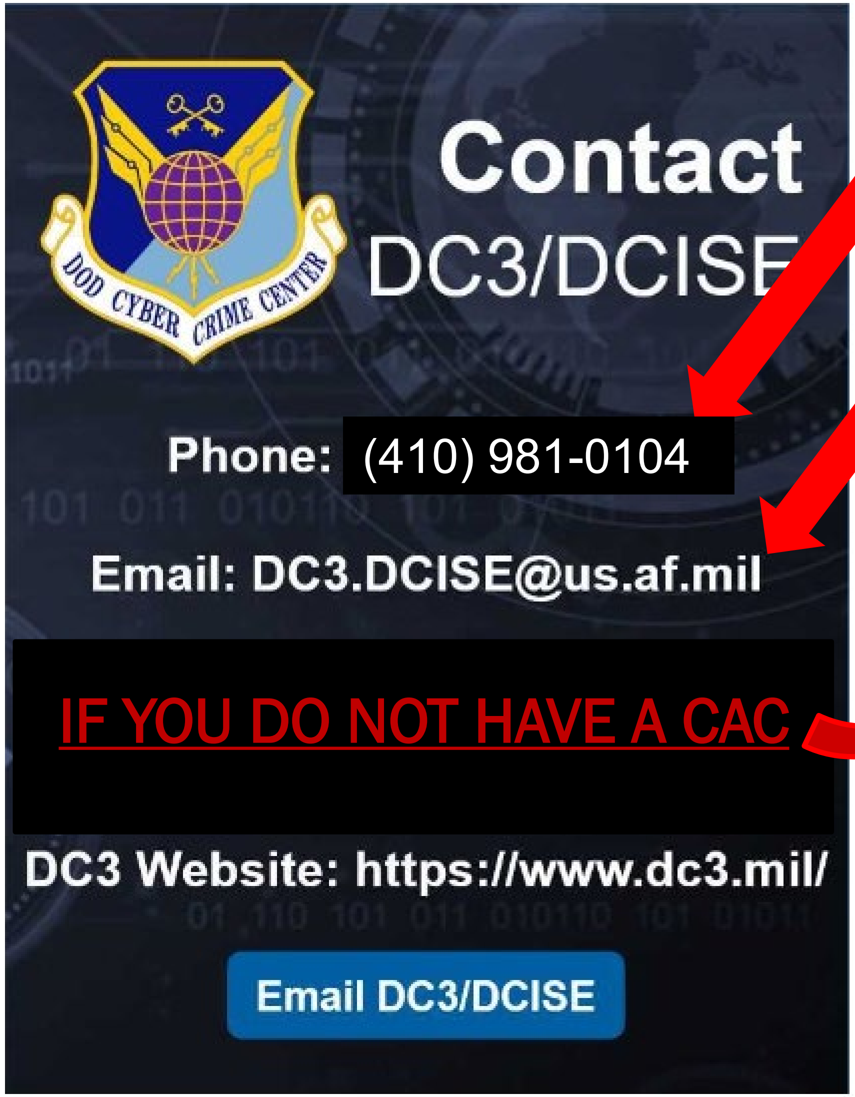
# If you are a DOD contractor, You must report cyber incidents to the DoD

https://dibnet.dod.mil/dibnet/

https://dibnet.dod.mil/dibnet/


Defense Industrial Base (DIB) Cybersecurity Portal
Report a Cyber Incident
DIB CS Member Login
Cyber Incident Reporting
FAQ
Policy and Resources
DC3
DIB CS Program
Weekly Cyber Threat Roundup
Contact Us
DIB CS Program Fact Sheet
PDF Download
DC3 Weekly Cyber Threat Roundup
PDF Download
DoD DIB Cybersecurity-as-a-Service (CSaaS) Services and Support
PDF Download
Obtain a Medium Assurance Certificate
More Info

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.



## Contact DC3/DCISE

Phone: (410) 981-0104

Email: DC3.DCISE@us.af.mil

IF YOU DO NOT HAVE A CAC

DC3 Website: https://www.dc3.mil/

Email DC3/DCISE

A DoD-Approved Medium Assurance Certificate is required to report a cyber incident via the portal.

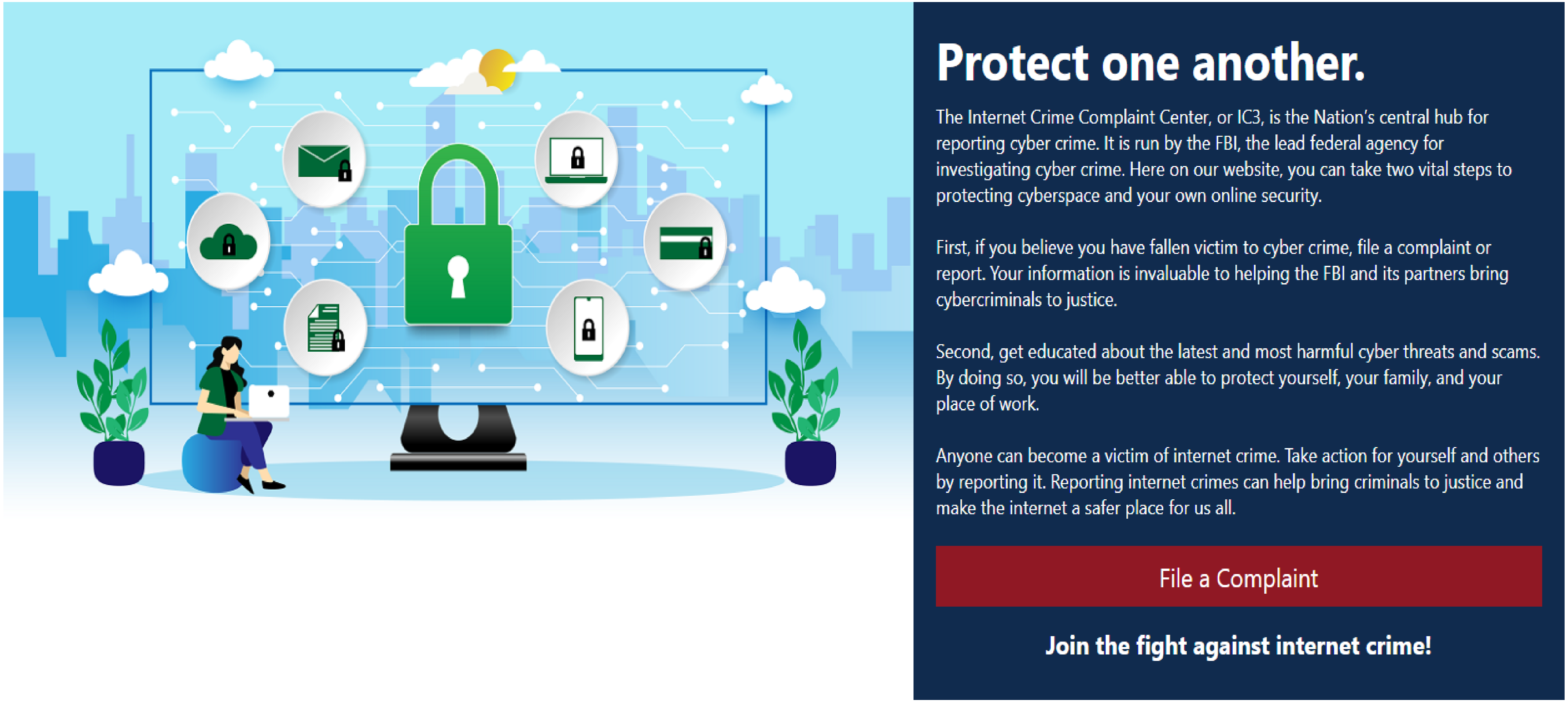
If you do not have a DoD-approved Medium Assurance Certificate

- please email DC3.DCISE@us.af.mil or
- call the DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) hotline at (410) 981-0104 for further assistance.

**This information repeats under the FAQs on the page**

# Internet Crime Complaint Center (IC3)

www.ic3.gov



## Protect one another.

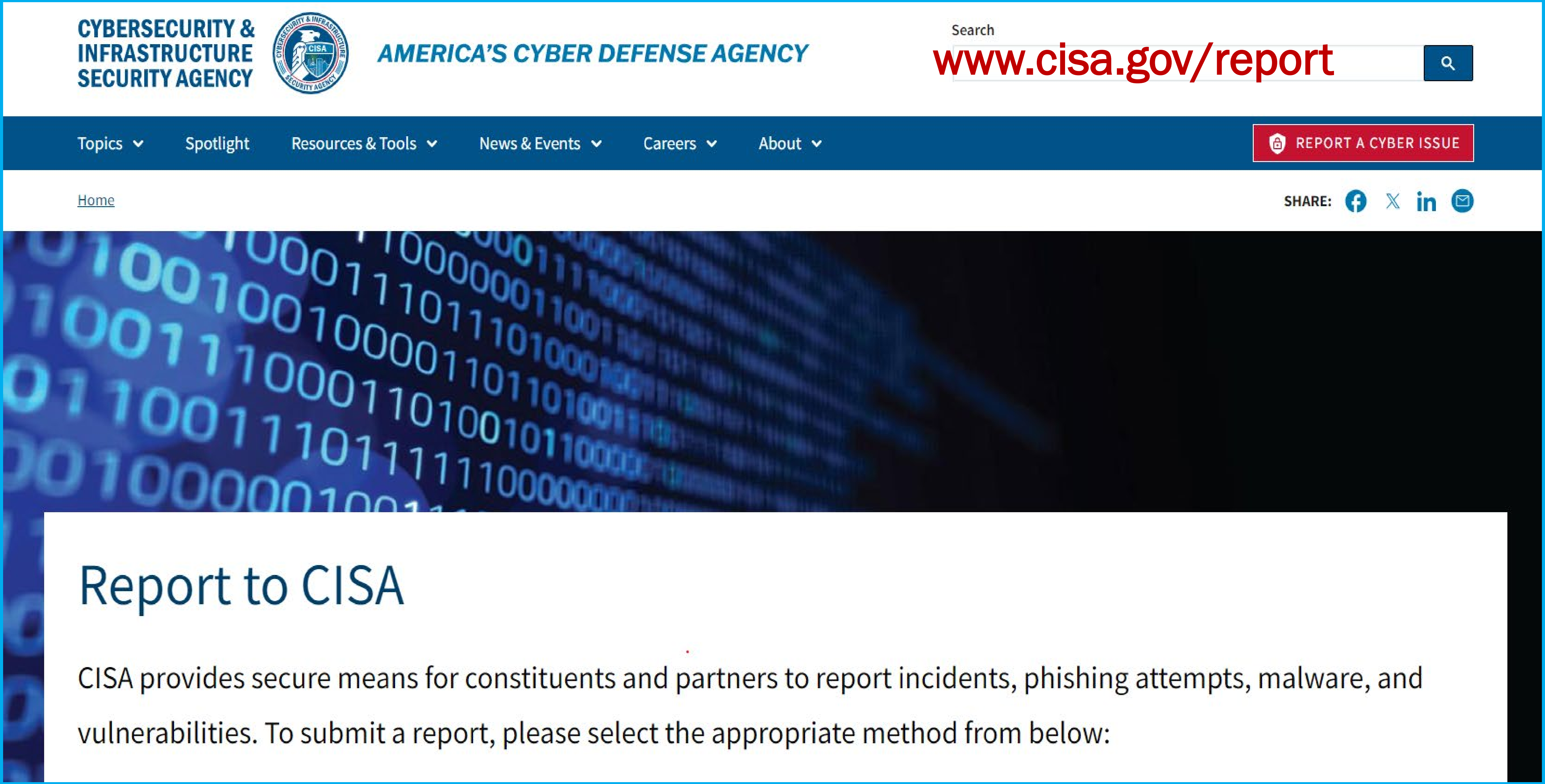
The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cyber crime. It is run by the FBI, the lead federal agency for investigating cyber crime. Here on our website, you can take two vital steps to protecting cyberspace and your own online security.

First, if you believe you have fallen victim to cyber crime, file a complaint or report. Your information is invaluable to helping the FBI and its partners bring cybercriminals to justice.

Second, get educated about the latest and most harmful cyber threats and scams. By doing so, you will be better able to protect yourself, your family, and your place of work.

Anyone can become a victim of internet crime. Take action for yourself and others by reporting it. Reporting internet crimes can help bring criminals to justice and make the internet a safer place for us all.

**Join the fight against internet crime!**

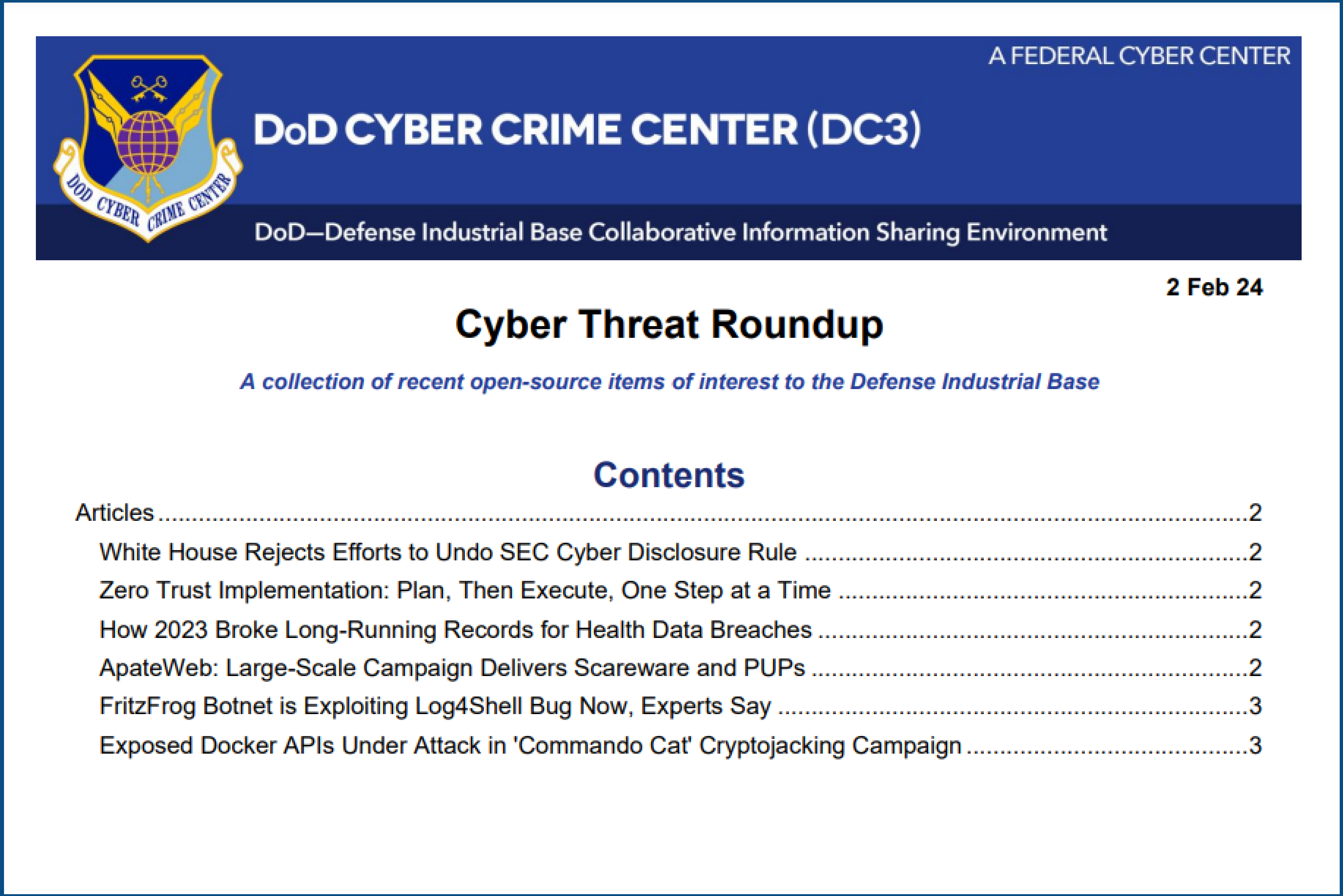


www.cisa.gov/report

# Report to CISA

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, please select the appropriate method from below:

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.



A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

**2 Feb 24**

# Cyber Threat Roundup

*A collection of recent open-source items of interest to the Defense Industrial Base*

## Contents

# DoD CYBER CRIME CENTER

**Contact Us:**

**Executive Support Staff**
410-981-1181
ExecutiveSupport@dc3.mil

**Cyber Forensics Laboratory (CFL)**
CFL@dc3.mil
National Center for Digital Forensics Academic Excellence:
CDFAE@dc3.mil

**Cyber Training Academy (CTA)**
Registrar: CTA.Registrar@dcita.edu

**DoD-DIB Collaborative Information Sharing Environment (DCISE)**
DCISE@dc3.mil

**Operations Enablement Directorate (OED)**
OED.Info@dc3.mil

**Technical Solutions Development (TSD)**
TSD@dc3.mil

**Vulnerability Disclosure Program (VDP)**
VDP-Questions@dc3.mil

**Public Affairs**
410-981-6610
INFO@dc3.mil

# DC3 CAPABILITIES FOR DoD REQUIREMENTS

## FORENSIC LAB SERVICES

DoD Center of Excellence for Digital and Multimedia (D/MM) forensics. DC3 Cyber Forensics Lab is an ISO 17025 accredited lab that performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD.

- Network Intrusions
- Malware/Reverse Engineering
- Enhancing Video and Voice Recordings
- Aircraft Mishap Data Recovery
- Damaged Media and Submerged Devices
- Mobile Device Encryption/Recovery
- DOMEX Forensic Partner

## DEFENSE INDUSTRY SHARING

DoD focal point for all cyber incident reporting affecting unclassified networks of Defense Industrial Base (DIB) contractors.

- Cyber Threat Information Sharing with DIB
- Cyber Incident and Malware Analysis
- Pilot Service Offerings (CSaaS)
- Mitigation and Remediation Strategies
- Partnership Exchanges
- Cyber Resiliency Analyses

## VULNERABILITY MANAGEMENT

DoD Vulnerability Disclosure Program Lead. Includes collaborative efforts with private-sector cybersecurity researchers to crowdsource the identification of vulnerabilities on DoD networks and systems.

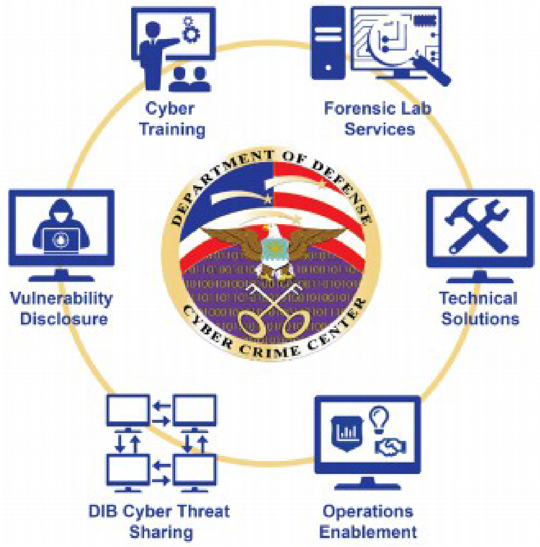
- Enhance Security of DoD Networks/Systems
- Independent Assessment of Cyber Defenses
- Improve Mission Assurance

## MISSION STATEMENT

Deliver superior digital and multimedia (D/MM) forensic services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the following DoD mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.

## VISION STATEMENT

Digital and multimedia technical and analytical center of excellence to improve DoD mission assurance and enhance warfighter capability.



## OPERATIONS ENABLEMENT

Amplifies the collective effects of DoD-wide law enforcement and counterintelligence investigations and operations by conducting expert technical analysis and all-source analysis and developing enhanced operational support capabilities.

- Collaborative Analytics with LE/CI/IC
- Focused All Source Intelligence
- Tailored Operational Production
- StormSystem Enhancement and Deployment
- CADO-IS Development and Integration

## CYBER TRAINING

Provides specialized in-residence and online cyber training (www.dcita.edu).

- Cyber Protection Team Training
- Network Defense
- Computer Technologies
- Basic and Advanced Forensic Examination
- Distance Learning/Webinar/Mobile Training
- Digital Forensics Certifications

## TECHNICAL SOLUTIONS

Tailored software and system solutions to support digital forensic examiners, DOMEX, and cyber intrusion analysis.

- Tool and Software Development
- Tool Test/Validation (Including GOTS/COTS)
- Counterintelligence Tool Repository
- Automated Malware Processing

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-2004, 25 Jun 2021.

# Any Questions?

- This briefing is not a substitute for reading the FARS/DFARS
- Resources and more modules like this are coming every day!
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions at https://www.safcn.af.mil/Contact-Us/