## WHAT TO REPORT

- All cyberthreats
- Aggressive port scanning outside normal network noise
- Advanced techniques / evasion techniques
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained storage of encrypted data
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltration
- Malicious codes or blended threats
- Unauthorized email traffic to foreign destinations
- Use of Department of Defense (DoD) account credentials by unauthorized parties
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or CUI
- Any cyberactivity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

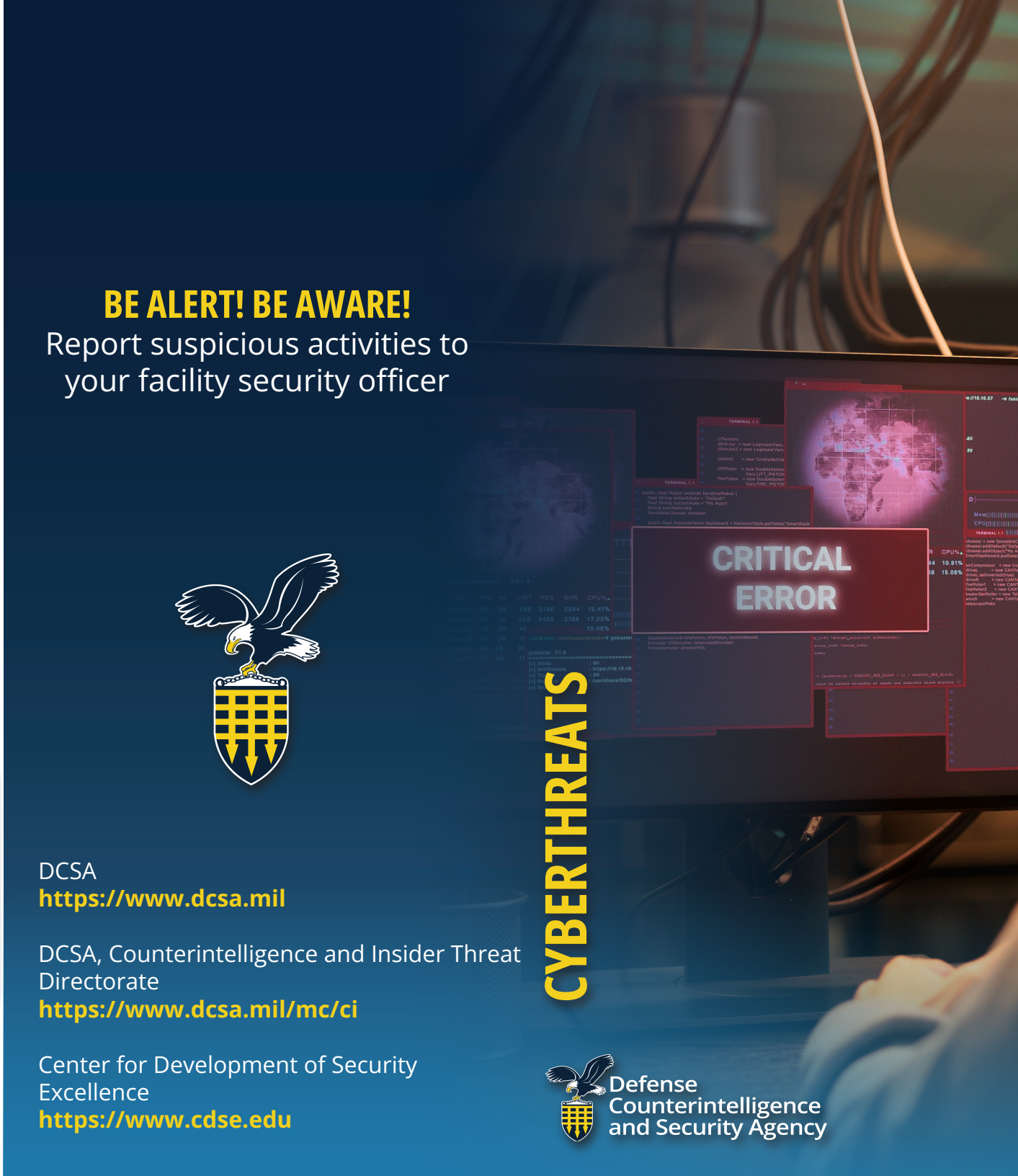
## REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

# BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer




# CYBERTHREATS

DCSA
**https://www.dcsa.mil**

DCSA, Counterintelligence and Insider Threat Directorate
**https://www.dcsa.mil/mc/ci**

Center for Development of Security Excellence
**https://www.cdse.edu**

Defense Counterintelligence and Security Agency

## WHAT ARE CYBER THREATS?

Our nation's cyberthreats have tools and tricks from a multitude of resources, including publicly available information on the Internet. This makes it difficult to differentiate between criminal and intelligence entities, exacerbated by the ease with which adversaries can obtain information about potential targets. We live in a world where the Internet of Things includes computers, cell phones, Smart TVs, Alexa, Ring, watches, satellite radio, refrigerators, and window shades.

## WHO IS BEING TARGETED?

**You**

Any individual, cleared or uncleared, regardless of job title or position, who can be used to gain access to an unsuspecting organization's network

**Your company**

Any organization or company, cleared or uncleared, with access to information coveted by our nation's adversaries

## WHAT IS BEING TARGETED?

- International Traffic in Arms (ITAR), export-controlled and critical technology, and controlled unclassified information (CUI)
- Research and development
- Company unclassified networks (internal and external), partner and community portals, commonly accessed websites, and unclassified search history
- Proprietary information
- Administrative and user credentials
- Patch update sequences/patterns

Foreign intelligence entities seek aggregates of CUI or proprietary documents which paint a classified picture.

## HOW ARE YOU BEING TARGETED?

- **Information Gathering:** Harvesting information
- **Targeting:** Coupling exploit with delivery methods
- **Delivery:** Infecting the target commonly using email, website hijacking, and removable media
- **Exploitation:** Exploiting a vulnerability on a system to execute code
- **Installation:** Malware providing persistence on targeted network
- **Command and Control:** Remote access computers, networks, or software/firmware
- **Actions on the Objective:** Access targeted information, data, and technology

### HOW ARE YOU VULNERABLE?

- Publicly available information
- Contract information
- Company websites with technical/program data
- Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or uncleared companies
- Employee association with companies or technologies made public through scientific journals, academia, social networking sites such as Facebook and LinkedIn, etc.

### PERSISTENT AND EMERGING CYBER THREATS

- Deepfakes: Creating fake images, sounds, and videos to fool the viewer
- Poisoning Attacks: Malicious injection into artificial intelligence program while it is learning
- Ransomware: New tactics, techniques, and procedures to exfiltrate data and release to the public
- Supply chain vulnerabilities
- Unsecure security products
- Malicious code injection
- Botnets
- Brute force
- Social network sites
- Credential harvesting

## COUNTERMEASURES

- Training
- Using complex passwords
- Educating employees on social networking and email targeting; phishing email signs and reporting
- Defense in depth
- Technical defenses
- Patch management
- Monitoring suspicious network activity
- Open lines of communication among facility security, counterintelligence (CI), and network defense personnel
- Having a failsafe relating to system administrators. One person should not have all of the "Keys to the Kingdom"
- Proper configuration–audit and automate secure configuration

**"The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million."**

Cost of a Data Breach Report 2023, IBM Security