REPORTABLE TO DCSA

- All of the persistent and emerging cyber threats
- Aggressive port scanning outside normal network noise
- Advanced techniques and/or advanced 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, such as through social networking sites
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltration
- Malicious codes or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Unauthorized email traffic to foreign destinations
- Use of Department of Defense (DOD) account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or CUI
- Any cyber activity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

REPORTING REQUIREMENTS

National Industrial Security Program Operating Manual (NISPOM) requires the reporting of suspicious contacts, behaviors, and activities.

If you suspect you or your company has been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting CI threats and mitigating risks. Reporting allows us to share and address risks together.

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence Directorate
https://www.dcsa.mil/mc/ci

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

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

CYBER THREATS

DEFENSE COUNTERINTELLIGENCE
AND SECURITY AGENCY

CYBER THREATS

Our nation's cyber adversaries have a plethora of tools and tricks from a multitude of resources, including publicly available information on the Internet. This access makes it increasingly difficult to differentiate between a criminal and an intelligence entity. This is exacerbated by the ease with which our adversaries can obtain information about potential targets. We live in a world where Internet of Things includes everything from computers, cell phones, Smart TVs, Alexa, Ring, watches, and even satellite radio, to refrigerators and window shades. Combine the two and the compounding problem becomes extreme and daunting. Sometimes the best solution is to go back to the basics and educate the workforce.

WHO ARE THEY TARGETING?

- Any organization or company, cleared or uncleared, with access to information coveted by our nation's adversaries
- Any individual, cleared or uncleared, regardless of job title or position, who can be used to gain access to an unsuspecting organization's network
- YOU and YOUR company

WHY ARE YOU A TARGET?

- Publicly available information (identifies people with placement and access)
- Contract information (bid, proposal, award, or strategies)
- Company website 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, public speaking engagements, and social networking sites such as Facebook and LinkedIn, etc

WHAT ARE THEY TARGETING?

- International Traffic in Arms, 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 (business strategy, financial, human resource, and product data)
- Administrative and user credentials (usernames, passwords, tokens, Virtual Private Network [VPN] data, etc.)
- Patch update sequences/patterns, i.e., is the company using a set date to update its systems?

Foreign intelligence entities seek the aggregate of CUI or proprietary documents which could paint a classified picture

HOW DO THEY COMPROMISE NETWORKS, SYSTEMS, AND TECHNICAL DATA?

- **Information Gathering**: Harvesting information (names, emails, relationships, publicly available vulnerabilities, and social engineering, etc.)
- **Targeting**: Coupling exploit with delivery method, such as email
- **Delivery**: Infecting the target commonly using email, website hijacking, and removable media (through insiders)
- **Exploitation**: Exploiting a vulnerability on a system to execute code
- **Installation**: Malware installation likely providing persistence on targeted network
- **Command and Control**: Communication avenue for adversary to remotely access a computer, network, or software/firmware
- **Actions on the Objective**: With access, the adversary can now access the targeted information, data, and technology

POTENTIAL COUNTERMEASURES

- Training! Training! Training!
- Using complex passwords
- Educating employees on social networking and email targeting; phishing email signs and reporting
- Defense in depth
- Technical defenses (firewalls, Domain Name System proxy, Internet content filtering, etc.)
- Patch management
- Monitoring suspicious network activity (even third-party vendors). Your network and your proprietary data are at stake
- Opening lines of communication among facility security, counterintelligence (CI), and network defense personnel–a one-sided defense is a failed defense
- 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

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 procedure to exfiltrate data and release to the public
- Supply Chain vulnerabilities
- Insecure Security Products (vulnerabilities)
- Malicious Code Injection
- Botnets
- Brute Force
- Social network sites
- Credential Harvesting