Reporting Definitions

Cyber Espionage: The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense using cyberspace with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

What to Report

- **Advanced techniques** and/or **advance evasion techniques**, which imply a **sophisticated adversary**

- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading

- Pre-intrusion aggressive port scanning

- 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. automated information systems

- Tampering with or introducing unauthorized elements into information systems

- Unexplained user accounts, administrator accounts, and expansion of network privileges

- Data exfiltrated to unauthorized domains affecting classified information, systems or cleared individuals

- 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 DoD account credentials by unauthorized parties

- Unexplained storage of encrypted data

- Network spillage incidents or information compromise

- Unauthorized transmissions of classified or controlled unclassified information

- Any cyber activity linked to suspicious indicators provided by the Defense Security Service (DSS), or by any other cyber centers and government agencies

Reportable activities are not just limited to those activities that occur on classified information sytems. Industrial Security Letter 2013-05 (which clarifies National Industrial Security Program Manual (NISPOM) paragraph 1-301) instructs cleared U.S. companies s that they must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on unclassified information systems.

NISPOM paragraph 1-302b reminds cleared U.S. companies that they "shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.

Be Alert! Be Aware!

Report suspicious activity to your local security official.

Cyber Threats

Defense Security Service
Counterintelligence Directorate
www.dss.mil

CYBER THREATS

Why Are You a Target?

- Publicly available information helps foreign intelligence entities identify people with placement and access.
  - Contract information (bid, proposal, award or strategies)
  - Company website with technical and program information
  - Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or non-cleared companies
- Employee association with companies or technologies made public through scientific journals, academia, public speaking engagements, social networking sites, etc.

What Do They Target?

- Company unclassified networks (internal and extranets), partner and community portals, and commonly accessed websites
- Proprietary information (business strategy, financial, human resource, email, and product data)
- Export controlled technology
- Administrative and user credentials (usernames, passwords, tokens, etc.)
- Foreign intelligence entities seek the aggregate of unclassified or proprietary documents that could paint a classified picture

How Do They Compromise Networks, Systems, and Technical Data?

Reconnaissance: Research phase used to identify and select targets by browsing websites to obtain names, emails, business and social

relationships, and technical information.

Weaponization: The foreign intelligence entities assemble the payload and wrapper, such as coupling a remote access exploit with a prepared spear-phishing email.

Delivery: The foreign intelligence entity infects the target, most commonly using email, website hijacking, or removable media (through insiders).

Exploitation: Successful compromise of targeted vulnerability to allow malicious code to be run.

Installation: Executed malicious code inserts malware, such as a Remote Access Trojan or opens a backdoor connection to the target system – may allow for persistence.

Command and Control (C2): The malware will communicate to a controller server to send or receive instructions from the foreign intelligence entity.

Actions on the Objective: After completing the above actions, the foreign intelligence entity can fulfill their requirements. Intelligence requirements can range from exfiltration, using the system as a strategic position to compromise additional systems within the targeted network (hop-point), or sabotaging the system and network.

Countering Threats to Networks and Cleared Individuals

Employees

- **Everyone is a potential target**
- Use complex passwords, change them regularly, and don't reuse
- **Be wary when connecting with unknown individuals on social networking sites**
- Spear-phishing can happen on any account, including personal email accounts
  - Do not open emails, attachments, or click links from unfamiliar sources, even if they look official

IT Department & Management

- Train all personnel on:
  - Spotting a spear phishing, phishing, or whaling email attempt
  - Social networking site connections
  - Proper cyber security procedures and concerns
- Implement defense-in-depth: a layered defense strategy that includes technical, organizational, and operational controls
- Implement technical defenses: firewalls, intrusion detection systems, internet content filtering, and a DNS proxy
- Update your anti-virus software daily and download vender security patches for all software
- Do not use manufacturers' default passwords on software or hardware
- Monitor, log, analyze and report attempted and successful intrusions to your systems and networks – even unsuccessful intrusions present a counterintelligence value!
- Maintain open communication between company counterintelligence and network defense personnel. Defense only is not a comprehensive strategy