DETECT AND REPORT CYBERSECURITY INCIDENTS

Cybersecurity Incident Guide, Version 2.0

1 READINESS

Every employee is a potential target for the Department's adversaries, and everyone is responsible for protecting the Department's integrity—as well as one's own personal identity. Properly reporting cybersecurity incidents is critical.

Many cybersecurity incidents originate as attacks on a DHS employee's e-mail. Carefully evaluate all e-mails:

FIRST, decide if e-mails or attachments are suspect. Always think before you click on links, considering how activating questionable sources may impact the Department and yourself.

SECOND, when you suspect a compromise in information security, use the Cybersecurity Incident Checklist (Step 2) to gather necessary information.

THIRD, report the incident to your Security Operation Center (SOC) or your IT Service Desk (Step 3).

Always forward suspicious e-mails as an attachment to:

dhsspam@dhs.gov

Homeland Security

Office of the Chief Information Officer
Office of the Chief Information Security Officer

2 CYBERSECURITY INCIDENT CHECKLIST

WHAT IS THE INCIDENT TYPE?

- ☐ Denial of service
- ☐ Unauthorized access
- ☐ Hardware loss
- ☐ Social engineering
- ☐ FOUO data spill
- ☐ Malicious code
- ☐ Inappropriate use
- ☐ Website defaced
- ☐ Spearphishing
- ☐ Classified data spill

HOW WAS IT INITIALLY DISCOVERED?

- ☐ Popup windows
- ☐ SOC-issued alert
- ☐ Public media
- ☐ User suspicion
- ☐ User notification
- ☐ Social media

WHAT ARE THE INDICATORS/CHARACTERISTICS?

- ☐ Slower than normal
- ☐ Hard drive full
- ☐ Foreign/unfamiliar e-mail addresses
- ☐ Suspicious content
- ☐ Cursor moving on its own
- ☐ Increased network traffic
- ☐ Data corrupted
- ☐ Data/site unavailable
- ☐ People received e-mail from my address that I didn't send
- ☐ Other _____

HOW DOES THIS IMPACT YOUR MISSION?

- ☐ Unable to perform mission
- ☐ Data unavailable
- ☐ Able to continue at reduced capability
- ☐ No impact
- ☐ Public relations
- ☐ Service unavailable
- ☐ Minimal impact
- ☐ Other _____

WHAT HAS BEEN DONE SO FAR?

- ☐ Secured classified information
- ☐ Ran antivirus
- ☐ Patched system
- ☐ Deleted e-mail*
- ☐ Contacted another authority
- ☐ Changed password
- ☐ Rebooted system*
- ☐ Other _____

*Do not delete or reboot anything unless directed because SOC forensic investigators may need to collect evidence.

DEFINITIONS

classified data spill - release of classified data on unclassified information systems or to an information system with a lower level of classification

FOUO data spill - the transfer of For Official Use Only (FOUO) information onto an information security system not accredited (i.e., unauthorized) for appropriate security level, such as a home computer

malicious code - unwanted technology installed without a user's consent that is intended to perform unauthorized processes to steal data, damage or disable computers and computer systems, or compromise the confidentiality, integrity, and availability of an information system; malicious software includes viruses and worms, Trojan horses, keystroke loggers, spyware, and other code that vandalizes or steals sensitive or electronic data, including some adware

social engineering - an attempt to trick someone into revealing protected information (e.g., a password) that can be used to attack an enterprise

spearphishing - intentionally attempting to steal data from specifically targeted individuals by sending e-mails that appear legitimate but contain links or attachments that enable malicious executable software or attempt to obtain personal credentials, PII, or Sensitive PII

REMEMBER: CYBERSECURITY IS OUR SHARED RESPONSIBILITY

See DHS 4300A Sensitive Systems Handbook – Attachment F for additional guidance.

3 CYBERSECURITY EMERGENCY CONTACTS

CBP	703-921-6507 cbp.csirc@dhs.gov
FEMA	540-542-4762 fema-soc@fema.dhs.gov
FLETC	912-554-4444 fletcsoc@dhs.gov
HSDN	877-457-4736
HQ	800-250-7911 itsupport@hq.dhs.gov
ICE	888-347-7762 https://servicedesk.ice.dhs.gov/servicedesk/
OIG	202-254-4301 oig.helpdesk@dhs.gov
S&T	st_incident_reporting@hq.dhs.gov
TSA	877-242-4533 tsa-csirt@tsa.dhs.gov
USCG	866-424-2478, 703-313-5678 tis-sg-cgcirt@uscg.mil
USCIS	888-220-5228 uscisservicedesk@dhs.gov
USSS	202-406-5653 usss-soc@usss.dhs.gov

If your Component is not listed:

DHS SECURITY OPERATIONS CENTER (SOC)

877-DHS1NET (877-347-1638)
dhs.soc@dhs.gov
https://eoconline.dhs.gov