



CYBER INCIDENT REPORTING AID



OPSEC – DO NOT DISCUSS/TRANSMIT SENSITIVE INFORMATION VIA NON-SECURE MEANS

CLASSIFIED SPILLAGE INCIDENT REPORTING PROCEDURES FOR USERS

A Classified Spillage Incident is defined as information classified at a higher level appearing on or connected to a system classified at a level lower than the information.

- STEP 1** **STOP!** Disconnect network access. Discontinue use of system / do not shut down!
- STEP 2** **SECURE** affected systems / equipment! Ensure they remain under positive control of authorized personnel.
- STEP 3** **REPORT** incident immediately! DO NOT discuss classified details but report incident through Unit Cybersecurity Liaison (CSL) to Unit Security Manager (USM) and Comm Focal Point (CFP) immediately.

SUSPECTED COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

- STEP 1** **STOP!** Disconnect the network access. Discontinue use of system!
- STEP 2** **DROP** mouse and leave system on!
- STEP 3** **ROLL** out the notes! Record notes on the reverse side.
- STEP 4** **REPORT** it immediately! Contact your CSL to contact the Comm Focal Point (CFP) immediately!

NOTE: USE THIS CARD AS A REFERENCE WHEN REPORTING TO YOUR CSL OR CFP.

UNAUTHORIZED REMOVABLE MEDIA ON DOD SYSTEMS

Removable storage primarily includes flash media devices (such as memory sticks, thumb drives, and camera memory cards) and external hard disk drives and are not authorized on the network without prior approval.

- STEP 1** **NOTIFY** your unit CSL if you find unauthorized removable media!
- STEP 2** **SECURE** the device until give further instruction! Do not connect it to any other systems.
- STEP 3** **VIOLATORS** will have their network accounts suspended and must re-accomplish their annual DoD IAA CyberAwareness Challenge training plus their unit CC could impose additional administrative punishments!

AUTHORIZED REMOVABLE MEDIA ON DOD SYSTEMS

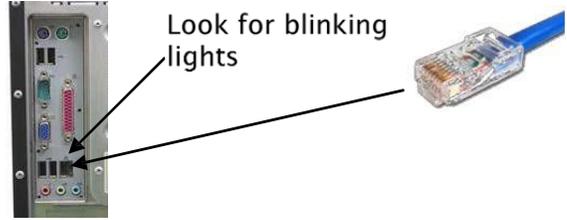
If a Mission Critical need for removable media (including flash media) exists, waivers are available!

- STEP 1** **CONTACT** your unit CSL!
- Consult with your unit CSL for further guidance using removable media on DOD systems.

35FWVA 33-1 2 October 2015 (Per AFI33-200)
Supersedes: 35FWVA 33-1, 15 July 2014 OPR: 35 FW WCO (35 CS/SCXSI)
ACCESSIBILITY: Publication and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering
RELEASABILITY: There are no releasability restrictions on this publication

DEPLOY/POST THIS AID NEAR CYBERSPACE SYSTEMS

To disconnect computer from the network:



Locate the LAN Jack on rear of computer. Depress tab on LAN cable connector and pull gently
DO NOT Log Off!
DO NOT Power Down!
DO NOT Reboot!

Your Unit Cybersecurity Liaison (CSL) is:

Unit CSL Phone: _____

Contact the CFP and USM!

CFP: 226-2666 USM: _____

For additional assistance contact:
35 FW Wing Cybersecurity Office
226-2001 / 35fw.ia@us.af.mil

Do Not Discuss Classified info on U nclassified phone. Use STE/VoSIP

Notes:

Use this area to record any known details of incident (Control notes at highest classification of information)

1. Exact File Name including extension of file contaminated with virus or classified info as applicable:

2. Subject of the e-mail containing virus or classified info as applicable:

3. Time and date received:

4. Who sent the file or e-mail:

5. List of people who received the file or e-mail as applicable:

6. Was the file or email forwarded beyond original recipients? If so to whom?

Additional Information:
