NETWORK INCIDENT REPORTING AID
OPSEC – *DO NOT DISCUSS/TRANSMIT SENSITIVE INFORMATION OVER UNAUTHORIZED SYSTEMS*

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	STOP! DISCONNECT THE LAN CABLE. *Discontinue use* of the system.
STEP 2	LEAVE THE SYSTEM POWERED UP. **DO NOT** click on any prompts, close any windows, or shut down the system.
STEP 3	REPORT IT IMMEDIATELY! Contact your section Cyber Security Liaison (CSL). If an CSL is unavailable contact the Communications Focal Point (CFP). (See List on Reverse Side)
STEP 4	If a message appears on the monitor of the affected system – WRITE IT DOWN!
STEP 5	WRITE DOWN ALL ACTIONS that occurred during the suspected virus attack. (i.e. Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked/unsecured files; etc.)
STEP 6	Answer questions on reverse side of this form.

NOTE: When reporting a suspected virus to your CSL or the CFP ensure that you answer questions on reverse side of this form and provide the technician with your name and number.

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network.

STEP 1	***STOP!*** **DISCONNECT THE LAN CABLE** *Discontinue use* of the system and **DO NOT** print the classified message.
STEP 2	**REPORT INCIDENT IMMEDIATELY TO UNIT SECURITY MANAGER. DO NOT** discuss details of the CMI over unsecure lines. Call an IAO, Supervisor, or the Communications Focal Point (CFP).
STEP 3	**SECURE** affected system(s) / printer(s), area / room and wait for CFP personnel to assist. Limit the exposure of the CMI. **DO NOT** leave the system until relieved by IAO or CFP Personnel.
STEP 4	Answer questions on reverse side of this form.

INFOCON LEVELS

INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer/telecommunication systems and networks. INFOCON levels are as follows:

INFOCON 5: Routine NetOps: Normal readiness of information systems and networks that can be sustained indefinitely.

INFOCON 4: Increased Vigilance: In preparation for operations or exercises, with a limited impact to the end user.

INFOCON 3: Enhanced Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end user is minor.

INFOCON 2: Greater Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end user could be significant.

INFOCON 1: Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end users.

USAFAVA17-201, 2 Jul 2017
PER AFMAN 17-1301
OPR: HQ USAFA/A6, Releasability: USAFA Personnel Only
Certified Current 18 June 2025

CyberSecurity
Is everyone's business

10 CS IT Service Desk

Bldg: 2354
Fairchild
Hall
USAF Academy,
CO 80840

333-4357

MY CyberSecurity Liason (CSL) IS:

What to tell CSL and/or CFP

Exact File Name including extension:

Subject of the email:

Who sent the file or email:

List of people the file or email was sent to:

Was the file or email forwarded: if so to whom?

DEPLOY/POST THIS AID NEAR COMPUTER WORKSTATIONS