

**NETWORK INCIDENT REPORTING AID
OPSEC DO NOT DISCUSS/TRANSMIT CRITICAL
INFORMATION VIA NON-SECURE MEANS**

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS	
STEP 1	STOP! DISCONNECT THE LAN CABLE. Discontinue Use
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel <u>should not</u> click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system - WRITE IT DOWN!
STEP 4	WRITE DOWN ALL ACTIONS that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, CD ROM, etc..?)
STEP 5	REPORT IT IMMEDIATELY! Contact Communications Focal Point (CFP) Helpdesk at 294-2666 and/or your section's Client Support Technician(CST).
STEP 6	Mark the Computer "Do Not Use!" Turn this card over to display warning on Keyboard/Monitor

NOTE: When reporting a suspected virus to the CFP and/or a CST ensure that you give the following information to the technician:

- Event Date and Time
- Report Date and Time
- Your name, telephone number, bldg, and organization
- Name of your CST (if applicable)
- Location of infected system(s)

**CLASSIFIED MESSAGE INCIDENT (CMI)
REPORTING PROCEDURES FOR USERS**

A CMI occurs when classified information is transmitted via electronic media or stored on information systems not cleared for the level of data in question

STEP 1	STOP! DISCONNECT THE LAN CABLE of the affected computer system(s) and/or printer(s)
STEP 2	Do not delete the classified information. SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, Supervisor, CST (if applicable) and the CFP at 294-2666. Note: You may only say "I'd like to report a possible CMI" via non-secure means and wait for further assistance.
STEP 4	Mark the Computer "Do Not Use!" Turn this card over to display warning on Keyboard/Monitor

INFOCON LEVELS

The INFOCON system is a series of prescribed and standardized actions to maintain or reestablish the confidence-level of networks under a commander's authority.

INFOCON 5: Information networks are operational. Normal readiness of information systems and networks that can be sustained indefinitely.

INFOCON 4: Limited risk to ongoing military operations. Operational impact of degradation or loss of information and information systems is LOW to MEDIUM. Impact to end-users is negligible.

INFOCON 3: Risk to mission accomplishment is moderate. Requires vigilance to maintain network security. Impact to end-users is minor.

INFOCON 2: Risk of mission failure is HIGH. Operational impact of degradation or loss of information and information systems is MEDIUM to HIGH. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

INFOCON 1: Risk to mission operations is EXTREME. Operational impact of degradation or loss of information and information systems is HIGH. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

WARNING!

Do Not Use Computer

**DISPLAY/POST
THIS AID ON
KEYBOARD/MONITOR**