

Fort Gordon NEC
NETWORK INCIDENT REPORTING AID
OPSEC: DO NOT DISCUSS/TRANSMIT
CRITICAL INFORMATION VIA NON-SECURE MEANS



INFORMATION ASSURANCE INCIDENT REPORTING PROCEDURES FOR USERS	
STEP 1	STOP! Discontinue Use, mark computer “Do Not Use” and unplug the network cable from the computer .
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel should not click on any prompts or close any windows or shut the system down.
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 attack. (Did the virus come from an e-mail attachment etc.)
STEP 5	REPORT IT IMMEDIATELY! Contact your IMO and/or IASO. If unavailable contact the G6 Technical Reference Desk personnel.

Thumb drive non-usage/USB hard drive usage

“THUMB DRIVES of ANY TYPE ARE NOT AUTHORIZED for use on unclassified & classified government information systems”

“ONLY USE APPROVED/RECOMMENDED USB external hard drives on information systems “

“Ensure external hard drives and Information systems are marked/labeled with appropriate classification sticker”

Ensure external drives are completely scanned prior to every use, **formatted to NTFS**, and are government procured and issued.

NOTE: When reporting a suspected IA incident to your IMO, IASO, IAM and/or the NEC Help Desk ensure that you give the following information to the technician:

- Event Date and Time - Name of your IMO
- Report Date and Time - Location of infected system (s)
- Your name, telephone number, and staff section.
- Computer Name

When to sign and/or encrypt E-mail

PKI Digital Encryption – Use DoD PKI certificates to encrypt e-mails containing For Official Use Only, Privacy Act and Personally Identifiable Information; individually identifiable health information; and other sensitive, but unclassified information.

PKI Digital Signature - Use digital signatures whenever it is necessary for the recipient to be assured of the sender’s identity, have confidence the message has not been modified or when non-repudiation is required.

DATA COMPROMISE/SPILLAGE REPORTING PROCEDURES FOR USERS

Data Compromise/Spillage is the unintentional release of secure information to an insecure environment.

Protecting SI/PII

Ensure UNCLASSIFIED systems that store, process and/or transmit SI or PII are protected with an approved Data-at-Rest solution.

STEP 1	STOP! Discontinue Use, mark computer “Do Not Use”
STEP 2	SECURE affected system (s) and/or printers.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, IASO, IMO and/or the Helpdesk. Note: you may only say, “I’d like to report a possible Data Compromise/Spillage” via non-secure means and wait for the NEC IA Tech personnel to assist.

Report lost/stolen/compromised SI/PII immediately to the IAM and within one hour of discovery to US-CERT <https://forms.us-cert.gov/report/> and 24 hours of discovery to <https://www.rmda.army.mil/privacy/foia-incidentreport1.asp>.

DISPLAY THIS AID NEAR COMPUTER INFORMATION

STAFF SECTION IA/SECURITY PERSONNEL

Section IMO: _____

Section IA Security Officer (IASO): _____

IA Manager (IAM): : 791-0042 and after duty hours: IOC 791-9748

Section Security Manager: _____

