# 6 AIR REFUELING WING
# COMPUTER QUICK RESPONSE AID

*(Revised 12 April 2022)*

## VIRUS/NETWORK ATTACK SYMPTOMS

- **Request to Provide, Reset, or Change Password**
- **Notification of Logon Attempts by Unknown User**
- **Unexplained Inability to Log On, New Files/File Names**
- **Inability To save Files**
- **Unexplained Modifications/Deletion of Data**
- **Unfamiliar Error Messages**
- **Sudden Lack of Hard Drive Space**
- **Computer Continually Restarts**
- **Out-Of-Memory Error Messages (in a PC with Sufficient RAM)**

## COMPUTER VIRUS/MALWARE REPORTING PROCEDURES FOR USERS

| | |
|---|---|
| **STEP 1** | **STOP. DISCONNECT THE LAN CABLE.** Discontinue Use  |
| **STEP 2** | **LEAVE THE SYSTEM POWERED UP.** **DO NOT** click on any prompts, close any windows, or shut down the system. |
| **STEP 3** | **WRITE DOWN** any message that appears on the monitor of the affected system. |
| **STEP 4** | **WRITE DOWN ALL DETAILS** that occurred during the suspected virus/malware. (Did the virus/malware come from an e-mail attachment, CD or DVD, diskette, etc.?) |
| **STEP 5** | **REPORT IMMEDIATELY.** Contact your unit Cyber Liaison (CL) and report the incident. |

When reporting a suspected virus/malware to your CL ensure that you give the following information to the technician:

- Your name, telephone number, bldg, and org
- Name of your CLs
- Name and location of infected system(s)
- Event Date and Time
- Report Date and Time

Ref: NIST SP 800-83r1

## RESPONSE TO NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI) OR CLASSIFIED FILE INCIDENT (CFI) AND REPORTING PROCEDURES FOR USERS

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

| | |
|---|---|
| **STEP 1** | **STOP! DISCONNECT THE LAN CABLE** of the affected computer system(s) and/or printer(s).  |
| **STEP 2** | **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 secure telephone or in person to your unit CL.<br>*** Do not** report or discuss incident over **unsecure** line. You may only say, **"I am notifying you of a possible NDCI"** via non-secure means and wait for security personnel to assist. |

## ADDITIONAL NDCI and CFI INFO

For all Collateral Information Incidents (Confidential, Secret, and Top Secret) notify Wing Information Protection office and CyOC.

For Sensitive Compartmented Information incidents (SCI at any classification level) Notify the Senior Intelligence Officer (SIO), MAJCOM CISO, or the Air Force Intelligence Community (AF IC) Security Coordination Center (SCC).

For Special Access Program/Special Access Required (SAP/SAR at any classification level) notify the Program Security Officer (PSO) or Government SAP Security Officer (GSSO).

Ref: TASKORD 2019-007-001A

## PHISHING E-MAILS

| | |
|---|---|
| **STEP 1** | If you receive a possible phishing e-mail, do not provide any personal information or click on any links. |
| **STEP 2** | Forward the e-mail as an attachment to 33NWS.MAN@us.af.mil |
| **STEP 3** | Right click on email, click on Junk Email, then Add Sender to Blocked Senders List. Delete all Junk Email from the Junk Email Box |

## UTILIZING CUI TO PROTECT PII EMAILS

1. Put "CUI//" in the subject line of the email.
2. The first line of the email should be "This electronic transmission may contain CONTROLLED UNCLASSIFIED INFORMATION (CUI) and must be protected"
3. Digitally sign the email
4. Encrypt the email before sending

For more information on PII, please contact the base PII manager at **6cs.scxkrp@us.af.mil** or 813-828-5355

Ref: DODI 5200.48

## SPACE REQUIRED FROM CLASSIFIED SYSTEMS

| Device/Equipment Type | Distance | Distance in inches/feet |
|---|---|---|
| **NIPRNet Equipment** | **0.5 meters** | **20 inches** |
| **NIPRNet Line** | **0.5 meters** | **20 inches** |
| **Cell Phones** | **3 meters** | **Approximately 10 feet** |
| **LMR Hand-Held Radios** | **2 meters** | **Approximately 6.5 feet** |
| **Radio Transceivers/ Wi-Fi** | **3 meters** | **Approximately 10 feet** |

Ref: AFSSI 7702, CNSSAM TEMPEST/1-13 (Follow local Tempest Guidance)

## GOOD CYBERSECURITY TIPS

- Do not Leave your Common Access Card (CAC) or SIPR Tokens unattended
- Do not share CAC's, Tokens and/or Credentials
- Restart your computer at the end of the day for updates to take place.
- Check Software updates
  - ✓ Type "Software Center" into the Cortana Search box
  - ✓ Software Center opens click updates on the left side
  - ✓ If items populate, click "Install All"

## POINTS OF CONTACT

| | |
|---|---|
| Unit Security Manager (USM) | Name:<br>Ext: |
| Unit CL | Name:<br>Ext: |
| WCO | Name: **Wing Cybersecurity Office**<br>Ext: **813-828-4149**<br>Email: **6arw.cybersecurity@us.af.mil** |

## DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION

MACDILLAFBVA 17-4, 10 May 2023
SUPERSEDES MACDILLAFBVA 33-4, 12 Oct 2021
OPR: 6 CS/SCXS

Prescribed by: MPTO 00-33B-5007
RELEASABILITY: There are no releasability restrictions on this publication.