Appendix F – WPAFB End User Incident Quick Response Guide / Reporting Aid

COMPUTER EMERGENCY QUICK RESPONSE AID

VIRUS/NETWORK ATTACK SYMPTOMS

- Request To Provide, Reset, Or Change Password
- E-mail From Unfamiliar Source
- Notification Of Logon Attempts By Unknown User
- Unexplained Inability To Log On
- Unexplained New Files
- Unfamiliar File Names
- Inability To Save Files
- Unexplained Modifications/Deletion Of Data
- Unfamiliar Error Messages
- Denial Of Service
- Sudden Lack Of Hard Drive Space
- Computer Continually Restarts
- Difficulty Printing
- Out-of-Memory Error Messages (In a PC with sufficient RAM)

VIRUS/NETWORK ATTACK RESPONSE

1. STOP USING THE COMPUTER
2. DISCONNECT NETWORK CABLE.
3. DO NOT POWER OFF.
4. DO NOT LOG OFF.
5. Run a custom scan on your PC
   a. Right click on the Start Menu button on the Windows desktop. Then select "Open Windows Explorer".
   b. In the Windows Explorer window, left click "Computer".
   c. A list of all the storage devices will appear. Right click the device you want to scan for viruses. A small window called "Scan for threats" will appear. Select "Clean".
   d. Allow the scan to complete. Then close the scan window.
6. If viruses were detected, immediately contact your Unit Cybersecurity Liason (CL – previously IAO) or unit security manager.
7. Ensure no one uses the computer.
8. Follow the instructions of your POC; write down all of the information regarding the incident.

POINTS OF CONTACT

1. UNIT CYBERSECURITY LIASON (CL – previously IAO)	PHONE
2. Alternate UNIT CYBERSECURITY LIASON	PHONE
3. UNIT Security Manager	PHONE

CLASSIFIED MESSAGE INCIDENT

CMI OVERVIEW

A Classified Message Incident (CMI) occurs when higher classification level of data is transferred to a lower classification level system/device via email.

CMI RESPONSE

1. STOP USING THE COMPUTER
2. DISCONNECT NETWORK CABLE.
3. DO NOT POWER OFF.
4. DO NOT LOG OFF.
5. Do not delete, print, or forward the message.
6. Do not leave the computer unattended. The person protecting the computer should be cleared to the level of the message.
7. Immediately contact your unit CyberSecurity Liason (CL-previously IAO) or Unit Security Manager. DO NOT MENTION THAT YOU SUSPECT A CMI HAS OCCURRED UNTIL THE AREA IS SECURED OR YOU ARE ON A SECURE LINE. It's best to speak to them in person.
8. Treat information regarding the CMI at the same level of classification as the CMI.
9. Isolate all external media used (disks, CDs, etc.)

SUSPICIOUS EMAIL OR SPAM

If you receive any suspicious email, phishing, or spam, do not open attachments or go to any links. Open a blank email and attach the suspicious email to it. Then send it to 33NWS.MAN@us.af.mil

Next, right-click the message in the Inbox and select Junk > Block Sender.

SENSITIVE EMAIL

1. The email **must be encrypted** before sending.
2. Mark email correctly before sending:

Space required from classified information 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
Base Stations	3 meters	Approximately 10 feet
Radio Transceivers	3 meters	Approximately 10 feet

Base Communications Focal Point

656-2666

WRIGHTPATTERSONAFBVA33-1, 20 April 2016 (per AFI 33-115 & AFM 33-282)
OPR: 88 CG/SCX
RELEASABILITY: There are no releasability restrictions on this publication