RELEASABILITY: There are no releasability restrictions on this publication.

52 FW 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 PC with sufficient RAM)

VIRUS/NETWORK ATTACK RESPONSE

1. **STOP USING THE COMPUTER IMMEDIATELY!**
2. DO NOT Log off or disconnect power until directed.
3. DO NOT Allow further use of the device.
4. Disconnect the device from the network.
5. Immediately contact your Supervisor and Unit Security Manager.
6. Ensure no one uses the computer.
7. Follow the instructions of your POC; write down all the information regarding the incident.

ENCRYPT E-MAILS CONTAINING THE FOLLOWING:

- Controlled Unclassified Information (CUI)
- Privacy Act Information
- Personally Identifiable Information (PII)
- Individually identifiable health, DoD payroll, finance, logistics, personnel management, proprietary and foreign government information
- Contract data
- Export controlled technical data or information
- Operations Security (OPSEC) information
- Info specified for encryption (e.g., Critical Information List)

POINTS OF CONTACT

1. UNIT CYBERSECURITY LIAISON POC	PHONE
2. UNIT SECURITY MANAGER POC	PHONE
3. WING CYBERSECURITY OFFICE (WCO)	DSN: 452-5532
4. GENERAL TICKET QUEUE (SERVICECENTER)	DSN: 452-2666

NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI), Classified Message or File Incident

An NDCI occurs when classified information exists on a system that is not approved nor authorized to contain that level of classification.

1. **STOP USING THE COMPUTER IMMEDIATELY!**
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 PC unattended. The person guarding it should be cleared to the level of the message.
7. Immediately contact your Supervisor and USM. DO NOT mention that you suspect an NDCI has occurred until the area is secured, or you are on a SECURE LINE.
8. Treat information regarding the NDCI at the same level of classification as the incident.
9. Isolate all external media used (disks, CDs, etc.)

SUSPICIOUS E-MAIL

If you receive suspicious email, DO NOT open attachments or links, and interact with the email as little as possible. Open a blank email and attach the suspicious email as a file. Send the suspicious email to 33NWS.MAN@us.af.mil.

CPCON LEVELS

CPCON is a systematic process for Authorizing Officials/Commanders/Directors to adjust protection postures on the DODIN.

CPCON 5: Risk to mission is **very low** and applies when there is non-specific threat of adversarial activity with limited consequences.

CPCON 4: Risk to mission is **low** and applies when there is a specific threat of adversarial activity with limited consequences.

CPCON 3: Risk to mission is **high** and applies when there is a severe, credible threat of adversarial activity with **significant** consequences.

CPCON 2: Risk to mission is **high** and applies when there is a severe, credible threat of adversarial activity with **severe** consequences.

CPCON 1: Risk to mission is **very high** and applies when a **grave**, credible threat of adversarial activity exists with **catastrophic** consequences.

PERSONAL INFO: ADDITIONAL GUIDANCE

Add "**CUI//PII**" before the Subject and the following statement at the beginning of the e-mail: "**This e-mail contains Controlled Unclassed Information (CUI) information which must be protected under *The Privacy Act* and AFI 33-332.**" Only apply this statement to e-mails containing personal info. Do not send Privacy Act info to distribution lists or group e-mail addresses unless each person has an official need to know. To reach the base PII Manager, Contact 52CS.SCOK.BRM@us.af.mil or 452-6949

See AFMAN 17-1201 User Responsibilities/Guidance for IS

ENCRYPTING E-MAIL TO ORG BOXES

E-mails containing the types of data listed above and sent to org boxes must also be encrypted.

If your org box does not have encryption capability, please contact your Unit Cybersecurity Liaison to initiate the process.

Spangdahlem AB Visual Aid 17-1 (SABVA 17-1)

Prescribed by AFI 17-130 OPR: 52 FW WCO

Certified by 52 CS/CC

Created by the 52 FW Wing Cybersecurity Office (WCO)

Updated 17 Sep 2024

For further inquiries, please contact the Wing Cybersecurity Office

RELEASABILITY: There are no releasability restrictions on this publication.

[Published: 20250220, Prescribed By: AFI17-130]

RELEASABILITY: There are no releasability restrictions on this publication.

[Published: 20250220, Prescribed By: AFI17-130]