

Cyber Incident Response Procedures

REMEMBER OPSEC! NEVER DISCUSS CRITICAL INFORMATION BY NON-SECURE MEANS

PHISHING ATTEMPTS

1. **Network Security first!** - DO NOT reply, and never provide CAC PIN to anyone!
2. **Drag** email from Outlook Inbox and **save** to desktop
3. **Open** a new email and address it to 633ABW.ia@us.af.mil
4. **(Create attachment)** Attach **saved** email from desktop into a new email addressed to 633ABW.ia@us.af.mil and send email.

VIRUS

1. **Physically disconnect your** computer from the network.
(In the event you do not know how, contact your IAO.)
2. **Do NOT** turn off your computer!
3. **Write Down** any errors that your observed on your system.
4. **Mark the** computer "**DO NOT USE**".
5. **Contact** your IAO.
6. **IAO** Contact the Communications Focal Point (CFP) at DSN: 574-2666/
Comm: (757) 764-2666.
7. **Follow** CFP directions.

CLASSIFIED MESSAGE INCIDENT (CMI)

If classified information is inadvertently placed or found on your system, do the following **IMMEDIATELY!**

1. **Physically disconnect your** computer from the network.
(In the event you do not know how, contact your IAO.)
2. **Do not delete,** move, or save the message/file.
3. **Lock** your computer.
4. **Mark** your computer "**DO NOT USE**".
5. **Have someone** with the appropriate clearance physically guard the machine or secure in an area cleared for the same classification level.
6. **Notify** your IAO and Security Manager in person or via secure phone and call the CFP at DSN: 574-2666/Comm: (757) 764-2666.

CMI details are considered classified until all involved systems are sanitized.

7. **Follow** CFP instructions.

Primary IAO:

Alternate IAO:

Security Manager:

Cyber Incident Response Procedures

REMEMBER OPSEC! NEVER DISCUSS CRITICAL INFORMATION BY NON-SECURE MEANS

PHISHING ATTEMPTS

1. **Network Security first!** - DO NOT reply, and never provide CAC PIN to anyone!
2. **Drag** email from Outlook Inbox and **save** to desktop
3. **Open** a new email and address it to 633ABW.ia@us.af.mil
4. **(Create attachment)** Attach **saved** email from desktop into a new email addressed to 633ABW.ia@us.af.mil and send email.

VIRUS

1. **Physically disconnect your** computer from the network.
(In the event you do not know how, contact your IAO.)
2. **Do NOT** turn off your computer!
3. **Write Down** any errors that your observed on your system.
4. **Mark the** computer "**DO NOT USE**".
5. **Contact** your IAO.
6. **IAO** Contact the Communications Focal Point (CFP) at DSN: 574-2666/
Comm: (757) 764-2666.
7. **Follow** CFP directions.

CLASSIFIED MESSAGE INCIDENT (CMI)

If classified information is inadvertently placed or found on your system, do the following **IMMEDIATELY!**

1. **Physically disconnect your** computer from the network.
(In the event you do not know how, contact your IAO.)
2. **Do not delete,** move, or save the message/file.
3. **Lock** your computer.
4. **Mark** your computer "**DO NOT USE**".
5. **Have someone** with the appropriate clearance physically guard the machine or secure in an area cleared for the same classification level.
6. **Notify** your IAO and Security Manager in person or via secure phone and call the CFP at DSN: 574-2666/Comm: (757) 764-2666.

CMI details are considered classified until all involved systems are sanitized.

7. **Follow** CFP instructions.

Primary IAO:

Alternate IAO:

Security Manager:

