

EDWARDS AFB NETWORK INCIDENT REPORTING AID OPSEC – <i>DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION OVER UNAUTHORIZED SYSTEMS</i>	
COMPUTER VIRUS REPORTING PROCEDURES FOR USERS	
STEP 1	<i>STOP! DISCONTINUE USE.</i>
STEP 2	<i>LEAVE THE SYSTEM POWERED UP.</i> Personnel <u>should not</u> click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system – <i>WRITE IT DOWN!</i>
STEP 4	<i>WRITE DOWN ALL ACTIONS</i> that occurred during the suspected virus attacks. (i.e., Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked/unsecured files)
STEP 5	<i>REPORT IT IMMEDIATELY!</i> Contact your unit Information Assurance Officer (IAO) or 412 CS Information Assurance (IA) Office at 7-0658.
NOTE: When reporting a suspected virus to your unit IAO or the 412 CS IA Office, ensure that you give the following information: <ul style="list-style-type: none"> • Event Date and Time • Report Date and Time • Your name and telephone number • Name of your unit IAO • Location of infected system • If unable to contact any of the above contact 412 CS Client Service Center at 7-3444 	
CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS	
A CMI is defined as a classified message that has been sent and/or received over a network for which it is not approved. All information concerning CMIs is CLASSIFIED.	
STEP 1	<i>STOP! DISCONNECT THE LAN CABLE</i> of the affected computer system(s) or printer(s). <i>DO NOT DELETE ANY FILES!</i>
STEP 2	<i>REPORT INCIDENT IMMEDIATELY</i> by secure telephone or in person to your unit IAO, or 412 CS IA Office at 7-0658. <i>DO NOT DISCUSS CMI OVER UNSECURE LINES.</i>
STEP 3	<i>SECURE</i> affected system(s) and/or printer(s) and wait for your unit IAO or 412 CS IA Office to assist you.
INFOCON LEVELS	
The DoD INFOCON system is a series of prescribed and standardized actions to maintain or reestablish the confidence level of networks under a commander's authority. The INFOCON system incorporates a "readiness-based" strategy. INFOCON levels are as follows: <ul style="list-style-type: none"> • INFOCON 5. Routine NetOps: Normal readiness of information systems and networks that can be sustained indefinitely. • INFOCON 4. Increased Vigilance: In preparation of operations or exercises, with a limited impact to the end-user. • INFOCON 3. Enhanced Readiness: Increases the frequency of validation of information networks and their corresponding configurations. Impact to end-user is minor. • INFOCON 2. Greater Readiness: Increases the frequency of validation of information networks and their corresponding configurations. Impact to administrators will increase and impact to end-user could be significant. • INFOCON 1. Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact to administrators and end-users. 	
EDWARDSAFBVA33-200 (Per AFI33-200) 6 December 2012 NETWORK INCIDENT REPORTING AID	
Certified By: 412 CS/CC (Keith Repik) OPR: 412 CS/SCXSA RELEASABILITY: There are no releasability restrictions on this publication	

EDWARDS AFB NETWORK INCIDENT REPORTING AID OPSEC – <i>DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION OVER UNAUTHORIZED SYSTEMS</i>	
COMPUTER VIRUS REPORTING PROCEDURES FOR USERS	
STEP 1	<i>STOP! DISCONTINUE USE.</i>
STEP 2	<i>LEAVE THE SYSTEM POWERED UP.</i> Personnel <u>should not</u> click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system – <i>WRITE IT DOWN!</i>
STEP 4	<i>WRITE DOWN ALL ACTIONS</i> that occurred during the suspected virus attacks. (i.e., Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked/unsecured files)
STEP 5	<i>REPORT IT IMMEDIATELY!</i> Contact your unit Information Assurance Officer (IAO) or 412 CS Information Assurance (IA) Office at 7-0658.
NOTE: When reporting a suspected virus to your unit IAO or the 412 CS IA Office, ensure that you give the following information: <ul style="list-style-type: none"> • Event Date and Time • Report Date and Time • Your name and telephone number • Name of your unit IAO • Location of infected system • If unable to contact any of the above contact 412 CS Client Service Center at 7-3444 	
CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS	
A CMI is defined as a classified message that has been sent and/or received over a network for which it is not approved. All information concerning CMIs is CLASSIFIED.	
STEP 1	<i>STOP! DISCONNECT THE LAN CABLE</i> of the affected computer system(s) or printer(s). <i>DO NOT DELETE ANY FILES!</i>
STEP 2	<i>REPORT INCIDENT IMMEDIATELY</i> by secure telephone or in person to your unit IAO or 412 CS IA Office at 7-0658. <i>DO NOT DISCUSS CMI OVER UNSECURE LINES.</i>
STEP 3	<i>SECURE</i> affected system(s) and/or printer(s) and wait for your unit IAO or 412 CS IA Office to assist you.
INFOCON LEVELS	
The DoD INFOCON system is a series of prescribed and standardized actions to maintain or reestablish the confidence level of networks under a commander's authority. The INFOCON system incorporates a "readiness-based" strategy. INFOCON levels are as follows: <ul style="list-style-type: none"> • INFOCON 5. Routine NetOps: Normal readiness of information systems and networks that can be sustained indefinitely. • INFOCON 4. Increased Vigilance: In preparation of operations or exercises, with a limited impact to the end-user. • INFOCON 3. Enhanced Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end-user is minor. • INFOCON 2. Greater Readiness: Increases the frequency of validation of information networks and their corresponding configuration. Impact to administrators will increase and impact to end-user could be significant. • INFOCON 1. Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact to administrators and end-users. 	
EDWARDSAFBVA33-200 (Per AFI33-200) 6 December 2012 NETWORK INCIDENT REPORTING AID	
Certified By: 412 CS/CC (Keith Repik) OPR: 412 CS/SCXSA RELEASABILITY: There are no releasability restrictions on this publication	

Helpful Hints for Network Users

INFOCON PROTECTIVE MEASURES

- Use the proper password creation methods and utilize screensaver passwords, if applicable, under all INFOCON levels.
- Backup your data under all INFOCON levels. Consider more frequent backups as the level heightens. Ensure you have backups of mission critical data and verify backups work.
- Be aware that as the INFOCON escalates, so does the possible impact to you as an end-user. Prioritize network usage by mission criticality to reduce possible network impact and to maximize mission effectiveness.

Report suspicious activity. As the INFOCON level escalates, personnel should become increasingly mindful of situations that indicate information may be at risk. Stay alert for possible computer viruses/malicious code attacks and unauthorized persons asking for potentially sensitive information, i.e., user-ids, passwords, website or e-mail addresses. Heighten your awareness for signs that your e-mail, login account, or other correspondence might have been tampered with or opened.

TERMINAL SECURITY

- **Ensure your computer terminal is always protected.** Remove your CAC before leaving your terminal or press Ctrl, Alt, and Delete; then press the lock computer option to secure your terminal.
- **Never give out your password.** There is no official reason any AF agency will request your password.
- **Ensure your computer has the latest virus protection files.** Check the version and definition files by right clicking the McAfee icon and select "About". If Last Security Update is more than 3 days old, contact the 412 CS Client Service Center at 7-3444 to get the current date.

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

A PII Breach is defined as a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or access for an unauthorized purpose, to data, whether physical or electronic, where one or more individuals will be harmed (ID Theft, embarrassment, mental anguish, etc.).

- **STOP!** Take actions to mitigate further loss or compromise.
- **REPORT INCIDENT IMMEDIATELY** by phone/email to the Base Privacy Officer (412 CS/SCOK) at 7-3834/3015; Unit Privacy Act Monitor (FARM) and your unit Security Manager.
- COMPLETE United States Computer Emergency Readiness Team (US CERT) NOTIFICATION within one hour of the PII breach discovery at www.us-cert.gov.
- COMPLETE INITIAL PII BREACH REPORT (No names/use positions), Template with instructions located at the AF Privacy Act website, <http://www.privacy.af.mil/helpfulresources/index.asp>
- SUBMIT INITIAL PII BREACH REPORT WITHIN 12 HOURS to Unit Privacy Monitor and Base Privacy Officer via EAFB FOIA/PA Mailbox (foia@edwards.af.mil).
- Base Privacy Officer will validate report and submit to AFMC and senior leadership within 24 hours of breach discovery.

NOTE: Refer to AFI 33-332, AF Privacy Program for subsequent actions.

USB DEVICES

IAW CTO 10-084, Only properly inventoried, government-procured, owned and approved devices are permitted on government information systems.

IAW AFMAN 33-282, COMPUTER SECURITY, PARAGRAPH 6.8.4, "Do Not connect privately-owned media or peripheral devices (including, but not limited to; music/video CD/DVDs, i-devices, commercial MP3 players, and universal serial bus (USB) drives) to AF information systems and government furnished equipment.

LOSS OF CAC or PIN COMPROMISE

If you lose your CAC card take the following action:

- Military: Report loss to 412 SFS LE Desk
- Civilian: Obtain "Lost CAC" letter from 412 FSS/FSMC, Civ Per.
- CNTR: Obtain "Lost CAC" letter from contract Trusted Agent

Go to 412 FSS/FSMPS (CAC/DEERS Office), 7-2276, bldg. 3000, for new CAC.

If you suspect or know of unauthorized use, of your PIN or token, report it to your supervisor and CAC/DEERS Office, 7-2276. Go to one of the locations below to reset your PIN.

If you forget your PIN or enter it incorrectly 3 times, you will have to have to reset it at: 412 CS Client Service Center, bldg 3950 from 0630-1700 (recommended location); MPF, bldg 3000; or AFRL Tech Support Desk, bldg. 8352 Rm 127.

MY INFORMATION ASSURANCE OFFICER (IAO) IS:

Helpful Hints for Network Users

INFOCON PROTECTIVE MEASURES

- Use the proper password creation methods and utilize screensaver passwords, if applicable, under all INFOCON levels.
- Backup your data under all INFOCON levels. Consider more frequent backups as the level heightens. Ensure you have backups of mission critical data and verify backups work.
- Be aware that as the INFOCON escalates, so does the possible impact to you as an end-user. Prioritize network usage by mission criticality to reduce possible network impact and to maximize mission effectiveness.

Report suspicious activity. As the INFOCON level escalates, personnel should become increasingly mindful of situations that indicate information may be at risk. Stay alert for possible computer viruses/malicious code attacks and unauthorized persons asking for potentially sensitive information, i.e., user-ids, passwords, website or e-mail addresses. Heighten your awareness for signs that your e-mail, login account, or other correspondence might have been tampered with or opened.

TERMINAL SECURITY

- **Ensure your computer terminal is always protected.** Remove your CAC before leaving your terminal or press Ctrl, Alt, and Delete; then press the lock computer option and/or remove CAC.
- **Never give out your password.** There is no official reason any AF agency will request your password.
- **Ensure your computer has the latest virus protection files.** Check the version and definition files by right clicking the McAfee icon and select "About". If Last Security Update is more than 3 days old, contact the 412 CS Client Service Center at 7-3444 to get the current date.

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

A PII Breach is defined as a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or access for an unauthorized purpose, to data, whether physical or electronic, where one or more individuals will be harmed (ID Theft, embarrassment, mental anguish, etc.).

- **STOP!** Take actions to mitigate further loss or compromise.
- **REPORT INCIDENT IMMEDIATELY** by phone/email to the Base Privacy Officer (412 CS/SCOK) at 7-3834/3015; Unit Privacy Act Monitor (FARM) and your unit Security Manager.
- COMPLETE United States Computer Emergency Readiness Team (US CERT) NOTIFICATION within one hour of the PII breach discovery at www.us-cert.gov.
- COMPLETE INITIAL PII BREACH REPORT (No names/use positions), Template with instructions located at the AF Privacy Act website, <http://www.privacy.af.mil/helpfulresources/index.asp>
- SUBMIT INITIAL PII BREACH REPORT WITHIN 12 HOURS to Unit Privacy Monitor and Base Privacy Officer via EAFB FOIA/PA Mailbox (foia@edwards.af.mil).
- Base Privacy Officer will validate report and submit to AFMC and senior leadership within 24 hours of breach discovery.

NOTE: Refer to AFI 33-332, AF Privacy Program for subsequent actions.

USB DEVICES

IAW CTO 10-084, Only properly inventoried, government-procured, owned and approved devices are permitted on government information systems.

IAW AFMAN 33-282, COMPUTER SECURITY, PARAGRAPH 6.8.4, "Do Not connect privately-owned media or peripheral devices (including, but not limited to; music/video CD/DVDs, i-devices, commercial MP3 players, and universal serial bus (USB) drives) to AF information systems and government furnished equipment.

LOSS OF CAC or PIN COMPROMISE

If you lose your CAC card take the following action:

- Military: Report loss to 412 SFS LE Desk
- Civilian: Obtain "Lost CAC" letter from 412 FSS/FSMC, Civ Per.
- CNTR: Obtain "Lost CAC" letter from contract Trusted Agent

Go to 412 FSS/FSMPS (CAC/DEERS Office), 7-2276, bldg. 3000, for new CAC.

If you suspect or know of unauthorized use, of your PIN or token, report it to your supervisor and CAC/DEERS Office, 7-2276. Go to one of the locations below to reset your PIN.

If you forget your PIN or enter it incorrectly 3 times, you will have to have to reset it at: 412 CS Client Service Center, bldg 3950 - 0630-1700 (recommended location); MPF, bldg 3000; or AFRL Tech Support Desk, bldg. 8352 Rm 127.

MY INFORMATION ASSURANCE OFFICER (IAO) IS: