

# 914 AW NETWORK USERS QUICK REFERENCE CARD

**NETWORK USER "DO's and DON'T's":** All network users can help ensure network integrity by following the below "DO's and DON'T's." These are all common-sense items that, if adhered to, will assist in maintaining network security and help thwart threat attempts by an unknown attacker.

**A Be aware of your surroundings** and report suspicious behavior such as "shoulder surfing" or unauthorized access to sensitive or classified information. Challenge unknown personnel in your areas, especially when their behavior is questionable!

**B Never leave your computer unattended** without using a password/PIN-protected screen saver, removing your common access card (CAC), or logging off the network completely. Never leave your CAC unattended in your computer.

**C Protect your access to information** from the insider threat: DO NOT share your password/PIN. DO NOT write your password/PIN down so it can be accessed easily. Remember, the first places an intruder will check for your password/PIN are the most common places the people write them down: (1) on the back of keyboards, (2) bottom of the mouse, (3) posted on the wall and (4) printed on a piece of paper laying in a desk drawer.

**D Social engineering** is a very common network threat. Social engineering can be accomplished by email, telephone or even in person. A very common attack is an email asking you to test your password /PIN for composition compliance by "inserting it in the space provided and pressing Enter." There is no reason whatsoever for a network user to provide his or her password/PIN. No matter how official the email looks, no matter who the requestor says he or she is, no matter whether the individual is sitting there in your office—NEVER give your password/PIN to anyone for any reason. If you are aware of any type of social engineering, immediately contact the CFP/Help Desk, or the Wing Cybersecurity Liaison (WCSO)

**E Don't download personal software, games or programs** from the internet without obtaining prior approval. No software is to be loaded on any workstation that is not approved by AFRC. Downloaded files may contain malicious logic such as viruses or Trojan Horse programs. Report suspicious computer behavior to your Cybersecurity Liaison.

**F Distributed Denial of Service (DDoS)** – a common threat, mostly originating in the form of an email (maybe from someone you know, but having unusual subject lines) containing an attachment having an embedded script that gets your entire address book, looks everyone up in it and sends a copy of the email (with the attachment) to them. Do not open suspicious emails – immediately delete them and notify your Cybersecurity Liaison

**G Internet Hoaxes** - emails purporting to warn of a new virus, a moneymaking scheme or a chain letter asking you to forward them to all your friends! Do not respond to these emails; delete them and contact your Cybersecurity Liaison.

**H Scan all (authorized) removable media for viruses before accessing!**  
Common symptoms of malicious behavior include: (1) slow performance, (2) files disappearing, (3) constant error messages, (4) erratic screen flashing or (5) constant email error messages. Contact your Cybersecurity Liaison

**I Unauthorized Remote Access** – If your mouse begins to jump around the screen, and files/programs access without your direct action, it is a possible security incident – notify your Cybersecurity Liaison immediately!

**J Personal Electronic Devices (PEDs)**—AFSSI 8502 para. 3.5.1.10 explicitly prohibits connecting any PED to a government computer. This includes cell phones, MP3 players, etc. In addition, AFNOC NTO 2008-323-001 prohibits connecting devices containing "flash" memory (i.e., thumb /jump drives, camera memory cards) to the Air Force network.

**Points of Contact Unit Cybersecurity Liaison:**

**Wing Information Assurance Office:** 236-2032  
**CFP/Help Desk:** 236-3310

914AWVA 33-202 16 JUNE 2015 OPR: 914 CS/SCXS  
Supersedes: 914AWVA 33-202, 29 Oct 2010  
Prescribed by: AF133-200  
RELEASABILITY: There are no releasability restrictions on this publication

# 914 AW NETWORK USERS QUICK REFERENCE CARD

**NETWORK USER "DO's and DON'T's":** All network users can help ensure network integrity by following the below "DO's and DON'T's." These are all common-sense items that, if adhered to, will assist in maintaining network security and help thwart threat attempts by an unknown attacker.

**A Be aware of your surroundings** and report suspicious behavior such as "shoulder surfing" or unauthorized access to sensitive or classified information. Challenge unknown personnel in your areas, especially when their behavior is questionable!

**B Never leave your computer unattended** without using a password/PIN-protected screen saver, removing your common access card (CAC), or logging off the network completely. Never leave your CAC unattended in your computer.

**C Protect your access to information** from the insider threat: DO NOT share your password/PIN. DO NOT write your password/PIN down so it can be accessed easily. Remember, the first places an intruder will check for your password/PIN are the most common places the people write them down: (1) on the back of keyboards, (2) bottom of the mouse, (3) posted on the wall and (4) printed on a piece of paper laying in a desk drawer.

**D Social engineering** is a very common network threat. Social engineering can be accomplished by email, telephone or even in person. A very common attack is an email asking you to test your password /PIN for composition compliance by "inserting it in the space provided and pressing Enter." There is no reason whatsoever for a network user to provide his or her password/PIN. No matter how official the email looks, no matter who the requestor says he or she is, no matter whether the individual is sitting there in your office—NEVER give your password/PIN to anyone for any reason. If you are aware of any type of social engineering, immediately contact the CFP/Help Desk or the Wing Cybersecurity Liaison (WCSO)

**E Don't download personal software, games or programs** from the internet without obtaining prior approval. No software is to be loaded on any workstation that is not approved by AFRC. Downloaded files may contain malicious logic such as viruses or Trojan Horse programs. Report suspicious computer behavior to your Cybersecurity Liaison.

**F Distributed Denial of Service (DDoS)** – a common threat, mostly originating in the form of an email (maybe from someone you know, but having unusual subject lines) containing an attachment having an embedded script that gets your entire address book, looks everyone up in it and sends a copy of the email (with the attachment) to them. Do not open suspicious emails – immediately delete them and notify your Cybersecurity Liaison

**G Internet Hoaxes** - emails purporting to warn of a new virus, a moneymaking scheme or a chain letter asking you to forward them to all your friends! Do not respond to these emails; delete them and contact your Cybersecurity Liaison.

**H Scan all (authorized) removable media for viruses before accessing!**  
Common symptoms of malicious behavior include: (1) slow performance, (2) files disappearing, (3) constant error messages, (4) erratic screen flashing or (5) constant email error messages. Contact your Cybersecurity Liaison

**I Unauthorized Remote Access** – If your mouse begins to jump around the screen, and files/programs access without your direct action, it is a possible security incident – notify your Cybersecurity Liaison immediately!

**J Personal Electronic Devices (PEDs)**—AFSSI 8502 para. 3.5.1.10 explicitly prohibits connecting any PED to a government computer. This includes cell phones, MP3 players, etc. In addition, AFNOC NTO 2008-323-001 prohibits connecting devices containing "flash" memory (i.e., thumb /jump drives, camera memory cards) to the Air Force network.

**Points of Contact Unit Cybersecurity Liaison:**

**Wing Information Assurance Office:** 236-2032  
**CFP/Help Desk:** 236-3310

914AWVA 33-202 16 JUNE 2015 OPR: 914 CS/SCXS  
Supersedes: 914AWVA 33-202, 29 Oct 2010  
Prescribed by: AF133-200  
RELEASABILITY: There are no releasability restrictions on this publication

<b>914<sup>th</sup> AW</b> <b>NETWORK INCIDENT REPORTING AID</b> <i>OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS</i>	
<b>COMPUTER VIRUS REPORTING PROCEDURES FOR USERS</b>	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE.</b> Discontinue Use.
<b>STEP 2</b>	<b>LEAVE THE SYSTEM POWERED UP.</b> <b>DO NOT</b> click on any prompts, close any windows, or shut down the system.
<b>STEP 3</b>	If a message appears on the monitor of the affected system – <b>WRITE IT DOWN!</b>
<b>STEP 4</b>	<b>WRITE DOWN ALL ACTIONS</b> that occurred during the suspected virus attack. (Did the virus come from an email attachment, diskette, etc..?)
<b>STEP 5</b>	<b>REPORT IT IMMEDIATELY!</b> Contact your section's Cybersecurity Liaison and Helpdesk at 236-3310
<p><b>NOTE:</b> When reporting a suspected virus to your Cybersecurity Liaison and the Helpdesk, ensure you give the following information:</p> <ul style="list-style-type: none"> <li>- Event Date and Time</li> <li>- Name of your Cybersecurity Liaison</li> <li>- Report Date and Time (of event)</li> <li>- Location of infected system(s)</li> <li>- Your name, telephone number, building and organization</li> </ul>	
<b>CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS</b>	
<p>A <i>CMI</i> is defined as a classified message that has been sent and/or received over an unclassified network.</p>	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE</b> of the affected computer system(s) and/or printer(s) <b>DO NOT POWER OFF</b>
<b>STEP 2</b>	<b>SECURE</b> affected system(s) / printer(s), area / room. <b>DO NOT</b> leave system unsecured. Ensure it remains under control of authorized personnel with the appropriate clearance.
<b>STEP 3</b>	<b>REPORT INCIDENT IMMEDIATELY</b> by telephone or in person to your Security Manager, Supervisor, Cybersecurity Liaison and the help Desk at 236-3310. Note: You may only say, "I'd like to report a possible CMI" via non-secure means.
<b>INFOCON LEVELS</b>	
<p>INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer and telecommunication systems and networks. INFOCON levels are as follows:</p>	
<p><b>INFOCON 5:</b> <u>Normal Net Ops</u>: Normal readiness of information systems and networks that can be sustained indefinitely.</p>	
<p><b>INFOCON 4:</b> <u>Increased Risk</u>: In preparation for operations or exercises, with a limited impact to the end user.</p>	
<p><b>INFOCON 3:</b> <u>Enhanced Readiness</u>: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end-user is minor.</p>	
<p><b>INFOCON 2:</b> <u>Greater Readiness</u>: Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end-user could be significant.</p>	
<p><b>INFOCON 1:</b> <u>Maximum Readiness</u>: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end-users.</p>	

<b>914<sup>th</sup> AW</b> <b>NETWORK INCIDENT REPORTING AID</b> <i>OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS</i>	
<b>COMPUTER VIRUS REPORTING PROCEDURES FOR USERS</b>	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE.</b> Discontinue Use.
<b>STEP 2</b>	<b>LEAVE THE SYSTEM POWERED UP.</b> <b>DO NOT</b> click on any prompts, close any windows, or shut down the system.
<b>STEP 3</b>	If a message appears on the monitor of the affected system – <b>WRITE IT DOWN!</b>
<b>STEP 4</b>	<b>WRITE DOWN ALL ACTIONS</b> that occurred during the suspected virus attack. (Did the virus come from an email attachment, diskette, etc..?)
<b>STEP 5</b>	<b>REPORT IT IMMEDIATELY!</b> Contact your section's Cybersecurity Liaison and Helpdesk at 236-3310
<p><b>NOTE:</b> When reporting a suspected virus to your Cybersecurity Liaison and the Helpdesk, ensure you give the following information:</p> <ul style="list-style-type: none"> <li>- Event Date and Time</li> <li>- Name of your Cybersecurity Liaison</li> <li>- Report Date and Time (of event)</li> <li>- Location of infected system(s)</li> <li>- Your name, telephone number, building and organization</li> </ul>	
<b>CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS</b>	
<p>A <i>CMI</i> is defined as a classified message that has been sent and/or received over an unclassified network.</p>	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE</b> of the affected computer system(s) and/or printer(s) <b>DO NOT POWER OFF</b>
<b>STEP 2</b>	<b>SECURE</b> affected system(s) / printer(s), area / room. <b>DO NOT</b> leave system unsecured. Ensure it remains under control of authorized personnel with the appropriate clearance.
<b>STEP 3</b>	<b>REPORT INCIDENT IMMEDIATELY</b> by telephone or in person to your Security Manager, Supervisor, Cybersecurity Liaison and the help Desk at 236-3310. Note: You may only say, "I'd like to report a possible CMI" via non-secure means.
<b>INFOCON LEVELS</b>	
<p>INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer and telecommunication systems and networks. INFOCON levels are as follows:</p>	
<p><b>INFOCON 5:</b> <u>Normal Net Ops</u> : Normal readiness of information systems and networks that can be sustained indefinitely.</p>	
<p><b>INFOCON 4:</b> <u>Increased Risk</u>: In preparation for operations or exercises, with a limited impact to the end user.</p>	
<p><b>INFOCON 3:</b> <u>Enhanced Readiness</u>: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end-user is minor.</p>	
<p><b>INFOCON 2:</b> <u>Greater Readiness</u>: Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end-user could be significant.</p>	
<p><b>INFOCON 1:</b> <u>Maximum Readiness</u>: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end-users.</p>	