914 ARW
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 Enterprise Service Desk (ESD), or your Cyber Security Liaison (CL)

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 CL.

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 CL.

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 CL.

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 CL.

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 CL 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:

Wing Information Assurance Office: 236-2032/2009
CFP: 236-3310/3684
AFRC/MCCC: DSN 497-1783 Comm. (478) 327-1783

914ARWVA 17-1301 Supersedes 914AWVA 33-302
8 November 2021
Prescribed by AFI 17-203 & AFMAN 17-1301
OPR: 914 CS/SCXS
914ARW Network Users Quick Reference Guide
RELEASABILITY: There are no releasability restrictions on this publication

914 ARW
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 Enterprise Service Desk (ESD), or your Cyber Security Liaison (CL)

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 CL.

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 CL.

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 CL.

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 CL.

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 CL 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:

Wing Information Assurance Office: 236-2032/2009
CFP: 236-3310/3684
AFRC/MCCC: DSN 497-1783 Comm. (478) 327-1783

914ARWVA 17-1301 Supersedes 914AWVA 33-302
8 November 2021
Prescribed by AFI 17-203 & AFMAN 17-1301
OPR: 914 CS/SCXS
914ARW Network Users Quick Reference Guide
RELEASABILITY: There are no releasability restrictions on this publication

914 ARW
NETWORK INCIDENT REPORTING AID
OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	***STOP! DISCONNECT THE LAN CABLE.*** Discontinue Use.
STEP 2	**LEAVE THE SYSTEM POWERED UP.** Personnel should not 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 – **WRITE IT DOWN!**
STEP 4	**WRITE DOWN ALL ACTIONS** that occurred during the suspected virus attack. (Did the virus come from an email attachment, diskette, etc..?)
STEP 5	**REPORT IT IMMEDIATELY!** Contact your section's Cyber Security Liaison (CL) and CFP at 236-3310 or 236-3684

NOTE: When reporting a suspected virus to your CL and the CFP, ensure you give the following information:

- Event Date and Time
- Report Date and Time (of event)
- Your name, telephone number, building and organization
- Name of your CL
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network.

STEP 1	**STOP! DISCONNECT THE LAN CABLE** of the affected computer system(s) and/or printer(s)
STEP 2	**SECURE** affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	**REPORT INCIDENT IMMEDIATELY** by telephone or in person to your Security Manager, CL, Supervisor and the CFP at 236-3310 or 236-3684. Note: You may only say, "**I'd like to report a possible CMI**" via non-secure means…wait for Help Desk personnel to assist.

INFOCON LEVELS

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:

INFOCON 5: Routine NetOps: Normal readiness of information systems and networks that can be sustained indefinitely.
INFOCON 4: Increased Vigilance: In preparation for 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 its 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 on administrators and end-users.

914 ARW
NETWORK INCIDENT REPORTING AID
OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	***STOP! DISCONNECT THE LAN CABLE.*** Discontinue Use.
STEP 2	**LEAVE THE SYSTEM POWERED UP.** Personnel should not 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 – **WRITE IT DOWN!**
STEP 4	**WRITE DOWN ALL ACTIONS** that occurred during the suspected virus attack. (Did the virus come from an email attachment, diskette, etc..?)
STEP 5	**REPORT IT IMMEDIATELY!** Contact your section's Cyber Security Liaison (CL) and CFP at 236-3310 or 236-3684

NOTE: When reporting a suspected virus to your CL and the CFP, ensure you give the following information:

- Event Date and Time
- Report Date and Time (of event)
- Your name, telephone number, building and organization
- Name of your CL
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network.

STEP 1	**STOP! DISCONNECT THE LAN CABLE** of the affected computer system(s) and/or printer(s)
STEP 2	**SECURE** affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	**REPORT INCIDENT IMMEDIATELY** by telephone or in person to your Security Manager, CL, Supervisor and the CFP at 236-3310 or 236-3684. Note: You may only say, "**I'd like to report a possible CMI**" via non-secure means…wait for Help Desk personnel to assist.

INFOCON LEVELS

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:

INFOCON 5: Routine NetOps: Normal readiness of information systems and networks that can be sustained indefinitely.
INFOCON 4: Increased Vigilance: In preparation for 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 its 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 on administrators and end-users.