

**BY ORDER OF THE COMMANDER
21ST SPACE WING**

21ST SPACE WING INSTRUCTION 33-415

2 APRIL 2015



Communication and Information

**PETERSON AIR FORCE BASE
NETWORK SECURITY ACCOUNTABILITY**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil/.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 21 CS/SCXS

Certified by: 21 CS/CC
(Lt Col John P. Heidenreich)

Supersedes: 21SWI33-415, 24 October 2012

Pages: 8

This instruction establishes guidance concerning network security accountability on all networks and information systems provided by the 21st Space Wing (21 SW). This instruction implements AFI 33-115, *Air Force Information Technology (IT) Service Management* and AFI 33-200 *Information Assurance (IA) Management*. This includes all systems located on Peterson AFB (including tenant units) and geographically separated units (GSU). All personnel assigned or attached to Peterson AFB, including contractors fulfilling contractual duties, are responsible for sustaining the integrity, availability, and confidentiality of the information transported on the 21 SW's networks and information systems. This publication applies to members of the Air Force Reserve and Air National Guard. All personnel must comply with AFI 33-332, *Air Force Privacy and Civil Liberties Program*, for documents containing privacy act information. All personnel must comply with DOD Regulation 5200.1-R, *Information Security Program* and USD (I) *Memorandum Interim Information Security Guidance*, for documents containing For Official Use Only information. Failure to observe the prohibitions and mandatory provisions in Paragraphs 5.3.1. thru 5.3.6., and 9 of this publication is a violation of Article 92 of the UCMJ, or that noncompliance may result in punishment under Article 92 of the UCMJ. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) *Records Disposition Schedule (RDS)*. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented.

SUMMARY OF CHANGES

This publication has been revised and must be completely reviewed. This rewrite of 21SWI33-415 includes, (1) Removing all AFI33-138 reference throughout as it is obsolete and reference changed to AFI 33-115, (2) Updating in reference Certifying Official Lt Col MICHAEL G. HUNSBERGER is hereby changed to Lt Col JOHN P. HEIDENREICH, (3) Updating in reference to Approving Official CHRIS D. CRAWFORD, Colonel is hereby changed to JOHN E. SHAW, Colonel, (4) Updating in reference Information Assurance Manager is changed to Information Systems Security Manager (ISSM), (5) Updating in reference Information Assurance Officer (IAO) is changed to Information Systems Security Officer (ISSO), (6) Updating in reference Information Assurance (IA) is changed to Cybersecurity, (7) Adding the new prescribing form 21SW Form 2, Virus and Incident Card. A margin bar (|) indicates newly revised material.

1. Overview. Program Overview and Other Compliances Areas.

1.1. This publication establishes guidance and responsibility for the Information Assurance Management Programs. The procedure includes complying with all applicable policies, directives, regulations, and statutes IAW AFI 33-115, *Air Force Information Technology (IT) Service Management* and AFI 33-200 *Information Assurance (IA) Management*, DoD Regulation 5200.1-R, *Information Security Program* and USD (I) *Memorandum Interim Information Security Guidance*. All 21st Space Wing, GSUs and Tenant units within the 21st Space Wing units/users at all levels must ensure compliance is to be followed. Who and what are the roles and responsible in ensuring the appropriate classification and marking of all information on the network. This publication defines a network security incident is any activity, event, or action that violates policy, guidance, or directives; introduces additional vulnerabilities; or increases risk to the network or the 21 SW information systems. A classified message incident (CMI) is a security incident that results in the inappropriate transfer of information on a system, applications, or media which is below the classification of the information

2. Roles and Responsibilities.

2.1. 21st Space Wing Commander (21 SW/CC).

2.1.1. The 21 SW/CC has the overall responsibility of implementing the Cybersecurity program for all networks and information systems and ensures users or personnel comply with AFI 33-200, Information Assurance (IA) Management.

2.2. 21st Communications Squadron Commander (21 CS/CC):

2.2.1. The 21 CS/CC is the lead for all Cybersecurity and Computer Security accounting. The 21 CS/CC is responsible for initiating actions to improve or restore Cybersecurity posture as well as reporting an annual review of all Cybersecurity programs that fall under the 21 SW.

2.3. 21st Space Wing Cybersecurity Office:

2.3.1. The Cybersecurity office provides assistance and guidance to the Host Wing for COMPUSEC, COMSEC and EMSEC requirements and implementation under the Cybersecurity program. The Cybersecurity office ensures ISSOs are informed on Air Force policies for all networks that fall under the 21 SW purview.

2.4. 21st Space Wing Information Systems Security Manager (ISSM):

2.4.1. The ISSM implements and maintains an IS-level Cybersecurity program and documents the Cybersecurity program through the Air Force C&A process in AFI 33-210.

2.5. Information Systems Security Officer (ISSO):

2.5.1. The ISSOs will report vulnerabilities and incidents on information systems according to AFI 31-401, *Information Security Program Management*, in coordination with their organization security manager. ISSOs act as the single liaison between the organization and ISSM or wing Cybersecurity office for COMPUSEC matters under the Cybersecurity program. They also ensure procedures are in place for users to notify the unit ISSO or alternate if problems arise during critical or classified processing.

3. Clearance, Training and User Agreements.

3.1. **Clearance.** Users and system support personnel must have the required security clearances, authorization and need to know before being granted access and for the duration of access to any 21 SW information system or network.

3.2. **Training.** Trained and knowledgeable information resource users and administrators are a key element of Defense in Depth. A viable Cybersecurity program must include initial, periodic, supplemental and remedial training to develop and maintain knowledgeable information resource users and administrators.

3.2.1. All personnel accessing 21 SW information systems must complete mandatory training as dictated by policies and directives. Failure to complete mandatory training will result in suspension of network and information resource access privileges. Access to network information systems will be restored upon completion of mandatory training requirements and with commander approval.

3.2.2. All personnel will receive initial training prior to accessing Peterson AFB and 21 SW information resources. Department of Defense (DoD) Cybersecurity Awareness training is available through unit training managers. Additionally, new network users will be given a 5-day grace period to accomplish the training through Advanced Distributed Learning Service (ADLS).

3.2.3. All personnel will complete DoD user awareness training and any other reoccurring training prescribed by Cybersecurity directives.

3.2.4. All personnel with elevated access privileges or Cybersecurity duties and responsibilities will be trained and certified IAW DoD 8570.01-M. Certification must be completed within 6 months of assignment into the position, for military and government civilians. Contractors must be certified prior to being engaged. Failure to complete certification could result in a denial of access to the network.

3.3. **Agreements.** User agreements provide guidance for use of information resources and dictate conduct on the network. Compliance with agreements is mandatory.

3.3.1. All personnel must sign a **Privileged User Agreement and/or Standard User Agreement** prior to accessing 21 SW network resources. See *Privileged User Agreement in DOD 8570.01-M, Appendix 4*.

3.3.2. Re-accomplishing user agreements will be mandatory when there are modifications made to the agreements.

4. Classified Message Incidents. All personnel are responsible for ensuring the protection of sensitive and classified information. In the event that a potential CMI has been detected on any electronic media, take the following actions:

4.1. Contact your ISSO and notify the security manager immediately. Your security manager and network administrative staffs will assist with the containment, verification, and sanitization, as required, of the questionable information.

5. Removable Media.

5.1. The use of flash media on the DoD networks is prohibited per USCYBERCOM Communications Tasking Order (CTO) 10-084. Further, transferring information to removable media on SIPRNet is prohibited per USCYBERCOM CTO 10-133. A waiver process is available for those units/missions which would incur mission failure if the media is not available.

5.2. **Universal Serial Bus (USB)** storage devices, re-writeable CDs (CD-RW), and re-writeable DVDs (DVD-RW) are not authorized for use with any 21 SW classified information resources without an approved waiver from the AF DAA. USB storage devices are not authorized on 21 SW unclassified information resources without previous written approval from the unit ISSO and Wing Cybersecurity Office. USB storage devices containing flash media are prohibited.

5.3. Although most offenses are not malicious, it is critical for all to adhere to removable media standards. Do not under any circumstance plug a device into a Department of Defense (DoD) computer, even if to only charge your cell phone. It constitutes a violation of the flash media ban. Consequences for violating CTO10-084 by using non-hard disk drive Universal Serial Bus (USB) devices are as follows:

5.3.1. Personally owned unauthorized devices will be confiscated, by unit ISSO, and will be turned over to the unit commander.

5.3.1.1. 21 SW ISSM will make a recommendation to owner's group commander or first O-6 in chain on disposition of the unauthorized device.

5.3.1.2. Group commander or first O-6 in chain will make final disposition decision.

5.3.2. The workstation will be re-imaged before reuse.

5.3.3. User will lose network privileges until an investigation of the violation is completed. Violations involving classified media must be formally reported through the Unit Security Manager to Wing Information Protection (IP) as a security incident.

5.3.4. User must re-accomplish DoD IAA Cyber Awareness Challenge and Defense Information Systems Agency (DISA) Portable Electronic Devices and Removable Storage Media training and provide certificates to the Wing Cybersecurity Office before network privileges will be reinstated.

5.3.5. If the individual's access to the network is mission critical, the individual's Unit Commander must contact the 21st Mission Support Group Commander to request remediation.

5.3.5.1. 21 SW Cybersecurity office will require a digital signed email from users' unit commander requesting network access re-instatement.

5.3.6. Unit Commanders will ensure users are counseled or disciplined for first offenses. Repeat offenses will result in disciplinary action as the Unit Commander deems necessary.

5.3.7. The required training is located at: <http://iase.disa.mil/eta/online-catalog.html#iaatraining>

6. Data Transfers. Users will follow Cybersecurity policy regarding electronic file transfer. Improper transfer will initiate a security incident, and could result in a compromise. Users will contact their unit ISSO for assistance with data transfer. Improper transfer will be reported to the applicable security manager and 21 SW Cybersecurity.

6.1. High-to-low: This transfer is when a user takes unclassified information from a classified system and moves it to an unclassified system. This type of transfer is NOT AUTHORIZED unless there is a waiver to CTO 10-133 on file exempting the system and user and an approved Cross Domain Solution is used to make the transfer.

6.2. Low to high: This transfer is when a user takes unclassified information from an unclassified system and moves it to a classified system. Unclassified information/records are to be maintained on unclassified systems, unless they are needed to complete or update classified information/records. Low-to-high transfers are approved but will be accomplished as follows:

6.2.1. Use only CD or DVD optical disks (no re-writeable disks).

6.2.2. Do not use flash media.

6.2.3. Ensure the session is "closed" after the files are written to the disk(s).

6.2.4. Once the disk is inserted into the classified system it will take on the classification of the system.

7. Procedures. All communications regarding a suspected security incident will be conducted by a secure means of communications. Any employee who identifies or suspects a policy violation has occurred must immediately contact his/her unit ISSO or unit security manager.

8. Investigations. Incidents will be investigated and reported IAW DoD 5200.1-R, CJCSI 6510.01F and AFI 31-401.

9. Violations. Personnel in violation of the policies and regulations listed within this document are subject to administrative or punitive action under DoD 5200.1-R, military members may also be charged under the Uniform Code of Military Justice and/or applicable criminal law. DoD

military and civilian personnel may be sanctioned by warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, or loss of security clearance. Violations by contractor personnel will be reported to the 21st Contracting Squadron for sanctions. Administrative actions may include suspension or revocation of network access privileges. Commanders will ensure corrective actions and punishments will be implemented, as appropriate.

JOHN E SHAW, Colonel, USAF
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 31-401, *Information Security Program Management*, Nov 2005

AFI 33-200, *Information Assurance (IA) Management*, Dec 2008

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, Dec 2008

AFI 33-332, *Air Force Privacy Program*, May 2011

AFMAN 33-363, *Management of Records*, Mar 2008

HQ AFSPC/A6 Memorandum, *Combined Implementation Guidance for United States Cyber Command (USCYBERCOM) Communications Tasking Orders (CTO) 10-084 and 10-133*, Dec 2013

CJCSI 6510.01F: *Information Assurance (IA) and Computer Network Defense (CND)*, Feb 2011, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

DoDD 5200.1-R, *Information Security Program*, Jan 1997

DoDD 8570.01-M, *Information Assurance Workforce Improvement Program*, Dec 2005

Prescribed Forms

21SW Form 2, *Virus and Incident Card*.

Adopted Form

AF Form 847, *Recommendation for Change of Publication*

Appendix 4, DOD 8570.01-M, *STANDARD USER Agreement*

Abbreviations and Acronyms

21 CS—21st Communications Squadron

21 SW IA—21st Space Information Assurances

21 SW—21st Space Wing

ADLS—Advanced Distributed Learning Service

AF—Air Force

AFB—Air Force Base

AIA—Air Intelligence Agency

C&A—Certification and Accreditation

CD—Compact Disc

CD—RW —Compact Disc Read Writable

CFP—Communications Focal Point

CMI—Classified Message Incident

COMPUSEC—Computer Security
COMSEC—Communications Security
CS—Communications Squadron
CTO—Communications Tasking Order
DAA—Designated Accrediting Authority
DoD—Department of Defense
DVD—Digital Video Disc
EMSEC—Emissions Security
GSU—Geographically Separated Unit
INOSC—Integrated Network Operations Support Cell
ISSO—Information Systems Security Officer
ISSM—Information Systems Security Manager
IS—Information System
NIPRNet—Non-Classified Internet Protocol Router Network
SIPRNet—Secret Internet Protocol Router Network