

**BY ORDER OF THE COMMANDER
NATIONAL AIR AND SPACE
INTELLIGENCE CENTER**

NASIC INSTRUCTION 33-201

11 JULY 2013



Communications and Information

**NASIC MEDIA ACCOUNTABILITY
PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: NASIC/SCXP

Certified by: NASIC/SCX
(Mr. Manuel Gomez)

Pages: 11

This new instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*. It establishes the policy and guidance needed to ensure standardized management of removable media within the National Air and Space Intelligence Center (NASIC). It provides the NASIC implementation plan for compliance with Intelligence Community Standard (ICS) Number 500-18, *Removable Media Management*. This instruction applies to all NASIC civilian and military personnel as well as all Air Force Reserve Command (AFRC) Units and Air National Guard (ANG) Units assigned to NASIC. All personnel are required to adhere to the policies and standards in this instruction to ensure the effective management of all removable media within the NASIC complex and its annexes. This NASIC instruction may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this instruction to the OPR using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field to NASIC Publications Office (NASIC/SCOK), 4180 Watson Way, Wright-Patterson AFB, OH 45433-5648, ATTN: Publications/Forms Managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. Contact supporting records managers as required. If information is collected by one or more organizational components and transmitted to other organizational components for management purposes, the Information Collection and Reports (ICR) Manager must review for accuracy and compliance with AFI 33-324, *The Air Force Information Collections and Reports Management Program*. The use of the

name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

1. SCOPE.

1.1. Authorizations.

1.1.1. Authorizations for this Instruction are derived from and based on ICS 500-18, which, in turn, are authorized via Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation*.

1.1.2. The key provisions of the ICS and ICD governing removable media are:

1.1.2.1. All removable media, and uses thereof, must be authorized prior to use.

1.1.2.2. All authorized uses of removable media must be consistent with ICS 500-18.

1.1.2.3. Removable media must be accounted for (registered, tracked, distributed, decommissioned) by the responsible parties in accordance with this instruction.

1.1.2.4. Media will be tracked throughout its lifecycle from creation to final disposition.

1.2. Applicability.

1.2.1. This instruction applies to all removable media located in a SCIF or Secret Open Storage area. For the purpose of this document, removable media is defined as being any of the following:

1.2.1.1. Compact Disks (CD-R, CD-DA)

1.2.1.2. Digital Video Disks (DVD-R, DL-DVD)

1.2.1.3. Blu-ray Discs (BD, BD-R, BDXL-R)

1.2.1.4. External Hard Drives (USB, eSATA, FireWire, etc).

1.2.1.5. Magnetic Tape (LTxx, 8mm, VHS, 4mm, etc).

1.2.1.6. Flash Media (MicroSD, Compact Flash, etc).

1.2.1.7. Magnetic Disks (Floppy, Zip, etc).

1.2.1.8. Dongles (license / authentication key hardware).

1.2.1.9. Thumb Drives (additional restrictions apply).

1.2.1.10. Any portable electronic device connectable to PCs or Information Systems.

1.2.1.10.1. Portable Electronic Devices (PEDs) will be handled in accordance with ICD 705, *Sensitive Compartmented Information Facilities*, NASICI 31-106, *Portable Electronic Devices*, and any subordinate policy documents.

1.2.1.10.2. Personal PEDs such as MP3 players and personnel audio/video devices with potential recording capability must be specifically authorized before entry into or operation in the SCIF. Refer to NASICI 31-106 for additional information regarding personal PEDs and personal music CDs which have been

commercially produced.

1.2.2. This instruction does not apply to media contained in a sealed, closed system such as internal hard drives, internal flash drives, solid state drives (SSDs), or tape storage or robotic systems.

1.2.3. All media types must be approved by the Information Assurance Office before being brought into the center. Some media types are not permitted in the Center. See the Information Assurance Office (NASIC/SCXS) for specific guidance.

1.2.4. All NASIC employees must comply with this instruction. If visitors bring media into the SCIF, a NASIC employee must register and track the media. If the media is removed from the building at the end of the visit, the transfer must be documented appropriately. A NASIC employee must provide positive control of such media at all times when the media items are within the SCIF.

2. RESPONSIBILITIES.

2.1. Groups/Directorates will:

2.1.1. Exercise responsibility for controlling removable media within their organizations.

2.1.2. Appoint Media Accountability Managers (MAMs) and Media Accountability Administrators (MAAs). Groups may assign additional MAMs or MAAs as needed to fulfill the responsibilities of the Media Accountability program. A sample appointment letter is included in Attachment 2.

2.2. Directorate of Communications and Information (NASIC/SC) will:

2.2.1. Appoint the Lead Media Accountability Manager (LMAM).

2.2.2. Execute purchases for removable media used at NASIC.

2.2.3. Manage distribution of blank media.

2.2.4. Develop jointly with the Directorate of Security (NASIC/SO) the NASIC Media Accountability Program and associated training to mitigate vulnerabilities, threats and risk associated with the management of removable media.

2.2.5. Provide MAM services for the support directorates.

2.3. Information Assurance Office (NASIC/SCXS) will:

2.3.1. Manage the NASIC Media Accountability Program to mitigate vulnerabilities, threats and risk associated with the management of removable media.

2.3.2. Develop and disseminate NASIC Media Accountability Program training materials.

2.3.3. Develop and maintain policies and/or tools for providing media accountability program compliance for personnel without access to the automated tool.

2.4. Applications & Web Services Office (NASIC/SCPW) will:

2.4.1. Create and maintain a tool to automate the tracking and auditing of removable media.

2.4.2. Provide enhancements to the automated tools to improve usability.

2.5. Production Services (NASIC/SCOK) will:

- 2.5.1. Distribute optical media, example formats include: CDROM, CDRAM, DVD, DVDROM, DL-DVD, Blu-Ray, Mini-CD.
- 2.5.2. Manage pre-print blank media and distribute to MAMs.
- 2.5.3. Manage production media by performing the following actions:
 - 2.5.3.1. Ensure production media is registered.
 - 2.5.3.2. Mark each piece of media with a unique media identification value (generated by the media accountability tracking system) using disk labeling software, permanent marker or other approved method.
 - 2.5.3.3. Transfer registered production media to removable media users.

2.6. Infrastructure Branch (NASIC/SCOI) will:

- 2.6.1. Destroy hard drives in accordance with applicable guidance. Tapes, USB devices, and other media items are not handled by NASIC/SCOI.

2.7. Client Services Branch (NASIC/SCOS) will:

- 2.7.1. Collect and maintain user agreements.

2.8. Directorate of Security (NASIC/SO) will:

- 2.8.1. Develop jointly with the Directorate of Communications and Information (NASIC/SC) the NASIC Media Accountability Program and associated training to mitigate vulnerabilities, threats and risk associated with the management of removable media.
- 2.8.2. Investigate reported violations of this instruction.
- 2.8.3. Serve as the advisor on all security matters related to the NASIC Media Accountability Program.

2.9. Directorate of Plans and Programs (NASIC/XP) will:

- 2.9.1. Ensure the provisions of this instruction are included on NASIC contracts which require a visitor group security agreement.

2.10. Logistics Group (NASIC/LG) will:

- 2.10.1. Supervise all Document Disintegration System (DDS) Operations.
- 2.10.2. Inspect DDS operations to ensure compliance with governing directives including DoD 5200.1, *DoD Information Security Program and Protection of Sensitive Compartmented Information* AFSSI 5020, and AFI 31-401.
- 2.10.3. Purchase DDS equipment required for media destruction, with exception of hard drive destruction equipment, which is purchased and operated by SC.

2.11. Document Disintegration System Operators (NASIC/LGM) will:

- 2.11.1. Accept media marked for destruction according to established procedures as described in section 3.4. Media includes both optical discs and magnetic tapes. Hard drives are handled by NASIC/SCOI as described in section 2.6.

2.12. NASIC Lead Media Accountability Manager (LMAM) will:

2.12.1. Direct and manage the NASIC Media Accountability Program to include the management of training, scheduling, audits, and overall program compliance.

2.12.2. Collect USB devices for destruction and ship USB devices to NSA for official destruction.

2.13. NASIC Media Accountability Managers (MAM) will:

2.13.1. Follow the procedures as described in Section 3.2 through 3.5

2.13.2. Conduct quarterly audits and report findings to the LMAM.

2.13.3. Report media accountability issues to the LMAM and NASIC/SOO.

2.14. NASIC Media Accountability Administrators (MAA) will:

2.14.1. Follow the procedures as described in Section 3.2 through 3.5

2.14.2. Assist the MAMs.

2.15. Authorized Users are personnel that use media in the performance of their duties within the Center. Authorized Users must have a Secret or higher security clearance and a signed agreement. Authorized Users are accountable for their media and will:

2.15.1. Complete initial and annual NASIC Media Accountability Program training.

2.15.2. Complete and sign the user agreement.

2.15.3. Follow the procedures for receiving and transferring media as described in Section 3.2 and Section 3.3.

2.15.4. Ensure all media in their possession is registered and marked.

2.15.5. Retain positive control of all registered media in their account.

2.15.6. Report removable media accountability issues to their assigned MAM.

2.15.7. Turn-in all unneeded removable media to their MAM for destruction.

2.15.8. Out-process NASIC by transferring their owned media to other NASIC user(s) and/or by turning-in removable media to their assigned MAM for destruction.

3. PROCEDURES.

3.1. Media Use and Accountability.

3.1.1. Government issued removable media, such as media obtained at formal training or conferences/seminars, may only be used in performance of assigned duties. Any personal use of government issued removable media is prohibited. Personally owned removable media such as factory printed CDs/DVDs/Blu-rays are prohibited on all information resources.

3.1.2. Removable media may be connected to another information resource only when specifically authorized.

3.1.3. Removable media users are responsible for registering, tracking, and initiating transfer and turn-in for all media in their possession.

3.1.4. Removable media must be clearly marked in accordance with applicable SF Form classification labels by the NASIC user responsible for the removable media. If the removable media is stored in a facility where classified information is processed, and it is not so marked or validated as blank by the appointed security officers, e.g., not in factory-sealed packages, then it must be protected at the highest level of classification processed within that facility until appointed security officers have reviewed and marked the removable media consistent with the classification guide.

3.1.4.1. Blank media will enter NASIC through SCOK only. Users will receive SCOK pre-printed blank media through their MAM.

3.1.5. Removable media may be used to transfer information between security domains only when an appropriate Cross-Domain Solution (CDS) is not available. If removable media is used to transfer data, the procedures in the Information Assurance Data Transfer Handbook must be followed.

3.1.6. Removable media users are responsible for reporting lost media to their MAM.

3.1.7. The MAM is responsible for overseeing the tracking, distribution, transferring and decommissioning of user's media.

3.2. Media Receipt.

3.2.1. Internal Receipt of unregistered removable media. Upon receipt of unregistered removable media, the media users will:

3.2.1.1. Register media in the media accountability tracking system.

3.2.1.2. Mark media with a unique media identification value using permanent marker or other approved method in such a way that the label is legible and not separated from the media. Unique media identification values are generated through the media accountability tracking system.

3.2.1.3. Scan media for malicious code using approved standalone workstation.

3.2.1.4. Mark media with classification of media contents, title, classification of title, and other security markings as applicable utilizing the appropriate SF Form labels.

3.2.1.5. Properly protect, store, and handle media commensurate with its classification level.

3.3. Media Custodial Transfer.

3.3.1. Internal Transfer. Media must be previously registered in the media accountability tracking system.

3.3.1.1. Conduct a transfer transaction of media. This transaction is tracked through the media accountability tracking system. A transfer is not complete until both parties accept the transaction.

3.3.1.2. Physically transfer media to assigned user.

3.3.2. External Transfer. Media must be previously registered in the media accountability tracking system:

3.3.2.1. The transferring agent will ensure the external transfer is recorded.

3.3.2.2. Media user physically transfers media to authorized user via approved method in accordance with SCOK's "NASIC Collateral Mail Center's Customer Guide", SCOK's "Customer Guide to Transfer SCI Material", and applicable security directives.

3.4. Media Turn-in and Destruction.

3.4.1. Media users will turn in unneeded media to assigned MAM for destruction.

3.4.2. MAM will update the associated record(s) in the media accountability tracking system to identify that each piece of submitted media has been marked for destruction.

3.4.3. MAM will sort media by type (CDs, DVDs, hard drives, magnetic tape, etc).

3.4.4. After the associated record has been updated in the media accountability tracking system, the MAM will place the media in a properly labeled classified waste bag or container separated by media type. The MAM will mark the waste bag or container in accordance with NASICI 31-103, *Security Operations*.

3.4.5. MAMs will turn in all media marked for destruction (with the exception of hard drives which are given to SCOI) to the DDS Operators (NASIC/LGM) for media destruction.

3.4.6. DDS Operators (NASIC/LGM) will destroy or transfer removable media in accordance with DoDM 5200.1, *DoD Information Security Program: Protection of Classified Information*, AFSSI 5020, and AFI 31-401.

3.4.7. DDS Operators will segregate, store, and transfer or destroy the media according to applicable directives.

3.4.8. DDS Operators will notify branch supervisor when unauthorized materials are discovered in classified waste bag. Branch supervisor will have prerogative to inform leadership of any negative trends that might jeopardize the safety of DDS personnel or cause damage to the equipment.

3.5. Blank CD/DVD/Blu-ray Disc Management.

3.5.1. Authorized Users may request blank discs through their MAM.

3.5.2. Production Services (SCOK) will distribute preprinted blank discs of the requested type to the MAM.

3.5.3. The MAM will distribute the disc(s) to the Authorized User by performing the following actions:

3.5.3.1. Ensure each piece of blank media is registered prior to dissemination to the requesting user.

3.5.3.2. Ensure the unique media identifier mark (media accountability tracking system generated media ID) is on each piece of media being transferred.

3.5.3.3. Ensure the user completes the transfer transaction process.

3.6. Media Misuse or Compromise.

3.6.1. Suspected misuse or compromise of removable media or information contained therein must be reported to an appropriate security officer and incident response team(s)

in accordance with NASIC policy. Such incidents may be deemed a security infraction or violation.

4. TRAINING.

4.1. Removable Media Users Training.

4.1.1. Removable media users must undergo initial and annual NASIC media accountability training. This training will include an overview of this instruction, user training for the media accountability tracking system and an overview of the specific requirements of ICS 500-18.

4.2. Media Accountability Manager Training

4.2.1. The LMAM will provide Media Accountability Program training to new MAMs when assigned.

AARON M. PRUPAS, Colonel, USAF
Commander

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

AFI 31-401, *Information Security Program Management*, 30 January 2013

AFI 33-324, *The Air Force Information Collections and Reports Management Program*, 6 March 2013

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSSI 5020, *Remanence Security*, 15 April 1991

AFISRAI 31-402, *Disintegration and Destruction of Classified Material and Media Degaussing*, 29 July 2011

AFPD 33-3, *Information Management*, 8 September 2011

DoD 5200.1, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, 13 Jun 2011

DoDM 5200.1, *DoD Information Security Program: Protection of Classified Information*, 19 March 2013

ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation*, 15 September 2008

ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010

ICS 500-18, *Removable Media Management*

NASICI 31-106, *Portable Electronic Devices (PEDS)*, 8 June 2012

NASICI 31-103, *Security Operations*, 12 August 2012

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Center

AFRIMS—Air Force Records Information Management System

ANG—Air National Guard

CDS—Cross-Domain Solution

DDS—Document Disintegration System

DoD—Department of Defense
IAW—In Accordance With
ICD—Intelligence Community Directive
ICS—Intelligence Community Standard
LMAM—Lead Media Accountability Manager
MAA—Media Accountability Administrators
MAM—Media Accountability Manager
OPR—Office of Primary Responsibility
PED—Personnel Electronic Device
RDS—Records Disposition Schedule
SSD—Solid State Drive

Attachment 2

MEDIA ACCOUNTABILITY MANAGER APPOINTMENT LETTER TEMPLATE

Figure A2.1. Media Accountability Manager Appointment Letter.



DEPARTMENT OF THE AIR FORCE
NATIONAL AIR & SPACE INTELLIGENCE CENTER (AF ISR AGENCY)
WRIGHT-PATTERSON AFB OHIO

Date

MEMORANDUM FOR NASIC/SCXS

FROM: Enter Office Symbol

SUBJECT: Appointment of Media Accountability Personnel

1. The following individuals have been appointed as Media Accountability Managers (MAMs) as indicated below:

<u>OFFICE</u>	<u>NAME</u>	<u>PHONE</u>	<u>Permissions Level</u> (2-3-4 letters managed)

2. The following individuals have been appointed as Media Accountability Administrators (MAAs) as indicated below:

<u>OFFICE</u>	<u>NAME</u>	<u>PHONE</u>	<u>Permissions Level</u>

3. The individuals named above will perform their duties in accordance with NASICI 33-201 and ICS 500-18. This letter supersedes all previous appointments. If you have any questions, please call: enter commander's DSN.

Commander's Signature Block

"Freedom Through Vigilance"