

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



NASIC INSTRUCTION 31-107

**11 AUGUST 2010
Certified Current 1 June 2012
SECURITY**

**MULTI-FUNCTION DEVICES SECURITY
OPERATIONS AND PROCEDURES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications 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/SCXS

Certified by: NASIC/SCX (Mr. O'Brien)

Supersedes: NASICI31-107, 1 May 2006

Pages: 5

This instruction establishes policies and procedures governing the issuance, control and connectivity of multi-function devices (MFDs) on the NASIC's corporate networks (JWICS, SIPRNET and NIPRNET) to comply with the security and operation standards in the *Joint DoDIIS/Cryptologic SCI Information Systems Security Standards*, DoDD8500.1, *Information Assurance*, and DoDI8500.2, *Information Assurance Implementation*. This publication applies to all NASIC civilian and military personnel, contractors, as well as all Air Force Reserve Command (AFRC) Units and Air National Guard (ANG) Units assigned to NASIC. 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 Form 847s from the field to NASIC Publications Office (NASIC/SCOK), 4180 Watson Way, Wright-Patterson AFB, OH 45433-5648 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/gcss-af61a/afirms/afirms/>. Contact supporting records managers as required. 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. POLICY: All MFDs must meet network certification and accreditation, and TEMPEST requirements.

1.1. Use AF Form 3215, *SC IT Requirements Document*, (see NASICI 33-108), for all new requests for multi-function devices.

1.2. All MFDs must meet the same certification and accreditation requirements as the network they are installed on.

1.2.1. All MFD will be labeled with the appropriate SF 710, SF 707 or SF 712, *ADP Media Classification Labels*, according to the level of classification printed, copied, scanned, etc. or network connection.

1.3. MFDs connected to a NASIC network will process at the same accredited classification level as the network.

1.4. MFDs will have all hard drives removed when removed from the facility. If Random Access Memory (RAM) is a part of the configuration, information stored in RAM must be purged when the device is unplugged.

1.5. Phone line connections are prohibited.

1.6. Modem chips will be removed and/or disabled to eliminate the possibility of transmitting both facsimiles and data.

2. APPLICABILITY: These procedures apply to all users of MFDs within the NASIC facility. The facility is comprised of all NASIC spaces under the oversight of NASIC Information Assurance Manager (IAM).

3. PROCEDURES:

3.1. It is necessary to purchase MFDs outright (not lease them) in order to comply with security requirements, since these devices could have internal electronic memory components. Maintain absolute control of all electronic parts that contain a memory/data remanence capacity, and have a maintenance contract that provides for maintenance support by cleared personnel.

3.2. Printed circuit boards/memory boards and components that could possibly contain residual information are to be destroyed as classified trash.

3.3. All communications ports not specifically required for networked or contractual maintenance must be removed or permanently disabled. Only hardwired connections are permitted (no infrared, radio frequency, or audio communications). This provision must be included in the purchase contract.

3.4. If laptops are required for diagnostics, the NASIC IAM must approve their purchase and be provided the means for securing these systems within NASIC facilities. Wireless is not authorized and only minimum software present to perform required diagnostics.

3.5. Maintenance records will be maintained by maintenance contractors.

3.6. MFDs have a scan/e-mail function that allows users to attach a document and send it via e-mail. The email is only authorized to be sent to the user performing this function. This function can replace faxing. To use this function, you must have an account on the network, which can be requested through the Communications Focal Point (CFP)/SCOS/71248/R2517 or R2345.

3.6.1. NIPRNET connected MFDs with scan/e-mail function will have a stop sign sticker attached to the CAC card reader (attached to the MFD) reminding users to perform a "two-person" check of the information before scanning.

4. RESPONSIBILITIES:

4.1. The NASIC IAM, in conjunction with the DAAR, shall:

4.1.1. Ensure MFDs installed in NASIC facilities have the appropriate certification and accreditation documentation and authorizations.

4.2. Group Commander/Directors shall:

4.2.1. Appoint equipment custodians as required by AFI 33-112, *Information Technology Hardware Asset Management*, who will ensure equipment is entered into the NASIC equipment inventory.

4.3. The NASIC TEMPEST/EMSEC Manager shall:

4.3.1. Ensure all MFDs meet the TEMPEST standards of AFISRA 33-203, *Air Force Intelligence, Surveillance and Reconnaissance Agency TEMPEST and Emission Security Program*, and TEMPEST/1-92, *National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM)*.

4.4. Equipment Custodians shall:

4.4.1. Ensure appropriate classification and usage labels are properly affixed to the equipment.

4.4.2. Ensure MFDs are included in the NASIC equipment inventory.

Note: AFVA 205-9 (Classified Reproduction Rules) and AFVA 205-8 (Stop, Do Not Use This Machine for Classified Reproduction Stop) have been **RESCINDED**.

Note: Monthly meter readings are not required for MFDs.

4.5. Users shall:

4.5.1. Report all IS security incidents to your Office Security Manager (OSM)/Staff Agency Security Manager (SASM) and the Security Office during duty hours and the Communications Focal Point after duty hours.

4.5.2. Submit CFP Service Requests for all maintenance on MFDs (or call the Communications Focal Point, SCOS/71248/R2517 or R2345, Room 8292).

4.5.3. Read/review this instruction (NASICI 31-107) annually and take any training required.

4.6. LG is responsible for purchasing paper supplies for MFDs connected to the corporate networks.

4.7. SC is responsible for purchasing ink supplies and installing and removing MFDs to/from the corporate networks.

4.8. SC is responsible for removing all hard drives before removing an MFD from the facility.

5. PRESCRIBED AND ADOPTED FORMS

5.1. Adopted Forms:

AF Form 3215, *SC IT Requirements Document*

SF 710, Unclassified Label for ADP Media in SCI Facilities

SF 707, Secret ADP Media Classification Label

SF 712, Classified SCI ADP Media Classification Label

AF Form 847, Recommendation for Change of Publication

KATHLEEN C. SAKURA, Colonel, USAF
Commander

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

JDCSISSS, “Joint DoDIIS/Cryptologic SCI Information Systems Security Standards.”

Director of Central Intelligence Directive (DCID) 6/3, “Protecting Sensitive Compartmented Information Systems within Information Systems.”

AFI 33-203, “Emission Security.”

NASIC 33-108, “NASIC Strategic IT Management”

ABBREVIATIONS AND ACRONYMS

IS-Information Systems.

TERMS

DAAR—Designated Approving Authority Representative or Designated Accrediting Authority Representative (NASIC/SC). The official with authority to formally assume responsibility for operating a system (or network) at an acceptable level of risk.

Digital Copier—Computer-based, network-capable devices with processors, memory, hard-drives, fax modem capability, and image retention components.

IAM—The Information Assurance Manager is assigned to NASIC/SCXS and is responsible for automated information security management for all AIS in the NASIC facility.

MFD— Multi-function devices have the capability to copy, print, and scan.