NATIONAL APPEALS DIRECTIVE	**No.** NAD-07-01
SUBJECT: Control and Protection of Electronic and Non-Electronic Sensitive Security Information	**APPROVED:** **DATE:** July 12, 2007

1. Purpose

This policy sets forth guidance and requirements for National Appeals Division (NAD) employees for safeguarding unclassified Sensitive Security Information (SSI) against unauthorized use or disclosure. The guidelines in this policy conform to U.S. Department of Agriculture (USDA) requirements set forth in DM 3525-003 (Chapter 5, Part 3, Telework & Remote Access Security) for safeguarding SSI that is considered low risk.

2. References

Title 7, Code of Federal Regulations (7 C.F.R.) Part 1

Department Manual 3505-001 (Part 2, Part 3, Computer Incident Response Procedures)

Department Manual 3525-003 (Chapter 5, Part 3, Telework & Remote Access Security)

Department Manual 3535-001 (C2 Level of Trust)

Department Regulation 3440-002 Appendix A, Part 6

Department Regulation 4080-811-002 (Appendix A, Teleworking Program)

3. Responsibilities

All NAD employees are responsible for protecting SSI from unauthorized disclosure and for reporting SSI incidents. Additionally, employees will take measures to facilitate data integrity and disaster recovery, by either deleting SSI when no longer useful or using secure network storage for electronic information that is no longer active.

4. Policy

This policy establishes controls that apply to NAD employees who transmit, store, and gain access to NAD SSI at NAD offices, other locations, or while on travel. In general, SSI includes unclassified information of a sensitive nature that, if publicly disclosed, could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity. USDA DR 3440-002 Appendix A, Part 6 provides definitions for SSI that include employee personal information. In addition to the types of SSI defined by the USDA directive, NAD employees will treat as SSI all information contained in a system of records defined under the Privacy Act, such as information contained in NAD case records and NADTrack.

5. Requirements

USDA requires specific data encryption measures for employees that telework and access USDA systems from remote locations. In accordance Department Manual 3525-003 (Chapter 5, Part 3, Telework & Remote Access Security), NAD employees will use data encryption for all electronic SSI, if working from locations that are not with NAD Regional or Headquarters offices. Acceptable forms of encryptions are all NAD-provided encrypted portable memory devices and encryption software, both local and network. Consistent with the requirements, NAD employees stationed at a Regional or Headquarters office, who access systems operated on the USDA network are not required to encrypt electronic data.

The following requires NAD employees to implement security measures in specific situations. Unless otherwise identified, employees will ensure that *one-layer* of security will protect SSI. The *one-layer* can be either physical, electronic, or within one's personal control (within line of sight).

Regional Offices and Headquarters Office

- Electronic SSI: No data encryption required: During normal duty hours, the standard computing environment exists. During off-duty hours, users log off systems; office spaces are locked or secured by access cards / keys.
- Non-Electronic SSI: During duty and off-duty hours, no additional security measures are required.

Other Locations

- Electronic SSI: Employees encrypt data with NAD-provided encrypted portable memory devices and encryption software; for SSI no longer used, employees will store data on USDA network storage.
- Non-Electronic SSI: Employees secure files in locking file cabinets; access to workspace is controlled by lock or card access.
- Electronic Devices: All portable electronic devices, including Digital Voice Recorders (DVR) and laptop computers, will be secured in locking file cabinets during off-duty hours.

On Travel

- Electronic SSI: Employees encrypt data on laptops with NAD-provided encrypted portable memory devices or encryption software. All portable electronic devices, including Digital Voice Recorders (DVR) and laptop computers, with SSI will remain in employee's personal control or a locked vehicle, meeting or hotel room, or container.
- Non-Electronic SSI: Employees keep SSI within personal control, or ship hard copy information through a secure carrier such as FedEx, United State Postal Service, DHL, or UPS. An employee keeps non-electronic SSI in a locked vehicle, hotel room, or container.

Electronic Storage

- Employees will delete or save electronic SSI no longer active onto the USDA network storage provided by NAD. An employee may store any other work related data on the network drive for safeguarding.

Data Disposal

- Employees disposing of non-electronic SSI will shred data prior to being placed in recycling bins or in trash.
- All electronic media such as: compact disks, floppy disks, zip disks, and USB memory drives will be destroyed. All hard disks will be returned to the NAD Information Technology Specialist.

Security Incident Notification

- Security incidents include the loss of both electronic and non-electronic SSI, loss of electronic devices suspected of having SSI stored on the device, and all other actions deemed harmful to the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity.
- Within 24 hours of detecting a security incident, an employee will submit a completed form NAD-0307, Security Incident form, to the NAD Information Systems Security Officer (ISSO). A copy of the form is attached to this policy.
- If the security incident prevents an employee from completing the NAD-0307 form, the employee's respective Regional or Headquarters office is responsible for completing the form. Employees are responsible for immediately notifying their respective supervisors of the security incident.
- If an employee suspects an electronic messaging (email) attack, the employee will not send an incident notification though any email system. Regional and Headquarters offices will become responsible for the incident notification. Employees are responsible for immediately notifying their respective supervisors of the security incident.

6. Training

- All employees are required to complete USDA Cyber Security training on information technology security literacy and privacy on an annual basis. The training requirements will be promulgated through the authority of Planning, Training, and Quality Control (PTQC) section within NAD.

DISPOSAL DATE:	**DISTRIBUTION:**
When updated or superseded	All NAD employees

SECURITY INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED WITHIN 10 DAYS OF DISCOVERY OF A SECURITY INCIDENT. (The affected individual is responsible for gathering pertinent information and completing this form.)

I. GENERAL INFORMATION [Section I, must be completed entirely]

Primary Contact: ____________________
E-Mail Address: ____________________
Telephone number: ____________________
Cell Phone Number: ____________ FAX number: ____________
Pager number: __________
Physical Location of Incident: ____________

II. HOST INFORMATION [Section II, must be completed entirely]

Please provide information about all host(s) involved in the incident. Each host shall be listed separately.

Computer name: ____________________
IP Addresses: ____________________
Computer hardware: ____________________
Operating System and version: ____________________
Where on the network is the involved host? – (Home, Shared Lease space, Regional and Headquarters):____________________
Nature of the information at risk on the involved host – NAD Case Files, Personnel, Financial, Privacy Act.

____

Time zone of the involved host: ____________
Was the host the source or victim of the attack or both:

____

Was this host compromised as a result of the attack? ○Yes ○No
Hours system down__________

III. INCIDENT CATEGORIES

All categories applicable to the incident shall be documented.

Data Loss(es): ____________________

Hardware Loss(es): ____________________

Intruder gained "access" ○Yes ○No

Cracked password ○ Yes ○ No
Easily-guessable password ○ Yes ○ No
Misuse of host(s) resources ○ Yes ○ No

IV. SECURITY TOOLS

At the time of the Incident, was the individual using any of the following? ○ Yes ○ No
Banner Warning: ____________________
Authentication/Password tools: ______________
Anti-Virus tools: ____________________________________
Other tools: data encryption, hardware encryption(s)

Were logs being maintained: If so, please describe.

____

V. DETAILED INCIDENT DESCRIPTION

Detailed Incident Description: This should be as detailed as possible, especially when writing lesson learned or after the incident follow-up report. Please use separate sheets of paper to address the following:

A. Duration of Incident:

B. How was the incident discovered?

C. Method(s) used by intruders to gain access to host(s):

D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections:

E. Hidden files/directories:

F. Source of attack (if known):

G. Did system contain classified/sensitive information? What type?

H. Was the information compromised?

Submit by Email | Print Form