CNSS Advisory Memorandum
Information Assurance 01-10
December 2010

Advisory Memorandum

Reducing the Risk of Removable Media in National Security Systems

CNSS Advisory Memorandum
Information Assurance 01-10

NATIONAL MANAGER

FOREWORD

1. Using removable media presents serious risks to the security of National Security Systems (NSS). Risks include the loss/compromise of data and the unauthorized transfer of classified national security information. This Advisory Memorandum establishes additional criteria for using removable media with NSS. (For additional information please reference CNSSP 26, “National Policy on Reducing the Risk of Removable Media” (Reference a).)

2. I encourage dissemination of the contents of this Advisory Memorandum to all Government entities, contractors, or agents engaged in Information Assurance (IA) activities associated with NSS.

3. In addition to this Advisory Memorandum, further configuration guidance is available to assist operators and users of NSS with mitigating the threats named herein. The National Security Agency (NSA) is available to provide technical consulting to CNSS members to assist in threat mitigation. For further information, please contact your IAD Client Advocate office at (410) 854-4790 or call the CNSS at (410) 854-6805.

4. Additional copies of this Advisory Memorandum may be obtained at www.cnss.gov.

FOR THE NATIONAL MANAGER:

//s//

DEBORA A. PLUNKETT

Advisory Memorandum
Reducing the Risk of Removable Media in National Security Systems

SECTION I - APPLICABILITY

1. This Advisory Memorandum is issued under the authority of Reference b and applies to all Executive Departments and Agencies and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in Reference c.

SECTION II – BACKGROUND

2. The use of removable media resulting in unauthorized data transfers on classified networks is a serious risk to the security of NSS and, thus, of great concern to all Executive Departments and Agencies. In addition to the requirements found in Reference a, the following guidelines are intended to reduce and mitigate the unauthorized release of sensitive or classified data from NSS and thereby increase their security. This guidance is based on current best practices for limiting the security risks of using removable media on NSS. As stated in Reference a, a layered defense that addresses training, technology, procedures and personal accountability is encouraged to manage risks to NSS that result from the use of removable media.

3. Removable media is defined as portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, and which is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), DVDs, thumb drives, pen drives, Personal Digital Assistants (PDAs) (to include smart phones) and similar USB storage devices.

SECTION III – GUIDANCE

4. Operators and users of NSS should begin using physical configuration, software settings, a capability such as a Host-Based Security System (HBSS) (a DoD capability designed to address exploit traffic on network hosts), or any combination of these, to disable all “write” privileges for all forms of removable media devices on NSS. Ensure all removable media is prohibited from use on all NSS workstations unless specifically authorized by appropriate authority.

5. The following functions should be performed to prevent unauthorized data transfers from occurring on NSS:

a) Direct all personnel to cease data transfers on NSS unless approved by appropriate authority and until adequate technical measures are put in place.

b) Implement technical capabilities to limit write functionality (Windows, Mac, Linux, Unix, etc.) to only those authorized servers, systems, and stand-alone workstations which have a valid operational need and mission requirement.

c) Provide written authorization to the organization's Information Assurance Manager (IAM) for each user approved to use removable media.

d) Provide written authorization to the organization's Information Assurance Manager (IAM) for each server, system, and stand-alone workstations approved to use removable media.

e) Set guidelines and procedures for approval/disapproval of removable media use on NSS.

f) Write access auditing should be enabled for all removable USB, Firewire, Windows Portable Devices (WPD) (including MP3 players and PDAs) and PC Cards. In addition, this audit log should be reviewed on a weekly basis to ensure only authorized users are performing these write functions, and looking for any abnormal large file transfers to these media types.

g) Identify and report violations of requirements and procedures identified in this document to the organization's senior leadership to determine needed corrective action.

h) Ensure the acceptable use and approval process for the use of removable media devices is included in the organization's network user training programs.

i) Maintain a list of all personnel and systems that have been authorized to use removable media devices on NSS within their environment, and review and update on a regular basis.

j) Conduct random and periodic inspections to ensure compliance with organization policy and report findings to appropriate authorities.

6. Operators and users of NSS should establish a program for authorized personnel responsible for conducting "read/write/download" data transfers within their area of responsibility. The authorized personnel should be required to:

a) Agree to comply with organizationally-directed rules for conducting data transfers on NSS via user agreement.

b) Acquire prior written approval from the appropriate authority before conducting data transfers to or from NSS.

c) Only use removable media in manner specifically authorized by the appropriate authority.

d) Identify and report any violations within their authority.

e) Physically protect removable media used in NSS.

f) Report lost/stolen removable media used in NSS.

g) Ensure all data transfers on NSS are authorized by appropriate authority.

h) Only perform approved data transfer requests.

i) Request a read receipt verifying only the intended recipient has received the transferred data.

j) Record all data transfers performed and provide status to the organization’s leadership every 30 days.

7. Operators and users should label and use removable media devices as follows:

a) Ensure all removable media devices are clearly labeled and traceable by a bar code tag or a serial number to an assigned authorized individual.

b) For small devices, provide clearly labeled lanyards or other attached external marking to reduce the risk of misplacement or theft.

c) Ensure proper classification markings, storing, transportation, and destruction of all removable media.

d) Ensure removable media that are US Government-owned have been purchased from an authorized and trusted source.

e) Scan removable media for malicious software using approved methods before introducing the media into any NSS.

f) Limit use of removable media to authorized personnel with appropriate training.

g) Sanitize, destroy, and/or dispose of removable media used in NSS in accordance with an approved method, if the media are no longer required.

h) Implement a program to track, account for, and safeguard all acquired removable media, as well as to track and audit all data transfers.

i) Conduct both scheduled and random inspections to ensure compliance with applicable guidance regarding the use of removable media.

j) Implement system-level software restriction rules in order to significantly reduce the potential for malicious code execution by removable media.

k) Maintain a consistent operating system image that reflects the enterprise's secure default configuration for all software that the enterprise uses.

8. Operators and users of NSS are strongly recommended to:

a) Implement this guidance, evaluate its effectiveness and share lessons learned and best practices with other operators and users of NSS.

b) Ensure resources are available to implement this guidance.

c) Incorporate the content of this guidance into user training and awareness programs.

d) Publish and implement emergency response procedures.

9. Further configuration guidance is available to assist operators and users of NSS with mitigating the threats named in this Advisory Memorandum. The National Security Agency (NSA) is available to provide technical consulting to CNSS members to assist in threat mitigation. For further information, please contact your IAD Client Advocate office at (410) 854-4790 or call the CNSS at (410) 854-6805.

SECTION V – REFERENCES

10. The following references apply to this directive:

a) CNSSP No. 26, "National Policy on Reducing the Risk of Removable Media," dated November 2010.

b) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," dated July 5, 1990.

c) CNSS Instruction No. 4009, "National Information Assurance Glossary," dated April 26, 2010.