CNSSP No. 26
November **2010**

National Policy on Reducing the Risk of Removable Media

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

CHAIR

FOREWORD

Recent incidents, regarding malicious software on United States Government (USG) networks, demonstrate the inherent risks of using removable media. Risks include the loss of data and system availability, integrity, and confidentiality. This policy establishes the criteria for using removable media with National Security Systems (NSS). Removable media are widely used and it is important to note that the essential problem is not with the media themselves, but with the inability of networks in their typical default conditions to prevent malicious code from executing. The use of removable media can be allowed on NSS, provided safeguards are employed. To achieve enterprise-wide security, the goal is to include removable media in the enterprise approach to risk management in accordance with the general risk management policy of the Committee on National Security Systems Policy (CNSSP) No. 22 (Reference a).

CNSSP No. 26 is based on current best practices for limiting the security risks of using removable media. The policy will be updated as technology and best practices evolve. In case of policy overlap or conflict, Departments and Agencies should adhere to the most restrictive approach that allows mission accomplishment. This policy does not address procedures for moving information from NSS to unclassified information systems using removable media. Refer to the appropriate Department or Agency policies for such guidance.

Additional copies of this policy may be obtained at www.cnss.gov.

/s/
Cheryl J. Roby
Acting

CNSS Secretariat (I923)
National Security Agency * 9800 Savage Road * Suite 6716 * Ft Meade MD 20755-6716
cnss@radium.ncsc.mil

NATIONAL POLICY ON REDUCING THE RISK OF REMOVABLE MEDIA

SECTION I – PURPOSE

1. This policy establishes the criteria for the use of removable media in NSS. It is based on current best practices for reducing risks inherent with the use of the media. Protecting NSS and their associated information infrastructures requires keeping pace with evolving technology and the efforts of adversaries to penetrate, disrupt, exploit, or destroy critical elements of NSS. A layered defense addressing training, technology, procedures, and personal accountability is required to manage risks to NSS that result from the use of removable media.

SECTION II – AUTHORITY

2. This policy derives from certain responsibilities delegated both to the CNSS, and to the National Manager for National Security Telecommunications and Information Systems Security by National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems (Reference b).

SECTION III - SCOPE/APPLICABILITY

3. This policy applies to all Federal Departments and Agencies, including their supporting contractors and agents that operate, use, or manage NSS. Nothing in this policy should be interpreted as altering or superseding the existing authorities of the Director of National Intelligence.

SECTION IV – POLICY

4. While removable media offer a convenient way to transfer data from one information system to another, their use significantly increases the risk of virus infection, spread of malicious software, and data spillage. Therefore, Departments and Agencies should limit the use of removable media on NSS to those operational environments that require these media to achieve mission success and not simply for convenience. Further, Departments and Agencies should make maximum use of properly configured and secured network shares, web portals, or cross domain solutions to transfer data from one location to another. Departments and Agencies may prohibit the use of removable media as they deem appropriate.

5. If removable media are required, Departments and Agencies should use the following mitigation techniques, at a minimum, to reduce risks to NSS.

a. Craft, promulgate, and implement risk management policies concerning the use of removable media.

b. Restrict use to removable media that are USG-owned, and have been purchased or acquired from authorized and trusted sources.

c. Scan removable media for malicious software using a Department or Agency approved method before introducing the media into any operational systems.

d. Prohibit automatic execution of any content by removable media unless specifically authorized by the cognizant Chief Information Security Officer.

e. Implement access controls (e.g. read/write protections) for the removable media, as appropriate.

f. Encrypt data on removable media using, at a minimum, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.

g. Verify that the media contain only the minimum files that are necessary, and that the files are authenticated and scanned so that they are free of malicious software. This should be completed prior to the media being inserted into NSS. Use a verification process authorized by the Department or Agency for Assured File Transfer. This verification process should be performed on a non-networked, stand-alone machine.

h. Mark or label all removable media with the highest security classification, of any system into which the media have been inserted.

i. Prohibit use of the removable media for data transfer from the destination network back to the source network, or to any other network, unless the media have been erased/re-formatted, and re-scanned.

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

k. Sanitize, destroy, and/or dispose of removable media that have been used in NSS in accordance with a Department or Agency approved method, when the media are no longer required.

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

m. Conduct both scheduled and random inspections to ensure compliance with Department/Agency promulgated guidance regarding the use of removable media.

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

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

6. Additional guidance is available at www.nsa.gov/ia/guidance.

7. These mitigation techniques to reduce risk will only be effective if they are implemented in accordance with proper Department/Agency procedures and oversight, including accountability for violations.

SECTION V – RESPONSIBILITIES

8. Heads of Departments and Agencies are responsible for:

a. Implementing this policy, evaluating its effectiveness, and sharing lessons learned and best practices as they evolve.

b. Ensuring resources are available to implement this policy.

c. Incorporating the content of this policy into user training and awareness programs.

d. Publishing and implementing emergency response procedures.

SECTION VI – REFERENCES

9. The following references apply:

a. CNSS Policy No. 22, Information Assurance Risk Management Policy for National Security Systems, February 2009

b. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, July 5, 1990

c. CNSS Instruction No. 4009, "National IA Glossary", April 26, 2010

SECTION VII – DEFINITIONS

10. The definitions contained in Reference c apply to this policy.