Committee on National Security Systems

CNSS Policy No. 18
June 2006

National Policy
On
Classified Information Spillage

This document prescribes minimum standards.
Your department or agency may require further implementation.

Committee on National Security Systems

CNSS Policy No. 18

CHAIR

FOREWORD

1. The handling of "classified national security information" spillage is a Government-wide challenge. Current national policy does not provide guidance for handling such incidents. With the continued and ever increasing interconnection of information systems (ISs), the extent and risk of classified information spillage increase dramatically.

2. This policy provides a framework for the consistent handling of spillage of classified information onto an unclassified IS, or higher-level classified information onto a lower level classified IS, to include non-government systems.

3. Additional copies of this policy may be obtained from the Secretariat or the CNSS Website - www.cnss.gov.

/s/
John G. Grimes

CNSS Secretariat (I01C)
National Security Agency
9800 Savage Road * STE 6716 * Ft Meade MD 20755-6716
(410) 854-6805
UFAX: (410) 854-6814
cnss@radium.ncsc.mil

Committee on National Security Systems

CNSS Policy No. 18

NATIONAL POLICY
ON
CLASSIFIED INFORMATION SPILLAGE

SECTION I – SCOPE

1. This policy applies to the spillage of classified national security information[1] on any IS, be it government or non-government systems. It provides a framework for the consistent handling of the spillage of classified national security information onto an unclassified IS, or higher-level classified national security information onto a lower level classified IS or onto an IS not accredited to the appropriate level.

2. Nothing in this policy shall alter or supersede the existing authorities of the Director of National Intelligence (DNI).

SECTION II – REFERENCES

3. References are listed in ANNEX A.

SECTION III – DEFINITIONS

4. Definitions in Reference f. apply to this policy; additional terms are defined in ANNEX B.

SECTION IV – POLICY

5. All government departments, agencies, and their contractors (consistent with Reference b.) that own or operate IS used to collect, generate, process, store, display, or transmit/receive national security information shall establish policies and procedures for handling classified information spillage. Reference e. applies to all contractors. Information concerning a spillage incident shall be protected from disclosure consistent with References a. through d. (and as prescribed in the process below). These policies and procedures shall ensure that all classified information spillage, either onto an unclassified IS, or to an IS with a lower level of classification, or onto an IS not accredited to the appropriate level, is immediately:

[1] Classified national security information is defined in Reference a.

a. Reported to the appropriate authorities. These authorities shall minimally include the information owner, the Information Assurance Manager (IAM)/Information System Security Manager (ISSM), the Activity Security Manager, and the responsible incident response center in accordance with [provisions of] Reference c.

b. Isolated and contained to minimize damage and to preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counter intelligence purposes. All affected media will be considered classified at the same level as the spilled information until government departments, agencies, and their contractors have executed their process for information spillage.

c. Verified by the information owner, who shall also ensure an assessment is conducted, as appropriate, in accordance with References a. and d.

6. Decisions regarding mitigation procedures, including disposition of affected media (i.e., sanitization, physical removal, or destruction), shall realistically consider the potential harm that may result from compromise of spilled information.

SECTION V – RESPONSIBILITIES

7. Heads of Federal Departments and Agencies shall:

a. Ensure compliance with the requirements of this policy.

b. Ensure resources are available to implement this policy.

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

Encl:
ANNEX A REFERENCES
ANNEX B DEFINTIONS

ANNEX A

REFERENCES

a. Executive Order 12958, "Classified National Security Information," 28 March 2003, as amended.

b. Executive Order 12829, National Industrial Security Program, 16 September 1993, as amended.

c. Public Law 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act of 2002, 17 December 2002.

d. CFR Part 2001, "Classified National Security Information," (Information Security Oversight Office Directive No. 1), 22 September 2003.

e. Department of Defense 5220.22-M, "National Industrial Security Program Operating Manual," 28 February 2006. [2]

f. CNSS Instruction No. 4009, "National Information Assurance (IA) Glossary," May 2003 or its successor.

[2] Only applies to U.S. Government Contractors with classified contracts.

Committee on National Security Systems

ANNEX B

DEFINTIONS

Terms used in this policy are defined in Reference f. with the exception of the following:

ACTIVITY SECURITY MANAGER: Individual specifically designated and responsible for ensuring that classified information is properly handled during its entire lifecycle. This includes ensuring it is appropriately stored, processed, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure the appropriate corrective action is taken.

DESTRUCTION: Obliteration or disintegration by physically destroying the media (e.g., shredding, degaussing, smashing, grinding, melting…) so that the media cannot be reused.