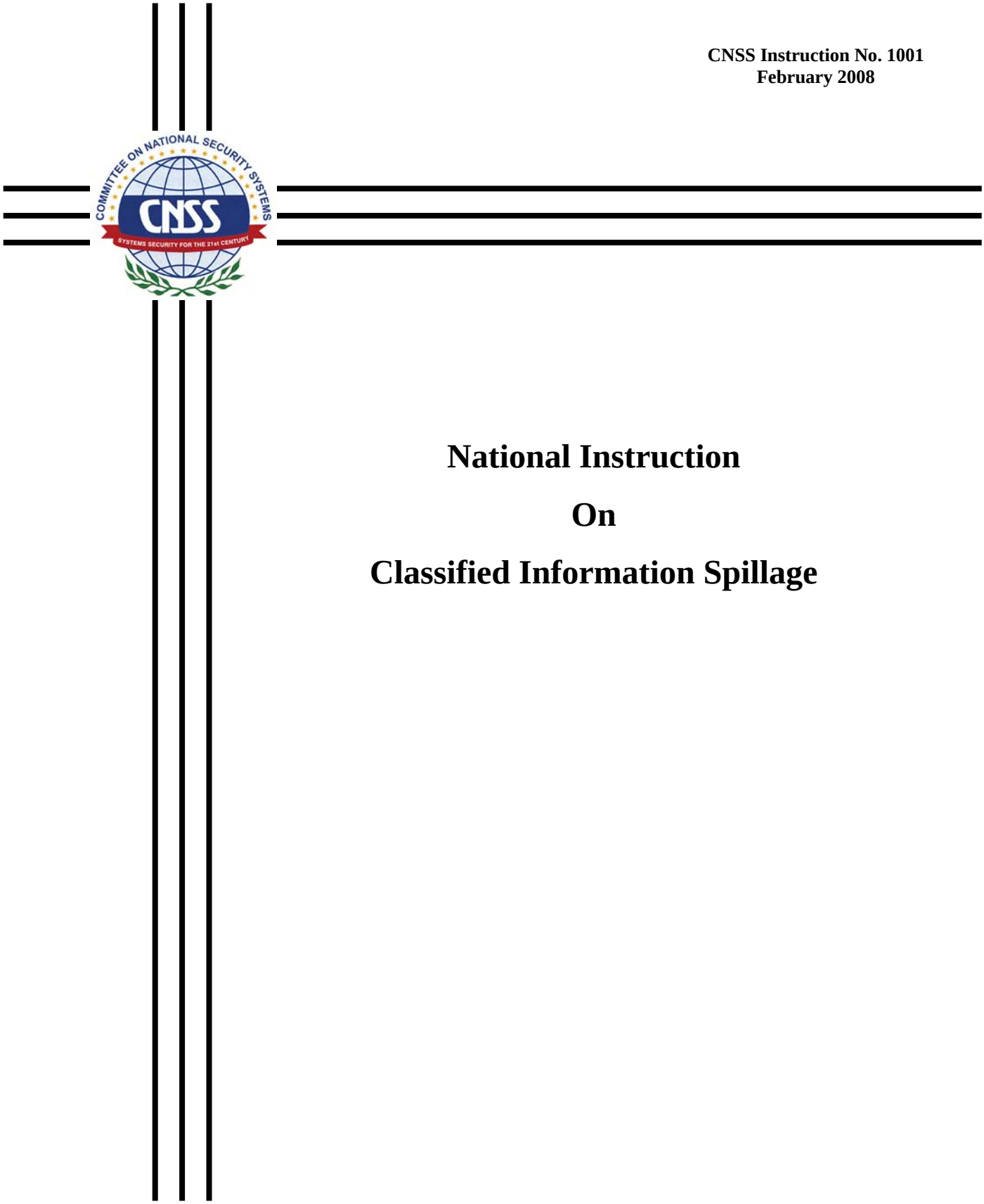
Committee on National Security System



CNSS Instruction No. 1001
February 2008

National Instruction

On

Classified Information Spillage

Committee on National Security Systems

CNSS Instruction No. 1001

National Manager

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 1001, "National Instruction on Classified Information Spillage" implements the Committee on National Security Systems Policy No. 18, reference 4.a, and is effective upon receipt.

2. Additional copies of this instruction may be obtained from the Secretariat or the Committee on National Security Systems website – www.cnss.gov.

//s//
KEITH B. ALEXANDER
Lieutenant General, U.S. Army

NATIONAL INSTRUCTION ON CLASSIFIED INFORMATION SPILLAGE

CNSS Secretariat (I923)
National Security Agency
9800 Savage Road - STE 6716 - Ft Meade MD 20755-6716
Office: (410) 854-6805
Unclassified FAX: (410) 854-6814
cnss@radium.ncsc.mil

TITLE	SECTION
PURPOSE	I
SCOPE	II
REFERENCES	III
DEFINITIONS	IV
PROCEDURES	V
RESPONSIBILITIES	VI

SECTION I – PURPOSE

1. This instruction establishes the minimum actions required when responding to an information spillage[1] of classified national security information[2] onto an unclassified Information System **(**IS**),** or higher-level classified information onto a lower level classified IS or onto a system not accredited to that category[3] (i.e. restrictive label) of information, to include non-government systems.

SECTION II – SCOPE

2. This instruction applies to the spillage of classified national security information on any IS, be it government, commercial, or private. In the case of private or commercial systems where there is no contractual requirement with the government, department/agency heads will ensure that an inquiry/investigation is conducted in accordance with references 3 b and c. In such cases, the actions established by this instruction will be implemented to the extent practical.

SECTION III – REFERENCES

3. References:

a. Committee on National Security Systems Policy No. 18, "National Policy on Classified Information Spillage," June 2006.

[1] CNSSI No. 4009, reference 3.d, defines spillage.
[2] Executive Order 12958, reference 3.b, defines classified national security information.
[3] CNSSI No. 4009, reference 3.d, defines category.

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

c. 32 CFR Part 2001 " Classified National Security Information," (Information Security Oversight Office Directive No. 1), 22 September 2003.

d. Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary, " June 2006.

e. Federal Information Security Management Act (FISMA), Title III of Public Law 107-347 (116 Stat 2948), and the E-Government Act of 2002, Public Law 107-347 (116 Stat 2899).

SECTION IV – DEFINITIONS

4. Definitions in references 3.b, c, and d apply to this instruction.

SECTION V – PROCEDURES

5. When there is evidence of a possible spillage of classified national security information, hereinafter "*classified information,*" an immediate notification shall be made to the information owner, the information assurance manager, the activity security manager, and the responsible Incident Response Center (IRC)[4]. Responsible personnel shall conduct an immediate preliminary inquiry to determine whether the classified information was subjected to loss, possible compromise, or unauthorized disclosure[5].

6. If the preliminary inquiry indicates a spillage has occurred, immediate steps shall be taken to contain and prevent further spillage of classified information. In all steps undertaken to isolate and protect the classified information from unauthorized disclosure, continuity of operations should be maintained. Continuity of operations factors should include: classification level and category of the information, perishability of the information, possible impact to ongoing investigations, or operational necessity. Consideration should be given to law enforcement implications and preservation of evidence.

7. Upon determination that a spillage has occurred, a formal inquiry shall be conducted. A team shall be formed to investigate. At a minimum, the team shall include the Information Assurance Manager, Information System Security Manager or equivalent[6], Activity Security Manager, information owner, responsible IRC, and law

[4] FISMA, reference 3.e, defines incident response center.
[5] Executive Order 12958, reference 4 b, defines unauthorized disclosure.
[6] The cited specialty titles may be equivalent to other titles used throughout organizations.

enforcement authorities, as appropriate. The team will address, at a minimum, the following questions:

a. When did the spillage occur?

b. What information was spilled?

c. What was the classification/category of the spilled information?

d. Was the classified information in question properly classified?

e. What steps were taken to contain the spillage?

f. What caused the spillage to occur?

g. Who was responsible for the spill?

h. What was the flow of information to reach its ultimate destination (e.g., specific web, mail, or file servers)?

i. Where is the information now stored?

j. What steps were taken to identify the person(s) responsible for the spillage?

k. What individuals had access to the information?

l. In what specific media did the classified information originate?

m. What IS(s) were affected and to what extent?

n. Will further inquiry increase the damage caused in the event of a compromise?

o. Is the information being handled as evidence?

8. The appropriate procedures for sanitizing or remediating the effects of a spill may include:

a. Using the operating system to delete the spilled information.

b. Re-labeling the media containing the spilled information to the appropriate classification/category and transferring the media into an appropriate environment.

c. Removing the classified information from the media by organization-approved technical means to render the information unrecoverable.

d. Erasing operating system, program files, and all data files.

e. Erasing all partition tables and drive formats.

f. Erasing and sanitizing the media.

g. Forfeiting the media.

9. Selection of the appropriate remediation procedure is dependent on several factors that may include:

a. The difference between the classification and category of the spilled information and the classification and category approved for the system containing the spilled information.

b. The requirements of the information owner regarding information sensitivity and risks from inadvertent disclosure.

c. Financial considerations, including costs of media replacement and resources required for remediating the spill.

d. Operation and mission impacts.

e. Pre-existing agreements between the information owner's and the spiller's organization(s).

f. Assessment of the effectiveness of the sanitization/remediation procedures.

10. Unless otherwise determined by the information owner, in cases where the spillage occurred within agency-controlled space, sanitization is not required until such time as the affected systems are removed from agency control. In such cases, immediate actions will be required to ensure that the spillage is isolated and contained, and that unauthorized access is precluded based on risk management decisions and operational considerations related to the loss of information services. Preclusion of unauthorized access may include software overwriting of affected data sectors in the interest of meeting operational needs. When the media is released from agency control, sanitization is required.

11. Once the extent of the spillage has been determined and the exact location(s) of the information on the system(s) are known, a final report must be completed and submitted to the information owner and must include a statement of recommended corrective action to prevent a recurrence. The information owner and the head or

designee of the department/agency where the incident occurred shall collaborate in the performance of a risk assessment to determine mitigation procedures, with input from the responsible IRC and other appropriate parties:

a. Such corrective actions include new procedures, technologies, security education, and other means to address technical and procedural deficiencies, or incidents of negligence and deliberate disregard.

b. When implementing the mitigation procedures, options should be taken to preserve continuity of operations.

c. If the conclusion of the inquiry is a loss, possible compromise or unauthorized disclosure of classified information, the degree of damage to national security shall be ascertained.

SECTION VI – RESPONSIBILITIES

12. The head of each department/agency shall:

a. Provide policy and direction for reporting and investigating spillages of classified information onto an unclassified IS, or higher-level classified information onto lower level classified IS or onto a system not accredited to that category of information, to include non-government systems.

b. Monitor investigations of spillages of classified information.

c. Review findings of initial inquiry and/or investigation of spillages of classified information.

d. Determine whether an additional internal investigation is appropriate, depending on the results of the initial inquiry and/or investigation. Consultation should take place with the department/agency having original classification authority for the information.

e. Determine whether the incident should be referred to the Department of Justice for investigation and/or criminal prosecution.

f. Notify the Director, Information Security Oversight Office as required by reference b.[7]

g. Request the initiation of comprehensive analyses and damage assessments when such disclosures affect intelligence or counterintelligence activities, capabilities, and techniques.

h. Ensure cooperation with the agency having original classification authority in their conduct of comprehensive damage assessments, analyses, and/or operations.

i. Designate, at their discretion, a responsible department/agency official for implementing the responsibilities listed above.

13. Responsible department/agency officials shall:

a. Notify the head of the department/agency or designee about any spillage of classified information, and provide the information listed in Section V, paragraphs 7 and 8 in accordance with internal guidance or procedures.

b. Serve as the principal point of contact on counterintelligence and security investigative matters related to the spillage that involve other government organizations.

c. Determine whether further investigation is appropriate when the initial inquiry or investigation does not identify the person responsible for or cause of a spillage.

d. Report the investigative results and any corrective and/or disciplinary action taken to the department/agency head.

e. Refer the incident to the appropriate counterintelligence organization, when there are indications that show a foreign intelligence service or an international terrorist group or organization may be involved.

14. Department/agency security personnel, Information Technology/Information Assurance personnel, and others shall:

a. Ensure that all known or suspected instances of spillages of classified information are promptly reported and render full cooperation in any investigation.

b. Ensure that all known or suspected instances of spillages of classified information are promptly investigated pursuant to their areas of responsibilities.

[7] Section 5.5. (e) (2) of Executive Order 12958, reference b, as amended, states, “notify the Director of the Information Security Oversight Office when a violation under paragraph (b) (1), (2), or (3) of this section occurs.”

c. Ensure appropriate actions are taken to isolate and contain the spillage, as well as to preclude unauthorized access, while using risk management principles to maintain continuity of operations.

d. Ensure notification of the spillage to the responsible IRC.

15. Users shall report all known or suspected instances of spillages of classified information per department/agency guidance and render full cooperation in any investigation.