OUTLINE SHEET 8.1

Loss and Compromise of Classified Information

REFERENCES

SECNAV M5510.36, Chapter 12
JAGINST 5800.7D, Manual of the Judge Advocate General

OUTLINE

A. Basic Policy (ISP 12-1)

1. Definitions:

   a. Compromise - The unauthorized disclosure of classified information to a person(s) who does not have authorized access, valid clearance, or a need-to-know

   b. Possible compromise - When classified information is not properly controlled

   c. Electronic spillage – Occurs when data is placed on an IT system possessing insufficient information security controls to protect the data at the required classification.

2. The loss or compromise of classified information presents a threat to national security

   a. Occurs when information cannot be physically located or accounted for

   b. Threat when loss/compromise occurs will be evaluated and measures taken to negate or minimize effects

   c. Any person finding classified information out of proper control, shall: (see figure 8.1-1)

      - Take custody of and safeguard information
      - Notify proper authority

3. All loss or compromise of classified information shall be reported, investigated, and corrected to preclude recurrence

B. Reporting Responsibilities (ISP 12-2)

1. Commanding Officer

   a. Immediately initiate a Preliminary Inquiry (PI) when a loss or compromise of classified occurs

   b. Ensure the local NCIS office is notified if it is determined during conduct of the PI that a loss or compromise of classified information did occur (timely referral is imperative to ensure preservation of evidence)

      NOTE: NCIS will advise whether or not it will open an investigation and provide advice and assistance to the PI as necessary

   c. Ensure any incident of deliberate compromise or involvement with foreign intelligence agencies is immediately reported to NCIS **(ISP 12-8)**

2. Security Manager

   a. Responsible for overseeing the PI

   b. Coordinate any compromises or possible compromises on an IT system with the IAM (The IAM will ensure the possibly compromised classified information is sanitized from the affected system)

   c. Ensure command personnel are trained in what to so if they discover a security violation (see figure 8.1-1) and the consequences of being involved in a security violation (see figure 8.1-2)

3. Individuals

   a. If a person becomes aware that information is lost or compromised they shall <u>immediately</u> report incident to Security Manager or CO, as well as their supervisory chain of command

   b. If person believes CO or Security Manager are involved – report to next echelon of command or

supervisor or to local NCIS office if such notification is impractical

4. Any incident of deliberate compromise or involvement with foreign intelligence agencies shall be immediately reported to NCIS **(ISP 12-8)**

Security Incidents and Actions

	Security Container Found Open	Classified Information Found Adrift	Unauthorized Removal	Missing Material
Report	X	X	X	X
Guard/Protect	X	X	X	
Inspect/Turn-In	X	X	X	
Lock/Secure	X	X	X	
Inventory	X			X
Confiscate		X	X	
Notify CO/XO	X	X	X	X

Figure 8.1-1. Security Incidents and Actions.

Consequences of Security Incidents

Possible Actions		Military	Civilian
Administrative Sanctions	Warning	X	X
	Reprimand	X	X
	Suspension Without Pay		X
	Forfeit Pay	(UCMJ)	X
	Loss of Access/Clearance	X	X
	Removal	X	X
	Discharge	(Hon, Admin Other)	
Civil Remedies	Fines		X
Disciplinary Actions	UCMJ	X	
	Federal Court	X	X

Figure 8.1-2. Consequences of Security Incidents.

C. Preliminary Inquiry (PI) Report (Non Electronic Spillage Incidents) (ISP 12-3 thru 12-7)

1. PI – An initial investigation to determine the facts surrounding a possible loss or compromise of classified information (see Exhibits 12A and 12B ISP for PI formats)

   NOTE: Convened by the command with custodial responsibility over the material

2. PI officer assigned, in writing, by the CO will:

   a. Have security clearance eligibility and access at or above the level of the information involved

   b. Have ability to conduct an effective, unbiased investigation

   c. Not be someone involved with the incident

3. PI will be initiated and completed within **72 hours** of initial discovery of the incident (format message or letter)

   a. If a delay cannot be avoided then notify administrative chain of command, CNO (N09N2), originator, OCA, local NCIS office of reason for delay and expected completion date

   b. Do not delay pending NCIS completion of investigation (unless advised to do so by NCIS SAC)

4. PI shall:

   a. Completely and accurately identify the information lost or compromised (i.e., subject/title, classification and any relevant associated markings, serial numbers, date, originator, OCA, number of pages, command POC, phone, UIC, etc.)

   b. Identify the NCIS agent contacted

   c. State whether a JAG Manual investigation will or will not be conducted

5. Keep PI unclassified unless:

   a. Information lost beyond jurdisction of the U.S. govt. and cannot be recovered

   b. If information involves a public media compromise and the PI contains information that could enable others to locate the classified information

6. Actions upon conclusion of PI

   a. Forward by message or letter to next senior in the chain of command, CNO (N09N2), (CMC (ARS) – USMC commands), originator, OCA, local NCIS office and any other addees required for special types of material) if PI concludes:

      - Loss or compromise of classified information occurred or if a significant command security weakness or vulnerability is revealed

      - Loss or compromise should be assumed unless the information did not leave the control of the U.S. Govt.

      NOTE: "Beyond the jurisdiction of the U.S. Govt." is considered if the information is, e.g., transmitted over the Internet, is publicly revealed, becomes the subject of a public media compromise, or is improperly revealed to an unauthorized individual or entity over which the U.S. Govt. has no authority

   b. A JAGMAN investigation is required in the event that disciplinary action is being considered or recommended by the PI or a compromise of classified information is considered likely to have occurred – all PI addees will be notified that a JAGMAN will be conducted

      NOTE: If the PI concludes that a significant security weakness or vulnerability exists due to the failure of a person to comply with established security practices and/or procedures CO will take any necessary corrective actions to prevent recurrence

c. Do not forward the PI if it concludes that a loss or compromise of classified information did not occur, or the possibility of compromise is remote due to belief that the info was never outside the control of cleared U.S. govt. personnel

d. A record of the PI must be kept regardless of its conclusions

7. CO has ultimate responsibility for determining course of action at the conclusion of a PI

8. Security Manager will advise the CO on recommended actions and take appropriate administrative action regarding any individual's failure to comply with established security practices

9. Reporting losses or compromises of special types of classified information and equipment **(ISP 12-8)**

a. The below listed special types of information/equipment have additional reporting requirements – see Chapter 12, paragraph 12-8 for guidance):

- Classified IT systems, terminals or equipment
- NATO
- FGI
- DOD SAPs
- RD/FRD/CNWDI
- SIOP/SIOP-ESI
- COMSEC
- SCI

b. Unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DOD information classified for security purposes, however unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons

D. Electronic Spillage (ES) Preliminary Inquiry (PI) Report (Navy Telecommunications Directive (NTD) 11-08)

1. All users must immediately report a suspected ES

to Security Manager and Chain of Command

2. Electronic Spillage – Data placed on an information system possessing insufficient security controls to protect the data at the required classification posing a risk to national security

3. Command originating ES

a. Upon notification of ES Security Manager will:

(1) Collect initial data from user discovering ES using Section 1 of OPNAV Form 5500/13, Electronic Spillage Action Form

(2) Notify CO and IAM of ES – Provide IAM with Section 1 of OPNAV Form 5511/13

NOTE: Additional reporting requirements shall be made per Chapter 12, Paragraph 12.8 for special types of classified information

b. Upon notification of spillage – CO will appoint a Preliminary Inquiry Officer

NOTE: For ES a PI is mandatory regardless if it meets criteria of Chapter 12 of ISP

NOTE: ES also applies to situations where Unclassified Naval Nuclear Propulsion Information U-NNPI) is introduced to non U-NNPI hardware – however these ES do not require a PI)

c. Preliminary Inquiry

(1) Assigned PI Officer will complete PI within 72 hours of initial discovery of ES. The following addees will be included on all PI reports:

CNO (N09N2, N 6, N6133)
NETWARCOM N5

(2) Security Manager

(a) Request OCA (Original Classification Authority) determination of spilled data as part of PI submission. Send PI reports via naval message, SIPRNET email or NIPRNET encrypted email. (For DON OCAs - See ES center website or www.navysecurity.navy.mil)

(b) Notify CO, IAM (and local NCIS office if NCIS investigation pending) of OCA classification determination (OCA required to report classification determination within 3 business days upon receipt of PI)

d. IAM reporting requirements – see NTD 11-08

4. Command receiving ES

a. Upon notification of ES Security Manager will:

(1) Collect data from user discovering ES using Section 1 of OPNAV Form 5500/13

(2) Notify CO and IAM of ES and provide Section 1 of OPNAV Form 5500/13 to IAM

(3) Notify originating command via appropriate communication method (e.g., email, naval message, phone) providing information collected

NOTE: A PI is not required from commands receiving an ES

b. IAM reporting requirements – see NTD 11-08

5. NETWARCOM – Cancel outstanding ES SITREP if OCA determines information not classified

6. Wireless devices are subject to requirements of NTD 11-08 - If affected by an ES – handle as classified devices at level commensurate with spilled data

7. Government furnished laptops or desktops used for remote access (e.g., outlook, etc.,) to Navy IS affected by an ES are subject to NTD 11-08 and must be delivered to command immediately for sanitization

E. JAGMAN Investigations ISP 12-9, 10 and Exhibits 12C and D)

1. The purpose of a JAGMAN is to provide a more detailed investigation and recommend corrective or disciplinary actions

   a. The CO shall appoint in writing an individual to conduct investigation who: **(ISP Exhibit 12C)**

      - Has clearance level equal to information involved
      - Is not be someone directly or indirectly involved
      - Is not the Security Manager

      NOTE: Exhibit 12D (ISP) has sample format for JAGMAN

   b. If determined during JAGMAN, no compromise occurred:

      - Terminate investigation
      - Notify all recipients of PI report with supporting statement

   c. NCIS Report of Investigation (ROI) (if conducted) will not be included in command investigation **(ISP 12-12)**

2. Investigative assistance **(ISP 12-11)**

   NCIS will provide professional or technical assistance if needed by command or if command lacks the resources or capabilities

3. Reporting results of JAGMAN investigation **(ISP 12-13)**

Forward, via administrative chain of command (with endorsements) (USMC commands – CMC (ARS) will be last via before CNO(N09N2):

To: CNO (N09N2)
Info: Originator/OCA
NSCDA and OJAG (Code 17)
Local NCIS office

4. Review of JAGMAN investigations by Superiors. Each superior in chain of command will: **(ISP 12-14)**

- Approve or disapprove
- Evaluate for completeness
- Evaluate corrective measures
- Review disciplinary action
- Determine if security practices are in conflict with regulation
- Endorse and forward to CNO (N09N2)

NOTE: Classified information found after being reported lost shall be reported to all who were notified of the loss

F. Security and Classification Reviews (ISP 12-15 and 12-16)

1. Compromised information requires an initial local security review

2. Local security review:

a. Done locally if expertise available

b. Forwarded to OCA with request for a “simple review” if local expertise not available

3. Damage assessment **(ISP 12-17)**

a. Determines effect of compromise on national security

b. Is a long-term, post prosecutive investigation

c. Not to be confused with OCA classification review

d. Is not completed to support PI or JAGMAN

G. Other Security Incidents

1. Public media compromises **(ISP 12-18)**

   a. Unofficial and unauthorized release of classified and unclassified information to the public

   b. Immediately notify CNO (N09N2)

   c. No statements will be made concerning information's public release

   d. CNO (N09N2) is responsible for investigating and reporting to proper authority

2. Incidents Involving Improper Transmission **(ISP 12-19 and Exhibit 12E)**

   a. If a command receives information improperly prepared or transmitted, but not subject to compromise, they will send a Security Discrepancy Notice (OPNAV Form 5511/51) to the sending command. Retain for 2 years.

   b. If a command determines that the classified information was subject to compromise because it was improperly handled, addressed, packaged, transmitted, or transported, the sending command will be immediately notified and a PI initiated. Some examples are:

      (1) Handled through foreign mail service

      (2) Shipping container damaged and contents exposed

      (3) Transmitted via unsecured facsimile, telephone, internet, posted to a publicly accessible website

3. Other incidents

   a. Disregard of security regulations shall be investigated by cognizant CO

   b. Reports of security incidents shall be maintained by command