



*Security*

**SECURITY INCIDENTS**

---

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available electronically on the USTRANSCOM electronic library.

**RELEASABILITY:** There are no releasability restrictions on this publication

---

OPR: TCJ3-FP (Steve Strait)  
Supersedes: USTRANSCOMI 31-11, Chapter 7

Approved By: TCJ3 (MG Michael J. Lally, USA)  
Pages: 6  
Distribution: e-Publishing

---

This Instruction establishes USTRANSCOM policy for reporting, investigating, and implementing process improvements pertaining to classified information security incidents. This instruction applies to all personnel assigned, attached, or contracted to USTRANSCOM. Refer recommended changes and questions about this instruction to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this instruction are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

**SUMMARY OF REVISIONS**

This revision includes spelling out acronyms and some minor language edits.

**1. References and Supporting Information.** References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

**2. General.**

**2.1.** The compromise of classified information presents a threat to national security. A security violation is any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. In all cases, appropriate action must be taken to investigate the incident to identify the source and reason for the actual or potential compromise, and identify remedial action to prevent recurrence.

**2.2.** Any suspected violation must be immediately reported to your Security Representative, your supervisor, and to the Antiterrorism and Security Branch, Force Protection Division (TCJ3-FP). If the incident involves a spillage of classified information onto the Non-Secure Internet Protocol Router Network (NIPRNet), Global Command and Communications Center (TCJ6-GCCC) must be notified immediately to begin clean up protocols.

**2.3.** Anyone discovering unsecured classified material must immediately secure the information and report the incident to TCJ3-FP. All Department of Defense (DOD) personnel are individually responsible for safeguarding classified information.

**2.4.** If classified information appears in the public media, do not make any statement or comment which would confirm the accuracy or verify the classified status of the information. If approached by a representative of the media, neither confirm nor deny the accuracy of or the classification of the information. Report any such contact immediately to USTRANSCOM Public Affairs (TCPA) and TCJ3-FP.

**2.5.** Security violations involving computer systems, terminals, or equipment shall be reported to your Security Representative, TCJ6, and TCJ3-FP.

**2.6.** Security violations involving foreign government information shall be reported to your Security Representative, the USTRANSCOM Directorate of Intelligence Foreign Disclosure Office (TCJ2-P), and TCJ3-FP.

**2.7.** Security violations involving Sensitive Compartmented Information shall be reported to your Security Representative, the Directorate of Intelligence Special Security Office (TCJ2-SSO), and TCJ3-FP.

**2.8.** Security violations involving Special Access Programs shall be reported to your Security Representative, the Directorate of Operations and Plans Special Technical Officer (TCJ3-SO), and TCJ3-FP.

### **3. Classified Information Spillage.**

**3.1.** A classified information spillage occurs when a higher level classified information is put on a lower level classified information system or onto a system not accredited to that category of information, to include non-government systems. Examples include Top Secret (TS) information placed on the Secret Internet Protocol Router Network (SIPRNet) and when classified national security information is put on the NIPRNet.

**3.2.** Classified information spillages can result in significant costs to USTRANSCOM and to the DOD.

**3.2.1.** Possible loss of confidentiality, integrity, or availability of information.

**3.2.2.** Possible operational affects to specific movements.

**3.2.3.** Possible fiscal costs such as replacing backup tapes.

**3.2.4.** Possible time spent in cleaning and loss of system use during repair.

**3.2.5.** Possible effect on other organizations if the information was forwarded via email to outside organizations.

**3.3. Actions for USTRANSCOM personnel upon discovery of a spillage.**

**3.3.1.** Report the incident immediately to TCJ6-GCCC, to TCJ3-FP, and to your Security Representative.

**3.3.2.** Do not delete the email without guidance from TCJ6. TCJ6-GCCC will need to verify where the email has been sent in order to ensure total cleansing of the network.

**3.3.3.** Do not forward the email containing the classified information.

**3.3.4.** Provide TCJ6-GCCC the following information:

**3.3.4.1.** Contact information of the caller, the originator of the classified information (e.g., file, e-mail, message, etc), network or systems affected.

**3.3.4.2.** Details of the message (from, to, date, subject, attachments, etc).

**3.3.4.3.** All recipients of the classified information, their organization, and contact information; including those to whom the message was originally sent and those to whom the message was forwarded.

**3.4. TCJ6-GCCC actions upon notification of a spillage.**

**3.4.1.** Collect information concerning the incident and verify classification of the reported incident with TCJ3-FP or the source of the information.

**3.4.2.** Record information on the incident on a Classified Military Incident report.

**3.4.3.** Make notifications as specified in the Classified Military Incident Spillage checklist.

**3.4.4.** Disable or direct the disabling of the affected user accounts until the cleanup is completed or as otherwise directed.

**3.4.5.** Direct appropriate technical staff elements to accomplish sanitization procedures and monitor execution actions until the event is resolved. USTRANSCOM technical support staff organizations (systems administrators, etc.) will provide technical assistance, recommendations, and support as requested, accomplish sanitization procedures as directed. Advise the TCJ6-GCCC when actions have been completed in order and affected user accounts may be re-enabled.

**3.4.6.** When multiple sites are involved, notify servicing network control center at the location where the message originated or was transmitted.

**3.4.7.** Track and compile information until the event is closed and provide periodic updates and distribute the final completed checklist/report to the SIPRNet Classified Military Incident spillage email address group.

#### **4. Security Inquiry Process.**

**4.1.** The security incident inquiry process within USTRANSCOM is as stated:

**4.1.1.** TCJ3-FP is notified of a security incident.

**4.1.2.** TCJ3-FP obtains initial information and ensures classified information is secured. If the incident is a spillage, ensure TCJ6-GCCC is notified.

**4.1.3.** TCJ3-FP immediately notifies Deputy Chief of Staff (TCCS-D) verbally or via email stating initial details of the incident.

**4.1.4.** TCJ3-FP submits a memo to TCCS requesting an Inquiry Official (IO) be appointed to:

**4.1.4.1.** Determine the facts associated with the incident.

**4.1.4.2.** Determine if a compromise of classified information occurred. If the IO believes a compromise has occurred, they must immediately notify TCJ3-FP. TCJ3-FP notifies TCCS-D.

**4.1.4.3.** Determine if a violation of existing security practices occurred.

**4.1.4.4.** Provide recommendations to TCCS for future mitigation or process improvements directed to prevent a similar occurrence.

**4.1.5.** The Joint Secretariat creates a tasker for the Directorate selected to appoint an IO.

**4.1.6.** TCCS selects an IO and signs out a letter to the IO designating them as such.

**4.1.7.** The IO receives a briefing on the basic facts of the incident and on inquiry responsibilities in accordance with chapter 10, DODR 5200.1-R, *Information Security Program*. The IO generally has ten days to complete the formal inquiry report. TCJ3-FP will provide guidance as required throughout the inquiry process.

**4.1.8.** Once the inquiry official completes a written report of findings, the report will be reviewed by TCJ3-FP prior to forwarding to ensure all required elements have been appropriately addressed. Upon completion of the review, the IO will submit the final report to TCJ3-FP.

**4.1.9.** TCJ3-F reviews the investigation and forwards package to TCCS with a cover memorandum signed by the Chief, Force Protection, commenting on the IO recommendations and concurrence or non-concurrence with the IO report.

**4.1.10.** TCCS reviews package and signs letter out to the appropriate Directorate or Element Commander to determine what actions are being taken in respect to the individual involved and what is being done to ensure similar violations are not repeated.

**4.1.11.** The Directorate or Service Element Commander takes appropriate action and reports back to TCCS.

**4.1.12.** The inquiry report package is returned to TCJ3-FP for follow-up action, tracking, and filing of closed out investigation.

**4.1.13.** TCJ3-FP notifies the IO that responsibilities are completed.

MICHAEL J. LALLY  
Major General, U.S. Army  
Director of Operations and Plans

## Attachment 1

### GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

#### Section A – References

DOD 5200.1-R, *Information Security Program*

#### Section B – Acronyms

DOD – Department of Defense

GCCC – Global Command and Communications Center

IO – Inquiry Official

NIPRNet – Non-Secure Internal Protocol Router Network

SIPRNet – Secret Internet Protocol Router Network

TCCS – Chief of Staff, USTRANSCOM

TCCS-D – Deputy Chief of Staff, USTRANSCOM

TCJ2-SSO – Special Security Office, Directorate of Intelligence

TCJ3-FP – Antiterrorism and Security Branch, Force Protection Division

TCJ3-SO – Special Technical Office, Directorate of Operations and Plans

TCJ6 - Directorate of Command, Control, Computer Systems and Chief Information Officer

TCPA – Public Affairs, USTRANSCOM

TS – Top Secret

USTRANSCOM – United States Transportation Command

#### Section C – Terms

**Inquiry Official.** A person (military or government civilian) assigned by the Chief of Staff to conduct an inquiry into the facts of a security incident with the primary responsibility to determine if a compromise of classified information has occurred. The Inquiry Official also reports if the security incident was the result of a deviation from USTRANSCOM security practices and provides recommendations for process improvements.

**Security Incident.** Any mishandling of classified information that could lead to unauthorized disclosure. Examples include spillages onto the NIPRNet; failures to secure classified; lost classified information, or personnel accessing classified without a clearance .

**Spillage.** The unauthorized placing of classified information on the NIPRNet or of Top Secret information on the SIPRNet.