UNITED STATES TRANSPORTATION COMMAND
Scott Air Force Base IL 62225-5357

USTRANSCOM INSTRUCTION 71-1
22 April 1996

Special Investigations

DAMAGE ASSESSMENT

This instruction establishes responsibilities and procedures for reviewing, analyzing, and reporting comprehensive damage assessments pursuant to the compromise of U.S. classified information from espionage. It implements Department of Defense (DoD) Instruction 5240.11, Damage Assessment. It applies to all personnel assigned to United States Transportation Command (USTRANSCOM) at Scott Air Force Base IL. Send comments and suggested improvements to this instruction on Air Force (AF) Form 847, Recommendation for Change of Publication, to USTRANSCOM/TCIM-P.

SUMMARY OF REVISIONS

The revisions throughout this Instruction consist of transferring responsibility for this program from the Chief of Staff (TCCS) to the Director of Intelligence (TCJ2) and changing USTRANSCOM Counterintelligence Support (TCCIS) to Counterintelligence Staff Officer (TCJ2-CISO). * Indicates changed material.

1. References, Abbreviations and Acronyms, and Terms. References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in the attachment.

2. Responsibilities:

2.1. When necessary, the Deputy Commander in Chief (TCDC) will appoint a USTRANSCOM Damage Assessment Committee (TCDAC) to examine the impact of a compromise of classified information.

***2.2.** TCJ2 will, after coordination with the tasked directorates and Direct Reporting Elements (DREs), recommend to TCDC a list of USTRANSCOM personnel to participate in the damage assessment committee, to include a Committee Chairman.

Supersedes USTRANSCOMR 124-1,1 Oct 92
OPR: TCJ2-CISO (Stewart R. Wilson)

Certified by: TCJ2 (Col Eric C. Peterson, USAF)
Pages: 5/Distribution: X (see signature page)

***2.3.** TCJ2-CISO, is the single point of contact within USTRANSCOM for issues relating to espionage directed against USTRANSCOM resources. Upon notification from any U.S. Counterintelligence Service of an espionage investigation, TCJ2-CISO will brief TCJ2, TCDC, and the USTRANSCOM Commander in Chief (TCCC). Briefings concerning ongoing espionage investigations will be kept to an absolute minimum audience based on need-to-know. Additionally, following notification of an espionage investigation, TCJ2-CISO will ensure Office of the Assistant Secretary of Defense Command, Control, Communications, and Intelligence (OASD/C3I) is provided a preliminary advisement of the situation. Furthermore, if the investigation is related to a significant foreign intelligence threat, the Joint Counterintelligence Support Branch (JCISB), Defense Intelligence Agency, will be notified in accordance with MCM-149-92-S. Appropriate civilian and military investigative agencies will also be notified of the investigation. TCJ2-CISO will maintain contact with the counterintelligence service conducting the investigation and brief TCJ2 as necessary.

2.4. The TCDAC will provide a written report to TCCC and OASD/C3I concerning the results of the damage assessment. Interim reports will be provided as requested.

2.5. Other directorates' and DREs' responsibilities:

2.5.1. When requested by TCJ2, provide the names of experienced personnel to participate in the TCDAC.

2.5.2. As required, provide office space and administrative support to the TCDAC.

3. Procedures:

***3.1.** Upon notification of an espionage investigation effecting USTRANSCOM, TCJ2-CISO will brief TCJ2, TCDC, and TCCC, as appropriate.

***3.2.** TCJ2 will recommend formation of the TCDAC and forward a proposed list of members to TCDC for approval. Membership of the TCDAC will consist, as a minimum, of representatives from TCJ2, Operations and Logistics Directorate (TCJ3/J4), Plans and Policy Directorate (TCJ5), Mobility Protection Branch (TCJ3-OSM), and TCJ2-CISO. Other directorates and DREs will be tasked to participate as the circumstances of the case dictate. Chief Counsel (TCJA) should monitor the damage assessment process and lend advice as warranted. Special consideration should be made for including Command, Control, Communications, and Computer Systems Directorate (TCJ6) on the committee when automated data bases or telecommunications equipment are involved.

***3.3.** The TCJ2-CISO, will brief the TCDAC on the specifics of the case.

3.4. The TCDAC will meet in a secure location to discuss the case and prepare the damage assessment.

3.5. The Chairman, TCDAC, will provide the finalized damage assessment report to TCCC, OASD/C3I and any other appropriately cleared U.S. agencies that are affected.

ERIC C. PETERSON
Colonel, USAF
Director of Intelligence

Attachment
Glossary of References, Abbreviations and Acronyms, and Terms

DISTRIBUTION: X (TCCC-X, TCIG, TCIM, TCJA, TCPA, TCRC, Office of Asst Secretary of Defense (C3I), Pentagon Rm 3C268, 6000 Defense Pentagon, Washington DC 20301-6000 - 1 each; TCJ8, TCSG - 2 each; JTCC, TCDC-JS, TCJ1, TCJ2, TCJ5, TCJ6, - 5 each; TCJ3/J4 - 13).

GLOSSARY OF REFERENCES, ABBREVIATIONS AND ACRONYMS, AND TERMS

Section A--References

Department of Defense (DoD) Instruction 5240.11, Damage Assessment

Chairman, Joint Chiefs of Staff (CJCS), MCM-149-92-S, Counterintelligence Support

Section B--Abbreviations and Acronyms--not used.

Section C--Terms

Classification Review: A formal finding that information subjected to loss or compromise is (was) legally classified at the time of the compromise. The review usually includes an assessment of the probability (risk) of damage to national security resulting from disclosure of this information or material to an unauthorized person. A classification review is obtained in all national security cases and is necessary when a determination must be made on the use of classified information as trial evidence under the Classified Information Procedure Act or Military Rule of Evidence 505 (references (h) and (I)), respectively.

Compromise: The known or suspected exposure of classified information or material or clandestine personnel to an unauthorized person.

Damage Assessment: A multidisciplinary analysis to determine the effect of a compromise of classified information on the national security. A damage assessment is normally a long-term, post-prosecution effort to determine in great detail the practical effects of an espionage-related compromise on operations, systems, materials, and intelligence. In special circumstances (e.g., the suspect escapes or flees U.S. jurisdiction), a damage assessment is not to be confused with the classification review, normally performed in support of an espionage prosecution, or damage control performed immediately on the discovery or disclosure of espionage.

Damage Control: Those actions taken immediately by the affected Component after the discovery of a loss of classified information to minimize risk, limit damage, and/or prevent further loss.

Espionage: Activity designed to obtain, deliver, communicate, or transmit information relating to the national defense with the intent or reason to believe it will be used to the injury of the United States or to the advantage of a foreign nation.

U.S. Counterintelligence Services: The Federal Bureau of Investigation, the U.S. Army Counterintelligence units, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.