
INTELLIGENCE COMMUNITY DIRECTIVE

NUMBER 702



TECHNICAL SURVEILLANCE COUNTERMEASURES

(EFFECTIVE: FEBRUARY 18, 2008)

A. AUTHORITY: The National Security Act of 1947, as amended; the Federal Information Security Management Act of 2002; the Counterintelligence Enhancement Act of 2002, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 12333, as amended; EO 12958, as amended; and other applicable provisions of law.

B. PURPOSE:

1. This Intelligence Community Directive (ICD) establishes the Director of National Intelligence (DNI) policy and assigns responsibilities for the oversight of Intelligence Community (IC) Technical Surveillance Countermeasures (TSCM) programs, in support of the National Intelligence Strategy and the protection of national intelligence and intelligence sources and methods. This ICD rescinds Director of Central Intelligence Directive 6/2, Technical Surveillance Countermeasures, 11 March 1999. Forthcoming IC policy guidance shall provide detailed implementation guidance.

2. "Technical Surveillance Countermeasures" represents the convergence of two distinct disciplines—counterintelligence and security countermeasures. These techniques and countermeasures are designed to detect and nullify a wide variety of technologies used to gain unauthorized access to classified national security information, restricted data, or otherwise sensitive information.

C. APPLICABILITY: This ICD applies to the IC, as defined by the National Security Act of 1947, as amended; and other departments or agencies that may be designated by the President, or designated jointly by the DNI and the head of the department or agency concerned, as an element of the IC.

D. POLICY:

1. The protection of national intelligence and intelligence sources and methods, and the neutralization of foreign intelligence threats are fundamental to the success of the IC mission. Senior Officials of the Intelligence Community (SOICs), as the senior representatives of the DNI

for security matters within their organizations, and associated contractors shall implement TSCM programs for facilities to enhance technical security in the face of ever-changing threat environments.

2. The National Integrated TSCM Committee (NITC), chartered by the DNI, shall provide policy, strategic, and procedural guidance on all TSCM matters involving the IC and its customers. The NITC shall meet at least quarterly. The NITC chair shall report annually to the DNI on IC compliance with this directive, compile TSCM programmatic and procedural recommendations, and submit a program and budget plan for consideration in coordination with the DNI Chief Financial Officer. The NITC shall be as inclusive as practical. NITC initiatives shall include the creation of a DNI funding mechanism that addresses TSCM issues of common concern.

3. The Assistant Deputy Director of National Intelligence for Security (ADDNI/SEC) shall chair the NITC. The National Counterintelligence Executive (NCIX) shall serve as vice-chair. The chair shall provide secretariat and administrative support for the committee, including the production of timely minutes, and shall direct the production by the secretariat of an annual strategy and operating plan satisfactory to the vice chair. The vice chair shall conduct a review of TSCM programs annually or semi-annually, as he or she may determine, by the staff of the Office of the NCIX.

4. All NITC members shall:

- a. Exchange technical security information,
- b. Coordinate TSCM training programs,
- c. Practice reciprocity,
- d. Conduct joint exercises and;
- e. Participate in NITC activities to the maximum extent possible.

5. Information concerning foreign technical penetrations, technical surveillance, or technical collection efforts against the United States (U.S.) shall be centralized and managed in accordance with any legal requirements. This includes intelligence information and techniques obtained through U.S. TSCM activities and subsequent counterintelligence investigations. Analysis and dissemination shall be in accordance with procedures and guidelines set forth in subsequent Intelligence Community Policy Guidance (ICPG) documents.

6. The NITC shall develop and propose a unified TSCM research and development program in coordination with the ADDNI/Science & Technology for approval by the DNI.

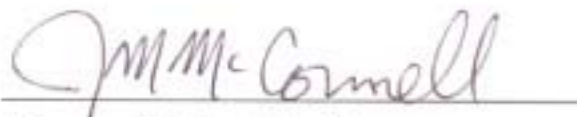
7. The NITC shall develop standardized training for TSCM personnel and other related requirements for approval by the DNI.

8. Threats will be determined in part from the national threat list derived from the NCIX National Threat Identification and Prioritization Assessment and the Human Intelligence/Technical threat evaluations of the Security Environment Threat List developed by the Department of State.

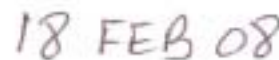
E. AUTHORITIES AND RESPONSIBILITIES:

1. NCIX shall provide counterintelligence policy guidance and be the vice chair to the NITC.
2. ADDNI/SEC shall provide security countermeasures policy guidance and chair the NITC.
3. Senior Officials of the Intelligence Community (SOIC) shall:
 - a. Implement this policy pursuant to the statutory responsibility of the DNI to protect national intelligence and intelligence sources and methods, and to detect, prevent, and neutralize foreign technical penetrations.
 - b. Deploy TSCM resources based on DNI endorsed risk management principles.
 - c. Designate senior level representatives to the NITC.
 - d. Effect appropriate notifications and coordination following the discovery of a technical penetration according to guidance contained in subsequent ICPGs.
 - e. Ensure TSCM personnel receive standardized training and meet other requirements prescribed by the NITC.

F. EFFECTIVE DATE: This ICD becomes effective on the date of signature.



Director of National Intelligence



Date