PDD/NSC 61 Energy Department Counterintelligence February 1998

In 1995 US officials became concerned that China might have acquired sensitive information from American nuclear weapons laboratories in the mid-1980s. The administration began working to tighten security at our weapons labs and prevent future breaches. DOE prepared a broad assessment of two decades of Chinese efforts to acquire nuclear weapons information from the United States and in July 1997 briefed senior administration officials on its conclusions. DOE's briefings focused attention on the need to address long-term security problems at the US nuclear labs, and within weeks, the administration created a special working group of the National Counterintelligence Policy Board to make recommendations for strengthening lab security.
The board's recommendations, forwarded in September 1997, became the basis for a Presidential Decision Directive (PDD-61), issued in February 1998. In the directive, President Clinton ordered the Department of Energy to establish a stronger counterintelligence program. Then-Secretary Federico Pena set up an independent Office of Counterintelligence, which began an intensive review of the counterintelligence program. Energy Department implementation of the requirements of PDD-61 has included:

- *hiring counterintelligence professionals to be based at the weapons labs*
- *doubling the budget for counterintelligence*
- *changing the screening and the approval process for foreign scientists seeking access to DOE labs*
- *making the lab directors directly accountable for foreign visits.*
- *instituting more extensive security reviews -- including the use of polygraphs -- for DOE scientists working in sensitive programs.*

The text of PDD-61 has not been released, and there is no White House Factsheet summarizing its provisions. However, one component of this PDD, relating to Technical Surveillance Countermeasures (TSCM), is reproduced here.

Section I - Policy

1. Heads of federal departments and agencies which process, discuss, and/or store classified national security information, restricted data, and sensitive but unclassified information, shall, in response to specific threat data and based on risk management principles, determine the need for Technical Surveillance Countermeasures (TSCM).
2. To obtain maximum effectiveness by the most economical means in the various TSCM programs, departments and agencies shall exchange technical information freely; coordinate programs; practice reciprocity; and participate in consolidated programs, when appropriate.

Section II - Responsibilities

1. Heads of US Government departments and agencies which plan, implement, and manage TSCM programs shall:
a. Provide TSCM support consisting of procedures and countermeasures determined to be appropriate for the facility, consistent with risk management principles.
b. Report to the Security Policy Board, attention : Chair, Facilities Protection Committee (FPC), for appropriate dissemination, all-source intelligence that concerns technical surveillance threats, devices, techniques, and unreported hazards, regardless of the source or target, domestic or foreign.
c. Train a professional cadre of personnel in TSCM techniques.
d. Ensure that the FPC and Training and Professional Development Committee are kept apprised of their TSCM program activities as well as training and research and development requirements.
e. Assist other departments and agencies, in accordance with federal law, with TSCM services of common concern.
f. Coordinate, through the FPC, proposed foreign disclosure of TSCM equipment and techniques.
2. The FPC shall advise and assist the Security Policy Board in the development and review of TSCM policy, including guidelines, procedures, and instructions. The FPC shall:
a. Coordinate TSCM professional training, research, development, test, and evaluation programs.
b. Promote and foster joint procurement of TSCM equipment.
c. Evaluate the impact on the national security of foreign disclosure of TSCM equipment or techniques and recommend policy changes as needed.
d. Develop guidance for use in obtaining intelligence information on the plans, capabilities and actions of organizations hostile to the US Government concerning technical penetrations and countermeasures against them.
e. Biennially, review, update and disseminate the national strategy for TSCM.

Section III - Definitions

1. Technical Surveillance Countermeasures (TSCM) - Techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to classified national security information, restricted data, and/or sensitive but unclassified information.
2. Classified National Security Information (CNSI) - Means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
3. Restricted Data (RD) - All data concerning design, manufacture or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to Section 102 of the Atomic Energy Act of 1954, as amended.
4. Sensitive but Unclassified - Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of

federal programs, or the privacy to which individuals are entitled under Section 522a of Title 5, US Code, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

SOURCES:

- Pe□a Takes Action to Boost Security at DOE Defense Nuclear Facilities November 7, 1997 Secretary of Energy Federico Pe□a today announced several actions to strengthen the safeguards and security at the Department's defense nuclear facilities.
- Richardson Names Director For DOE's Office of Intelligence October 5, 1998 -- Secretary of Energy Bill Richardson has selected Lawrence H. Sanchez to be the Director of the Office of Intelligence at the U.S. Department of Energy. As director, Sanchez will be responsible for foreign intelligence analysis and work closely with DOE's nonproliferation, nuclear weapons, stockpile stewardship and counterintelligence programs. Sanchez will serve the Energy Department on detail from the Central Intelligence Agency (CIA) beginning at the end of October