DEFENSE AUDIT SERVICE
1300 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22209

REPORT
NO. 80-143

September 29, 1980

REPORT ON THE REVIEW OF ACCOUNTING SYSTEMS FOR WIRETAP AND EAVESDROP EQUIPMENT

TABLE OF CONTENTS

Prepared by:
Intelligence and Communications
Audits Division
Project 9IG-028

REPORT ON THE REVIEW OF ACCOUNTING SYSTEMS FOR WIRETAP AND EAVESDROP EQUIPMENT

INTRODUCTION

We were requested by the Deputy Assistant Secretary of Defense(Administration), Office of the Assistant Secretary of Defense(Comptroller), to review the adequacy and accuracy of the Military Departments' inventory systems for wiretap and eavesdrop equipment, and determine whether the amount of equipment was appropriate to perform assigned missions. We were also asked by the Director for Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy Review, to include in our review an evaluation of the indexing system used to record interceptions of wire and oral communications.

Background

The interception of wire and oral communications for law enforcement purposes within the Department of Defense (DoD) is prohibited unless conducted in accordance with applicable laws and the provisions of DoD Directive 5200.24, "Interception of Wire and Oral Communications for Law Enforcement Purposes." Interceptions can only be made for properly designated purposes and are limited to those investigative offices within the Army, Navy and Air Force that have specific written authorization from the Head of the Department.

Responsibility for establishing policy and overseeing this area within DoD has been shifted several times in recent years and currently rests with the Director for Counterintelligence and Investigative Programs, Office of the Deputy Under Secretary of Defense for Policy Review.

DoD Directive 5200.24 provided that all applications for nonconsensual interception of wire and oral communications of U.S. persons must be approved by the DoD General Counsel and coordinated with the Department of Justice prior to seeking a court order for the intercept. Requests for consensual intercepts are approved or disapproved by the Secretaries of the Military Departments or their designees. The Directive required quarterly reporting to the U.S. Attorney General of all consensual interceptions by Military Department investigative units, however this requirement was eliminated during the review. An annual report was required of all nonconsensual interceptions made for law enforcement and investigative purposes abroad, as well as for interception applications which were not approved. The Directive also required the Secretaries of the Military Departments to submit annually to the Office of Secretary of Defense(OSD) a complete inventory of all

wiretap and eavesdrop equipment and devices. The establishment and maintenance of indexing systems (indexes) for all interceptions and denied interception applications were also required by the Directive.

Scope of Review

We examined the policies, procedures and practices used to account for and control wiretap and eavesdrop equipment in the designated investigative units of the Military Departments. Our review included a complete reconciliation of records for the entire inventory (737 items) and a physical count of 660 selected items. We statistically selected 2,953 of the 139,473 available criminal case files to test for unauthorized or unrecorded use of wiretap and eavesdrop techniques. Discovery sampling was used to test the accuracy of the indexing systems for cases where these techniques were authorized. The Appendix to this report lists the activities visited during our review.

RESULTS OF THE REVIEW AND RECOMMENDATIONS

We found no significant discrepancies between the quantities of wiretap and eavesdrop equipment recorded on Military Department inventory records and the quantities on hand. Furthermore, we found no evidence of unauthorized or unrecorded electronic surveillance operations by the investigative units. Overall, the Military Departments were effectively carrying out the responsibilities described in DoD Directive 5200.24. However, we found that improvements could be made in some areas, notably clarification of certain provisions governing the definition of interception equipment and its retention, and the adequacy of procedures for maintenance of prescribed indexes. These changes, if effectively implemented, could enhance overall investigative operations and reduce their potential for public criticism.

Recommendations

We recommend that the Deputy Under Secretary of Defense for Policy Review, in coordination with the General Counsel:

1. Revise DoD Directive 5200.24 to clearly define "wiretap and eavesdrop equipment."

2. Establish guidelines to be followed by users in determining minimum levels for such equipment.

3. Establish standardized procedures and forms for overall control of equipment when in use.

4. Request, from the Department of Justice, clarification of electronic surveillance indexing requirements based on anticipated inquiries.

5. Establish quality assurance procedures for indexing operations to ensure uniformity in accumulating, transcribing and verifying electronic surveillance data.

6. Require investigative units to review existing case files where electronic surveillance was used to identify and record data not previously indexed.

7. Revalidate prior responses to requests for surveillance information against those cases, disclosed by the review in recommendation 6 above, containing data not previously indexed.

Discussion

Equipment and devices used for intercepting communications must be properly controlled and safeguarded to prevent unauthorized access or use. Inventory records must be maintained to account for the equipment at all times and centralized storage of such equipment is encouraged wherever possible, consistent with operational requirements. The use made of the equipment has to be fully accounted for in written reports from the users. Annually, the Secretaries of the Military Departments are required to submit to the Office of the Deputy Under Secretary of Defense for Policy Review a complete inventory of all equipment and devices useful for operations covered under the provisions of DoD Directive 5200.24. The inventory consisted of 737 pieces of equipment with a value approximating $400,000. In addition to the inventory records and reports, the Directive requires that an indexing system (indexes) be established and maintained for all interceptions and denied interception applications. These indexes are keyed to names and other identifying data for each reasonably identifiable person whose communication was intercepted (intentionally or otherwise), or who was the target of the interception application. Indexes are kept for the purpose of providing centralized and readily accessible data to respond to various types of legal inquiries.

Equipment Inventories. The Army inventory manager for wiretap/eavesdrop equipment was the Intelligence and Materiel Development Support Office at Fort Meade, Maryland, while the Navy and Air Force managed their equipment inventories from the headquarters of their respective Investigative Commands. Items included in the inventories were mainly older pieces of equipment since minimal procurements have been made in the past 5 years.

Varying procedures existed for controlling and recording inventories of wiretap and eavesdrop equipment. Procedures used for recording withdrawals of equipment also varied among the Services. Some apparent confusion was evident over the types of equipment that should be controlled and accounted for. Examples included items such as ordinary tape recorders and equipment used by fire and police departments to record emergency calls.

Further, there were no standards established for determining the minimum quantity of equipment that should be maintained to meet expected operational requirements. Nevertheless, each Military Department certified in their inventory reports that existing quantities were being maintained at the lowest level, consistent with operational needs. In the absence of measurement standards, these certifications could not be supported. Other discrepancies were noted where the exact quantity or type of equipment used was not documented in case files although DoD Directive 5200.24 required such information. Sometimes case files did not show exact dates of usage, but only recorded the date the use was approved. Procedures further varied among investigative units on the periods of time for maintaining usage logs and related records.

Electronic Surveillance Data Indexes. The indexing systems used by the Military Departments to cross reference pertinent surveillance information were incomplete and did not contain the names of all identifiable persons whose wire/oral communications were intercepted. In other cases, addresses or telephone numbers (also required) were missing or only partially recorded. Further, although there was a 1975 requirement to establish a technical surveillance index, one Army investigative unit did not establish the index until early 1979 and used other indexes to answer data requests.

In 1974, the Department of Justice established the basic conceptual requirement for indexes. Upon receipt of the requirement, the responsible OSD office forwarded the requirement to the appropriate DoD investigative activities for implementation. However, DoD Directive 5200.24 was not revised to incorporate the indexing requirement until April 1978. In the absence of specific DoD guidance, each Military Department had developed its own methodology for keeping indexes. We contacted personnel at each of the locations where the indexes were maintained and found that these personnel, although basically familiar with the indexing requirement, lacked pertinent knowledge of internal control procedures. For example, none of the criminal investigative case files that contained surveillance data obtained with wiretap/eavesdrop equipment were marked to indicate that the data had been prepared for recording in the indexes. Listings used to record names in the indexes should have been in agreement, but were actually dissimilar, and names were recorded on one list but missing from another. In another instance, responsible personnel informed us that data were prepared for computer input but were never actually recorded in the indexes. Some files containing reports of criminal investigations that required indexing were misrouted. In other files, transcripts of conversations were improperly prepared, which precluded identification of the data to be indexed.

The responsibility for routine indexing generally rested with a single individual, usually a clerk. We believe that data to be indexed should be annotated, prepared and verified by different persons for more effective control. Similarly, we noted that quality assurance procedures were not being used to verify the accuracy of the transcriptions for the surveillance data. Because of the sensitivity of the data being handled, we believe more positive controls are needed. These would include independent verification of tapes, exact transcriptions of tapes when they are made, and recording in the indexes the names of all identifiable parties to a conversation including agents and confidential informants.

The basic intent for establishing the index concept was to facilitate data retrieval in a timely manner. However, this was hampered because uniform clerical and administrative procedures were not being used to accumulate and record data, and because index information on electronic surveillance data had not been centralized. While the Navy and Air Force had each established their indexes of electronic surveillance data in a single location, the Army had indexes at 4 different activities: the Criminal Investigation Command; the Intelligence and Security Command; the Special Operations Field Office; and the Law Enforcement Division, Office, Deputy Chief of Staff for Personnel. Presently, requests for surveillance data must be routed to all 6 locations.

Department of Justice Requests. We noted that some recent Department of Justice requests for surveillance data appeared to seek information over and above the guidance promulgated in 1974. These requests sought data on electronic surveillance authorized or received from any source, and whether DoD records reflected that another agency had at any time authorized, conducted or procured electronic surveillance. A particular surveillance may have been authorized but not used for a number of reasons; for example, the apprehension of a subject prior to use or the inability to set up a controlled situation for its use. In other instances, data may have been received from private sources who used their own equipment to record a harassing or obscene phone call. If data elements contained in the latest Department of Justice requests become the basis for indexing, then additional reviews of investigative files will be necessary. Conversely, we noted names in indexes which we believed did not belong there. Department of Justice guidance, as well as DoD Directive 5200.24, states that only the names of readily identifiable persons whose communications are intercepted should be indexed. However, we found the names of persons who were merely mentioned in the conversations intercepted, as well as partial names (first or last) having no other identifying data.

While we believe that revisions to existing electronic surveillance indexes are necessary, we also feel that DoD should

first request clarification from the Department of Justice about the extent and type of data to be maintained. After that occurs, it may be necessary to review investigative files, which contain such data, for accuracy. Also, it may be necessary to research prior requests for surveillance information against the updated index to revalidate the request.

Management Comments

The Director, Counterintelligence and Investigative Programs concurred in all but recommendation 2 and advised that action is in process to implement the remaining recommendations.

In response to recommendation 2 on the need to establish minimum levels of equipment, the Director stated:

> We agree that it would be desireable to have some calculus to establish standards, but believe this is not practical. . . . The small amount of purchasing in the last 5 years indicates the equipment accounts have not been bloated by unnecessary purchases. . . . As long as the amount of equipment is reasonable (i.e., not excessively large or small) we prefer to allow the best judgement of the respective agencies to stand.

Audit Response

DoD Directive 5200.24 Enclosure 2, "Procedures, Record Administration and Reports," requires Heads of the Military Departments to establish controls to ensure that only the minimum quantity of interception equipment required to accomplish assigned missions is procured and retained in inventories. The requirement to establish controls implies the use of objective criteria. Considering management comments that this is not practical, we believe the requirement should be deleted from Enclosure 2 and included as a general statement in the Policy section of the directive. Management comments on the other recommendations are responsive.

Defense Audit Service

Activities Visited

Department of Defense

Office of the Deputy Under Secretary of Defense for Policy Review, Washington, DC
Office of the Deputy Assistant Secretary of Defense(Administration), Washington, DC

Army

Deputy Chief of Staff for Personnel, Washington, DC

Assistant Chief of Staff for Intelligence, Washington, DC

U.S. Army Criminal Investigation Command, Falls Church, VA

U.S. Army Intelligence and Materiel Development and Support Office, Fort Meade, MD

U.S. Army Intelligence and Security Command, Arlington, VA

U.S. Army Special Operations Field Office, Berlin, Germany

Navy

Headquarters Naval Investigative Service, Alexandria, VA

Naval Investigative Service Resident Agent, Annapolis, MD

Air Force

Headquarters, U.S. Air Force Office of Special Investigations, Washington, DC

District 4, U.S. Air Force Office of Special Investigations, Andrews Air Force Base, MD

Other Government

Federal Bureau of Investigation, Technical Services Division, Directorate for Engineering, Washington, DC

COUNTERINTELLIGENCE