~~SECRET~~

Task Group Paper on Security of Classified or Sensitive Information

The protection of classified or sensitive information is normally provided by two general methods. One is through the prevention of access to the material by unauthorized persons, commonly called "physical security." The other is through encryption of information transmitted electrically which can be deciphered or understood only by authorized persons, commonly called "communications security." Various examples of physical security are safes, guards, clearances, and restricted dissemination. Examples of communications security (COMSEC) are cryptographic equipments or codes.

In the past, it has been relatively easy to draw lines (organizationally and technically) between the two methods. Physical security prevented access to information while COMSEC prevented those who listened to radio or wire electrical transmissions from understanding the information. This distinction is becoming increasingly more difficult to make as technological advances are made in both fields. For example, there are microphones and other "pickup" devices now available which not only permit one to listen to conversations in a room, but also to "break" or decipher the encryption system in that room and perhaps at dozens of locations around the world. Separate organizations, however, are concerned with these two aspects of the problem.

Communications Security (COMSEC)

Executive Order 10501, [illegible] November 5, 1953, has been interpreted to require that all classified information be encrypted before being transmitted through telecommunications.

The President, on October 24, 1963, directed the Secretaries of State and Defense to [illegible] the Committee of the U.S.I.B. on COMSEC matters. The Special Committee, with the concurrence of the Attorney General, and the DCI, approved on April 22, 1964, NSCID 5712, [illegible] which:

a. Established the U. S. Communications Security Board (State, Defense, Treasury, FBI, Army, Navy, Air Force, CIA, NSA, AEC);

b. Designated the Secretary of Defense as "Executive Agent of the Government for all COMSEC matters";

~~CONFIDENTIAL~~

c. Advised that NSA "shall act for the Executive Agent in all COMSEC matters set forth below" - primarily responsibilities for establishing adequate standards;

d. Defined COMSEC as "the protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study";

e. Defined telecommunications as "any transmissions, emission or reception of sign, signals, writing, images and sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system".

NSA prescribes Government-wide standards for the means of encryption - equipments, codes or other techniques - and only those approved by NSA may be used for the encryption of classified information. NSA also develops equipments where required. COMSEC equipments are available today to encrypt all standard communications methods - telephones, teletypewriter, high-speed data, television (black and white only), even computer-to-computer transmissions.

However, NSA has no authority to require encryption; the requirement for encryption is left to the agency head under the EO 10501. Moreover, they are positively prohibited from monitoring telecommunications to determine whether classified information is being revealed unless the agency head concerned approves in advance.

To date, there are no known telecommunications techniques which would permit unencrypted (clear) information to be transmitted safe from interception and from being read by unauthorized persons. As a result, the U. S. COMSEC Board and NSA make the assumption that all unencrypted telecommunications are being monitored and that the information being transmitted is compromised. While this is a physical impossibility, there can be no assurance that any particular transmission is not being intercepted and read. Therefore, NSA will assume no responsibility for the security of communications which are not encrypted in an approved cryptosystem.

The White House Communications Agency (WHCA) is responsible for providing all telecommunications for the President and to the White House, except for communications to and from the President's aircraft (Air Force I), which are the responsibility of the Air Force. WHCA is organizationally under the Defense Communications Agency (DCA). The WHCA program has not been reviewed by the Bureau. Kenneth O'Donnell provides policy guidance to the WHCA and has informed the DCA that no information on the size, program, or budget of the WHCA is to be revealed without his authority.

There is a very close working relationship between WHCA and NSA on all aspects of COMSEC, including possible "compromising emanations" as discussed below. However, WHCA has an impossible task in attempting to provide secure communications for the President so long as he uses the commercial telephone system. Unless WHCA can be informed of the specific locations and people to whom the President wishes to talk about sensitive or classified information, there can be no assurance that the conversations are not being monitored. However, if record communications (teletype) are involved, crypto-equipment can be quickly brought to the locations where a teletype capability exists. Crypto-equipments cannot now be installed for secure voice transmissions over the commercial telephone system.

Compromising Emanations

The above describes the traditional COMSEC problem where there is little relationship to the "physical security" problem, except insofar as physical security is required for the cryptographic equipment. In addition and more closely interrelated with the physical security problem is the problem of "compromising emanations" or radiation. Briefly, these are electrical or acoustic signals emanating from electronic and electro-mechanical equipments. If these signals can be intercepted, it is possible to read the information being processed by the equipment.

To protect against this danger, the U. S. COMSEC Board has approved (with concurrence by all concerned agencies including the Bureau) NSA electrical standards for all electronic or electro-mechanical equipments (computers, typewriters, etc.) which process classified information. [redacted] Each agency processing classified information through equipments is responsible for insuring that their equipments meet the standard.

A special subcommittee of the USCSB monitors this program and provides guidance and assistance to the concerned agencies. As might be expected, new offensive techniques are constantly being discovered which require additional defensive precautions. It is in this field that the line between communications security and physical security get fuzzy.

Physical Security

The term "physical security" has traditionally been associated with safes, guards, and fences. However, with the advent of sophisticated electronic eavesdropping techniques, most agencies have expanded the physical security role to provide protection against unauthorized access to classified or sensitive information either by people or by devices. [redacted] awareness of the threat posed by clandestine listening devices, the NSC, in December 1955, established a Special Committee on Technical Surveillance

Countermeasures. This Committee, composed of representatives of State, Defense (OSD and each Service), CIA, FBI and NSA, was charged with, inter alia:

a. Study and review of the domestic and foreign threat to the "security of classified defense information" presented by the "installation and operation of clandestine technical surveillance devices" in U. S. Government facilities or quarters.

b. Establishing and coordinating policies with respect to countering the threat.

The Committee meets at least monthly and submits annual reports to the NSC on its activities and findings. There is a close relationship between this committee and the USCIB committee on compromising emanations - in fact, there are a number of individuals who sit on both.

Each agency is responsible for carrying out its own technical surveillance functions within whatever common policy guidelines are established by the NSC committee (training, equipment to be used, etc.).

No clandestine devices of any kind have been discovered in the U. S. although over 100 were discovered in U. S. facilities overseas between 1949 and 1960. An additional 450 were discovered in friendly foreign overseas facilities between 1945 and 1960.

Conclusions

We are dealing with two separable (but in some measure interrelated) problems which in practice in Defense, CIA and other sensitive agencies involve two kinds of organizations. These are communications and physical security (protection against clandestine listening devices).

In the field of COMSEC, there already exists a clear assignment of responsibility to the Secretary of Defense as Executive Agent of Government for all COMSEC matters. The Secretary exercises his responsibility through NSA, recognized by all as a highly competent technical agency in this field. The Secretary receives policy guidance from an interagency board (USCIB) which has been fairly active and effective for its purpose. If the Board does not agree on matters before it, final actions are passed to the special committee of Secretaries of State and Defense.

Considering the case in point, we believe it would be appropriate for the White House (Mr. Bundy for the President) to request the Secretary of Defense to have NSA review and evaluate the President's Telecommunications facilities, including Air Force I, and to recommend actions to improve them. This task should include an examination of all equipments which process classified information to insure that no information may be

available to unauthorized persons through "compromising emanations." For a thorough evaluation, it may be necessary, if the White House desires, to request NSA to monitor White House communications on a sampling basis and advise the White House of the results.

On the matter of clandestine listening devices, the NSC Special Committee on Technical Surveillance Countermeasures should be charged with assessing the adequacy of the Secret Service procedures, equipment and level of technical skill, and recommending any changes necessary to attain the highest practicable level of performance.

We believe the Secret Service has the responsibility for protecting the Presidential establishment against clandestine devices since they support the Bureau on request. They are not members of the committee and, so far as we can determine, they do not receive committee reports nor do they contribute information to the committee. As a continuing matter, they should be made a member of the committee.

Recommended action:

1. That Mr. Bundy issue a NSAM providing that the Secretary of Defense, as Executive Agent for all communications security matters, will direct NSA to conduct a survey and make a report on the adequacy of present communications security measures in effect at the White House, including non-crypto communications.

2. That Mr. Bundy arrange through the NSC Special Committee on Technical Surveillance Countermeasures to secure a review and report on measures in effect at the White House to maintain surveillance and protection against clandestine listening devices.

3. That both reports be reviewed by the President's Committee on the Warren Report, augmented by Dr. Hornig and General O'Connell (OTM), for advice and recommendation to the President.