Sensitive Compartmented Information: Characteristics and Security Requirements

Prepared by
The
Security
Committee

June 1984

EXHIBIT A IN SUPPORT OF THE DECLARATION OF WILLIAM H. WEBSTER

Sensitive Compartmented Information:

Characteristics and Security Requirements

June 1984

Preface

This paper on the nature of sensitive Compartmented Information (SCI) and pertinent security controls was originally produced at the CONFIDENTIAL level in March 1984. It was intended for background use by legislative liasion officers responding to Congressional inquiries about SCI security requirements. It has been redrafted for issuance as an unclassified text because SCI security recently has become a matter of interest to all three branches of Government. The concept of providing special systems of compartmented protection to entire programs of intelligence collection and production is not widely known or understood. This paper is intended to assist those who must officially consider various aspects of SCI without the benefit of extensive experience with these programs.

In the continuing discussions of the appropriate security measures for protecting Sensitive Compartmented Information (SCI), including polygraph examinations and nondisclosure agreements, there has been little or no attention to what SCI is. These discussions raise issues about SCI which include:

> Does the nature of SCI lend itself to varying levels and kinds of security protection? Is the SCI accessed by "consumers" essentially different from the SCI dealt with by "producers"? Should some individuals be subject to stricter security screening for SCI access than others? Should the personnel of agencies not engaged in collecting or producing intelligence meet the same security standards for SCI access as those of intelligence agencies? Should political appointees be required to protect SCI from disclosure in the same manner as career federal employees? Are those who are granted access to SCI required to meet a higher standard of personnel security than those cleared for non-compartmented Confidential, Secret or Top Secret information? Is there a different assessment of acceptable risk in the SCI systems than for other classified information?

This report attempts to describe what SCI is, why it is sensitive, why the revelation of SC that an unwary individual might consider insignificant or trival can be damaging to an entire program for SCI collection, and why we should not be willing to accept any perceptible level of risk in decisions on personnel being granted access to SCI.

Sensitive Compartmented Information is data about sophisticated technical systems for collecting intelligence and the information collected by those systems. The characteristics of the systems that necessitated the development of SCI programs are (a) that compared to conventional intelligence activities employing human sources, many more people normally must know sensitive information in order to develop, build, and operate the systems and to analyze the material they collect; (b) that they generally produce large quantities of accurate, detailed intelligence, which is needed and relied upon by senior planners and policymakers, and which, by its nature, is extremely fragile, in that it reveals the characteristics of the systems that collect it; and (c) that they are extremely vulnerable to adversary countermeasures, i.e., denial or deception.

Most people can easily understand the need for tight security in classic espionage operations employing live agents. The need for strong security is dictated by the need for source protection and, of course, it is clear that the apprehension of an agent results in the loss of valuable intelligence. The neutralization of a technical collection system is more akin to the loss of a whole agent network than to the loss of a single agent and the loss of such systems has severe consequences. These include the loss of valuable intelligence

developing and producing new technical collection systems, which are extremely expensive, state-of-the-art programs; and the risks to the national security attendant to a lack of knowledge of what our adversaries are up to.

Communications intelligence, as defined by 18 U.S.C. 798, is the classic example of SCI, and normally is derived from intercepted communications. The unauthorized disclosure of such intelligence can reveal to the target country which of its messages are being intercepted and which ones are being read. If the targeted country takes the clearly indicated countermeasures, no further intelligence can be expected from that source and by that method. Similarly, the compromise of other technical collection systems, or intelligence derived from them, can tell our adversaries the capabilities of the systems and how to take countermeasures. Even worse, once the target country's government knows what the systems collect and how it is collected, it has the option of conducting deception operations, i.e., providing misleading data which may result in defective U.S. foreign and defense policies.

To guard against these risks, SCI security control systems have been evolved in the years since World War II, when the Japanese and German cryptographic systems were broken by the Allies, furnishing intelligence which was vital to victory over the Axis Powers. In structuring these systems, the lessons of Pearl Harbor have been borne in mind . . . the systems must permit timely dissemination of sensitive intelligence to those who need it to guide and carry out U.S. defense and foreign policy. Over the years, it has been demonstrated that the recipients' confidence in intelligence reporting has a direct relationship to the recipients' knowledge of the source or method producing it. Because of the amount of intelligence produced by the SCI systems and its broad utility, those with access to SCI number in the thousands.

The authority for SCI control systems is based upon the statutory responsibility of the Director of Central Intelligence (DCI), under the National Security Act of 1947, for the protection of intelligence sources and methods, and upon Executive Order 12356, which authorizes him to create special access programs for especially sensitive intelligence activities.

SCI systems, therefore, cover activities and information of extraordinary sensitivity and fragility from a security standpoint. They serve to restrict access to the protected information to persons who (a) have a clearly established official need for that information, and (b) who meet more rigorous and stringent personnel security criteria. Persons cleared for Confidential, Secret, or even Top Secret information are not automatically eligible by virtue of those clearances for access to SCI.

The personnel security criteria for access to all SCI are established by the DCI and are promulgated in Director of Central Intelligence Directive 1/14. Comparatively, the criteria for TS clearance require that denial be based upon a well-defined character or personality defect posing a threat to the national security. Because of the vulnerabilities and susceptibilities of SCI programs, special judgments must be made. In effect, no risk is tolerable where SCI is involved, and individuals who have been granted Top Secret

Top Secret does not automatically guarantee SCI access approval, the denial of SCI approval does not necessarily mean denial or revocation of TS clearance. This reflects the difference in the way SCI security is managed, and that it involves a higher order of security than non-SCI security.

SCI security control systems depend upon distinctive markings and restricted handling of material, stricter personnel security processing for access, and holding SCI material in "control centers" with physical and procedural barriers to preclude access by those who have not been formally approved. The SCI control systems provide an organized program for predetermining a generalized need-to-know regarding specific categories of intelligence and/or the sources and methods employed in their collection.

Everyone authorized access to SCI, regardless of that person's function, receives information that, if revealed to an unauthorized person, can compromise the system and reveal ways of countering it. Because the intelligence inherently is source-revealing, the reader of an SCI intelligence report is just as capable of revealing compromising data about a system as the builder or operator of the system. Material collected by SCI systems which does not reveal the characteristics and vulnerabilities of the source is considered to be sanitized and is disseminated outside compartmented channels.

In accepting sensitive compartmented information, the recipient accepts the accompanying responsibilities and restrictions in a most explicit way. Each individual approved for access is indoctrinated on the extreme vulnerabilities of the collection systems, the risk to the systems of the unauthorized disclosure of the intelligence they collect, and the rules for safeguarding SCI. As a condition of access, the newly approved individual signs an agreement to abide by the security rules for SCI.

To summarize, the rationale for SCI control systems includes the following concepts:

— Sources and methods producing quantities of high quality intelligence, which are extremely vulnerable to countermeasures, require an extraordinary degree of security protection.

— Extraordinary protection can be afforded by restricting knowledge of these sources and methods and, where necessary, the intelligence they produce, to persons who have been subjected to especially thorough security screening, whose knowledge of such information is required for the performance of functions essential to the national security, and who have entered into an agreement requiring that they protect these sources and methods in the manner prescribed by the U.S. Government.

— Because of the extreme vulnerability to countermeasures of the operations covered by SCI control systems, persons granted access to SCI must be determined by thorough investigation to be reliable and trustworthy. The objective of personnel security determinations for SCI access should be a risk-free population of approved individuals. Therefore, a substantially more vigorous personnel screening process

is necessary and a determination standard beyond that for other classified information must be used.

- Especially restricted channels are required for the transmission and use of data revealing the sensitive nature of these sources and methods, and of derived intelligence having the innate capability to compromise such data.

— Regardless of how carefully the security system is structured, the security of our secrets depends, in the final analysis, upon every person granted access. If any one of those entrusted with these secrets has vulnerabilities or susceptibilities which may be exploited, then our security can be breached. Every effort must be expended to avoid such an occurrence.