UDAC 87-123

Seminar for Unauthorized Disclosure Investigators
15 July 1987

Twenty-five Federal investigators, analysts, and supervisors concerned with the investigation of unauthorized disclosures of classified intelligence information met at the CIA Headquarters Building on 15 July 1987 to discuss the conduct of such investigations and how the process might be improved. The seminar was sponsored by the Unauthorized Disclosure Analysis Center (UDAC) of the Intelligence Community Staff. [redacted] 25X1

The Chief, UDAC, who served as moderator for the seminar, opened with a discussion of the UDAC's functions vis a vis leak investigations:

Extensive media review to detect potential unauthorized disclosures of classified intelligence information relating to sources and methods, including analytical processes, conclusions, finished intelligence reports and other aspects of the intelligence process.

Authentication procedures to determine that the apparent disclosure is a first-time public revelation of classified intelligence, including, where possible, identification of reports, briefings or documents on which the disclosure might be based.

Notification of the DCI, CIA's General Counsel, and other departments or agencies whose interests might be affected; requesting notification of the Department of Justice that an unauthorized disclosure has occurred; determination of whether to request investigation by the FBI; and efforts to ensure that all intelligence leaks are reported to the Department of Justice to establish a "track record" demonstrating that intelligence leaks occur frequently and, apparently, uncontrollably. [redacted] 25X1

[redacted] reference librarian assigned to the UDAC, briefed the seminar on the use of commercial databases as a valuable tool in the authentication, investigation and analysis of unauthorized disclosures. She described the capabilities of the public systems currently available, especially those relating to science and technology information of the type commonly disclosed without authorization. She noted that the systems of particular value to unauthorized disclosure investigations are current to within 24-to-48 hours. [redacted] 25X1

25X1 [redacted]

[redacted] chief of information services for the UDAC, explained the selection and preparation of data for inclusion in the Register of Unauthorized Disclosures of Intelligence (RUDI). He discussed the form used to record and transmit data to the computer and stressed the importance of both accuracy and completeness. Information from RUDI, he said, is used to prepare reports and analyses for use by senior managers in understanding the leak problem, for developing possible leads to investigation of unauthorized disclosures, and to promote efforts to stop classified leaks. [redacted] provided statistics on reports of disclosures and investigations sent to the UDAC by Intelligence Community agencies and services. He reported the database currently has information on 518 compromises in recent years, including items covered in the June 1984 DCI Security Committee Survey of Unauthorized Disclosures of Classified Intelligence FY 1979-FY 1983, and approximately 400 that have occurred since October 1983, the closing date of that study. [redacted] described a second database of "non-leaks," which records published articles that appear to be first-time leaks of classified intelligence, but which are determined to have been published previously, unclassified, or otherwise not qualified for inclusion in the leak database. Recording the authentication process resulting in the determination, he said, can eliminate redundant future efforts involving similar published information. The automated system has been announced in the Federal Register and specialized searches of the system can be done for investigators to support their efforts in specific cases. [redacted]

STAT

25X1

25X1

25X1

[redacted] consultant to the UDAC, provided technical information on the hardware and software used by the UDAC in maintaining the Register (RUDI) and in producing the UDAC's reports. [redacted]

25X1

25X1

The moderator briefed the participants on the UDAC Unauthorized Disclosure Summary, a limited dissemination publication for the purpose of keeping senior officials aware of the nature and scope of the unauthorized disclosure problem. He advised that all disclosures and investigations reported to the UDAC during the October 1983-December 1986 period had been submitted to the originating agencies for validation, amendment or additions, where appropriate. The revalidated material will be used by the UDAC in an update of the 1984 leak study. [redacted]

25X1

In the open discussion that followed, one participant noted that a problem for leak investigators is the lack of feedback on the outcome of cases. Some leaks may be investigated by several agencies, but the individual investigators ordinarily do not learn the outcome of the case, what investigative techniques worked well and what did not, etc. There was general agreement that this is a significant problem that diminishes the effectiveness and raises the cost of leak investigations. One attendee suggested a centralized database in which information on leak investigations would be indexed and made available to leak investigations throughout the Community. Subsequent discussion raised the issues of privacy and third-agency restrictions, but there was support for exploring the possibility of making more data available to investigators. [redacted]

25X1

Dr. Robert M. Gates, Deputy Director of Central Intelligence, addressed the seminar, saying there has been "too much fingerpointing on leaks" when there is "plenty of blame to go around." He suggested that the Executive Branch probably is responsible for most leaks, despite repeated charges that the Congress is leak-prone. It appears that most leaks come from senior officials, he said, but it is difficult to determine whether the discloser's action is malicious, inadvertent, a high-level policy ploy, or has another purpose. He also expressed a tendency to agree with the perception that the higher-up the offender, the less likely it is that the leaker will be penalized. 25X1

Among the senior people who leak, Dr. Gates said, many apparently don't even recognize that they are leaking. He noted that in his experience, those suspected of leaking often do not realize the danger or the costs of their actions. "We must educate them to the consequences of disclosures of intelligence," he said. 25X1

The DDCI believes some things can be done about the leak problem. One is to investigate vigorously to identify those who leak and take action against them. Another is to increase the degree of cooperation among agencies charged with investigating such disclosures. It is necessary, he said, to recognize what is important and what is not, i.e., setting priorities in allocating investigative resources. Similarly, recognition of the elements that reflect the potential for fruitful investigation is also important e.g. how many people had access to the information. 25X1

Dr. Gates emphasized to the attendees that despite the popular perception that senior level leakers get away with it and junior level leakers are punished, "As far as Director Webster and I are concerned, if you investigators make a strong case, we are prepared to take these issues to the highest levels of the government, without regard to the rank of the offender." 25X1

After a break, the moderator reviewed some familiar problems associated with leak investigations, including the broad dissemination of classified data, the consensual nature of the act of leaking, investigative policy constraints, the time criticality of leak investigations, etc. A general discussion, led by a panel of four attendees, attempted to explore problems, techniques, and the infrequent successes in investigating unauthorized disclosures of classified intelligence. One echoed Dr. Gates's remarks about high-level disclosers and the difficulty of determining whether the disclosures are officially authorized, partially sanctioned, or totally unauthorized. He noted that the attitude in the Executive Branch toward leaks is lax, and pointed to the disclosures that followed the Berlin disco bombing. He expressed the belief that there is now greater professionalism in leak investigations and more probability of success, particularly in taking administrative action against leakers, but "it takes its toll, it wears investigators down." 25X1

The discussion included thoughts on how leak investigators might improve their techniques, especially through the use of an indirect approach. It was generally agreed that direct, confrontational interviews of suspects were not likely to yield good results. In one case, several suspects denied knowing the reporter who published the leak under investigation. One of them was determined, through a review of visitor logs, to have sponsored visits by the reporter to his building. Confronted with evidence of his effort to deceive investigators, the suspect chose to resign rather than have the investigation continue. Later, an associate of the suspect, while undergoing a routine polygraph examination for assignment to a sensitive agency, admitted he had been present when the suspect had revealed classified information to a journalist on another occasion. 25X1

One experienced investigator expressed concern about acceptance of the attribution used by reporters in publishing classified information. For example, he cited the deception in which a reporter draws a correct conclusion and attributes the story to a notional source. He recalled a case in which a reporter attributed an unauthorized disclosure to "White House sources" in order to protect the Congressional committee staffer who was his actual source. The moderator noted that although attribution may be inaccurate or deliberately misleading, it is the only consistent measurable offering any insight at all into sourcing. The moderator wondered how often it has been determined that media people have used deceptive sourcing in their stories. 25X1

Another participant noted that CIA and NSA have the heaviest case loads of unauthorized disclosure investigations. He stressed that this does not indicate that more leaks emanate from CIA and NSA, but that more information originating from or affecting these agencies is leaked. He pointed out the heavy demands for manpower these leaks entail and the extensive coordination they require, as well as the high costs of changing or replacing collection systems to remedy the impact of unauthorized disclosures involving sensitive sources and methods. 25X1

All of those in attendance lamented the scarcity of human resources devoted to the investigation of leaks. It was pointed out that the FBI does not have enough investigators to develop the kind of information that can be produced by preliminary internal investigations conducted by individual elements of the Intelligence Community. It was noted that the FBI's sole function in this field is to develop prosecutable cases. Another participant reminded the meeting that it can be productive for the individual agencies to continue internal investigations even after FBI assistance has been requested. The moderator noted that NSDD 84 provided that the FBI could investigate leaks even in cases where administrative action, rather than prosecution, was likely to result. 25X1

It was explained that in order to bring a leak case to prosecution, the leaker must be identified and there must be evidence the leaker had reason to believe the disclosure would harm the United States or assist a foreign nation. This involves a Catch-22 for the investigator. If he obtains an admission of complicity, it is difficult to secure an admission of intent. Or, if the suspect acknowledges the disclosure is harmful, it is unlikely that he will admit to the act that he described as damaging to the national security. In the event it is impossible to obtain an admission that the suspect was aware of damage to the national security, it may be possible to secure such evidence from a second party or indirectly, through a previous acknowledgment by the suspect that such disclosures are damaging. [redacted] 25X1

There was extensive discussion of the need to answer the "11 questions" asked by the Department of Justice (DOJ) in unauthorized disclosure cases. It was suggested that time can be saved by answering the questions, including whether the disclosed information can be declassified to permit its use in court during prosecution. It was noted that DOJ does not ordinarily initiate cases which do not lead to prosecution, although in some cases a fallback position may be taken when prosecution proves impossible or impractical which permits the offender's parent organization to take administrative action. In cases going to prosecution, the importance of "jury appeal" was stressed, citing the Morison Case as one in which certain facts, e.g., that the defendant was being paid for information by a foreign publication, probably influenced the jury. [redacted] 25X1

One participant, discussing special inquiries into possible leaks, spoke of the need for a systematic approach. It is most important to find the best qualified geographical or technical specialists, for example, to provide validation and damage estimates. Such specialists are most likely to be aware of any officially-approved "backgrounders," a vital consideration in determining how to proceed with an investigation. Within his agency, the attendee said, a systematic validation process helps to eliminate those cases in which the leaked information originated with another agency, or was misrepresented by the media as classified when it was not, or where a source document cannot be located or a cited classified briefing cannot be verified, or, as is often the case, the leaked intelligence was so widely disseminated that investigation would be impractical. The speaker stressed the importance of developing strong cases and not gaining the reputation of "crying wolf." [redacted] 25X1

In response to a question, a participant advised that interviews of reporters to elicit information concerning the source of an unauthorized disclosure are rarely done because of policy considerations and because reporters will not answer the question anyway. In one of the rare exceptions, the participant recalled, the reporter's editor-in-chief became incensed and contacted the head of the investigator's agency to demand that such inquiries be handled "at the director's level." [redacted] 25X1

The previously-established focal point system for Community agencies to report intelligence leaks was raised. A straw vote determined that none of the attendees knew the identity of the current (or last extant) focal point for his or her agency. It appears that when the initial focal points transferred or retired, a replacement was not appointed or if one was appointed, the designation was not communicated to those who needed to know.

25X1

Various efforts by members of congress or executive branch agencies to seek legislation specifically outlawing unauthorized disclosures of classified information were reviewed; these include HR 1082, Title IV, "Federal Employee Unauthorized Disclosures of Classified Information Act," introduced by Rep. Bob Stump in 1985; and HR 271, Sec. 509, "Unauthorized Disclosure of Classified Information" introduced by Rep. Charles E. Bennett in 1985; and various CIA efforts to draft anti-leak legislative proposals. It was pointed out that none of these has reached the floor of either house. The suggestion was made that a Director of Central Intelligence Directive on unauthorized disclosures be issued, but it was agreed that without legislative relief, such a DCID probably would not have much impact on the situation.

25X1

One attendee expressed the opinion that the possibility of prosecution may be stronger under the Uniform Code of Military Justice than in civilian courts. Cases rejected by the DOJ might be prosecutable under the UCMJ if the suspect is subject to it.

25X1

25X1

Some of the baser aspects of leaker motivation, as established through investigation, included leaks designed to assist companies in which the leakers held stock and those calculated to gain favor with a company in which the leaker had prospects of employment after retiring from the government.

25X1

The practical advantages of "graymail" legislation in assisting prosecution of leak cases were discussed. The Classified Information Procedures Act is primarily helpful in cases where the court will accept a redacted copy of the compromised document, with the classified information deleted and replaced with a non-sensitive description of what was removed. If the court declines to permit deletion of sensitive material, the government has two choices: reveal the secrets in open court or drop the prosecution.

25X1

In summary, the group agreed that there is a need to enforce need-to-know over wide dissemination; to support the educational efforts advocated by the DDCI; to stimulate activism against the continued use of classified information to further policy objectives; and to recognize and beware of the skills of the media in eliciting classified data. In light of current attitudes and policies, the "best shot" is to seek administrative action against leakers. [redacted] 25X1

The seminar extended 30 minutes beyond its scheduled termination because of active discussion. It developed a consensus that it is important to share ideas and techniques, even if they must be expressed in hypothetical terms to protect sensitive information, to help all leak investigators benefit from the experience of others. There was considerable sentiment for another seminar soon, with more time allocated to sharing experiences and problem-solving exercises, preferably a two-day off-site meeting. [redacted] 25X1

SUBJECT: Notes on 15 July 1987 Leak Investigator Seminar [redacted] 25X1

Distribution: UDAC 87-123 ~~w/att~~
1-D/ICS; DD/ICS
1-D/CCISCMO
1-D/OCA
1-D/PAO
1-OGC
1-DOJ
1-FBI
1-OACSI
1-STATE
1-NIC
1-DIA
1-CIA
1-AFIS/INS
1-NSA/M5
1-UDAC Chrono
1-UDAC Subj
1-C/AP/UDAC
1-ICS/R

UDAC/ICS: [redacted] 07/29/87) 25X1