Shocking Security Breakdown Shown in Hanssen Report

by Edward Spannaus

Despite some superficial changes, the internal culture of the FBI seems not to have changed much, since the days of the notorious J. Edgar Hoover. That is the only conclusion to be drawn from the findings of the report on FBI security procedures issued in early April, growing out of the Robert Hanssen espionage case. When supplemented by the observations of present and former FBI officials, it makes clear that the internal life of the Bureau is dominated by bureaucratic, career-advancement considerations of "playing it safe," and "don't rock the boat," rather than a mission-orientation around the national security of the United States.

The newly issued report, "A Review of FBI Security Programs," is the product of a year-long investigation carried out by a special commission headed by William Webster, former Director of both the FBI and CIA. A declassified version was released on April 4.

FBI Security Failures

The report documents the complete breakdown of the most rudimentary security procedures in the FBI and the Justice Department. Over more than 20 years, FBI Special Agent Hanssen was able to obtain and pass on to the Soviets and then to the Russians, volumes of highly classified material and information, without ever being detected by the FBI—although there were numerous actions on his part which should have set alarm bells ringing.

The report showed that Hanssen was able to gain access to supposedly secure computer data bases, download or print out "reams of highly-classified information," and walk out of FBI facilities with thousands of classified documents. The FBI was tipped off a number of times that he was behaving suspiciously, yet he continued his spying unimpeded, until apparently exposed by a Russian security official to the FBI at the beginning of last year.

The Webster Commission conducted extensive interviews with Hanssen, and with hundreds of other FBI officials. The report describes the Hanssen case as "possibly the worst intelligence disaster in U.S. history," in which Hanssen, over the course of 22 years, "gave the Soviet Union and Russia vast quantities of documents and computer diskettes filled with national security information of incalculable value."

"As shocking as the depth of Hanssen's betrayal," the report declares, "is the ease with which he was able to steal material he has described as 'tremendously useful' and 'remarkably useful' to hostile foreign powers.

"Hanssen also did not hesitate to walk into Bureau units in which he had worked some time before, log on to stand-alone data systems, and retrieve, for example, the identities of foreign agents whom U.S. intelligence services had compromised, information vital to American interests and even more immediately vital to those whose identities Hanssen betrayed."

The commission found what it calls "significant deficiencies" which it says "flow from a pervasive inattention to security, which has been at best a low priority. . . . In the Bureau, security is often viewed as an impediment to operations, and security responsibilities are seen as an impediment to career advancement."

Ironically, some changes made after Sept. 11 only made things worse. In an effort to provide broader access to information, the already-weak restrictions on the FBI's automated records system were weakened further. One result, was that there was general access throughout the FBI to information obtained from national-security wiretaps and electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). "The use of that information in criminal investigations is tightly restricted by Constitutional considerations and Department of Justice guidelines," the report notes; yet this

highly classified information was broadly disseminated, violating the "need to know" principle.

Hanssen's Strange Spy Career

The report discusses three phases of Hanssen's espionage activities. The first was 1979-81, during which he gave the Soviets the identity of a high-ranking Soviet military intelligence officer who was a "defector-in-place" for the United States. In 1981, after transfer from New York to FBI Headquarters in Washington, Hanssen supposedly broke off contact with the Soviets, and told his wife, his priest, and his attorney about his espionage. The priest, a fellow member of the Opus Dei order, told Hanssen that he should donate the money received from the Soviets to charity, and pray for forgiveness. (The role of Hanssen's associates in Opus Dei, and at the Opus-Dei-linked St. Catherine of Siena parish in Great Falls, Virginia, has yet to be explained. FBI Director Louis Freeh, Supreme Court Associate Justice Antonin Scalia, and other high-ranking U.S. government officials are also parishioners at St. Catherine's.)

Hanssen's second spying period began in 1985 and continued until the 1991 fall of the Soviet Union. During this time, he gave the Soviets a "complete compendium of double-agent operations." An FBI internal report at the time noted serious compromises and disruptions in FBI recruitment of agents, and double-agent operations; it raised the possibility that the KGB had "somehow acquired inside or advance knowledge" of FBI operations—but the FBI never made any connection to Hanssen.

In 1993, Hanssen attempted to re-establish contact with Russian intelligence—and the Russians protested his approach, to the U.S. government. The FBI opened a case on the protest—but nothing came of it.

In October 1999, Hanssen began his third phase of espionage, which ended with his arrest on Feb. 18, 2001. He was done in by a Russian who provided key information and material to the FBI—not by any FBI investigation.

It is clear that the most cursory internal security efforts would have turned up clear evidence of Hanssen's spy activities, including his multiple bank accounts with deposits far exceeding his FBI salary, his frequent break-ins to sensitive FBI data-bases bypassing normal log-in procedures, and his regular smuggling of reams of classified documents out of the FBI headquarters building. Even when suspicions about Hanssen's activities were brought to the attention of the appropriate Justice Department and FBI officials—including a report by his own brother-in-law—no action was taken.

The unclassified portions of the Webster report constitute a damning indictment of the FBI's security breakdown; this may only be the tip of the iceberg, given what is likely to be contained in the secret, classified portions of the report. The report is not a damage-assessment of the consequences of Hanssen's espionage, nor does it delve into Hanssen's sexual perversions which have been reported elsewhere—which include his relationship with a stripper, whom he gave expensive gifts and took to church at St. Catherine's, and his extensive display of his sexual fantasies on Internet chat-rooms.

As one former FBI official told *EIR*, simply revamping security procedures within the Bureau will not be sufficient. The entire internal culture of the Bureau—with its competing fiefdoms of 56 separate field offices, 27 "Legat" offices in U.S. Embassies overseas, and the bureaucratic criteria by which promotions are awarded and careers advanced—would have to be overturned if the problems identified in the Webster report were to be tackled seriously.

The Comverse Leak Point

Another element of the FBI's security problems, not cited in the Webster report but already documented by *EIR*, is its penetration by Israeli security services. As we have shown (*EIR*, Dec. 21, 2001 and Feb. 1, 2002), a major supplier of wiretap equipment to the FBI and other law enforcement agencies, is Comverse Technologies, Inc., a company founded in Israel in 1982 by an Israeli military intelligence officer. Comverse does most of its manufacturing in Israel, where it is heavily subsidized by the government. FBI and other intelligence officials suspect Comverse is a source of leaks of law-enforcement and intelligence information; it has been a matter of intense controversy within the FBI and Justice Department.

Under the 1994 Communications Assistance for Law Enforcement Act (CALEA), wiretapping was transformed. Instead of the old system of tapping into individual phone lines, now, using Comverse software, law enforcement agencies use computers and software that tap into the elaborate nationwide system of telephone switchers and routers, grab the targetted phone conversations into computers, and transmit them to investigators authorized to do the wiretaps. Comverse manages and maintains the computers and the software, giving the firm potential access to all of the data.

According to a Fox News report, "Attorney General John Ashcroft and FBI Director Robert Mueller were both warned Oct. 18 in a hand-delivered letter from 15 local, state, and Federal law enforcement officials, who complained that 'law enforcement's current electronic surveillance capabilities are less effective today than they were at the time CALEA was enacted.' " What troubles investigators most, Fox reported, is that in some New York cases, "certain suspects have altered their behavior dramatically, right after supposedly secret wire taps have begun . . . and it has many gravely concerned that they were tipped in advance."

"But investigators within the DEA, INS, and FBI," Fox noted, "have all told Fox News that to pursue, or even suggest Israeli spying through Comverse is considered career suicide"—exactly the same problem suggested by the Webster report, and identified more strongly by others, that the internal structure and culture of the Bureau discourage any effective security procedures.