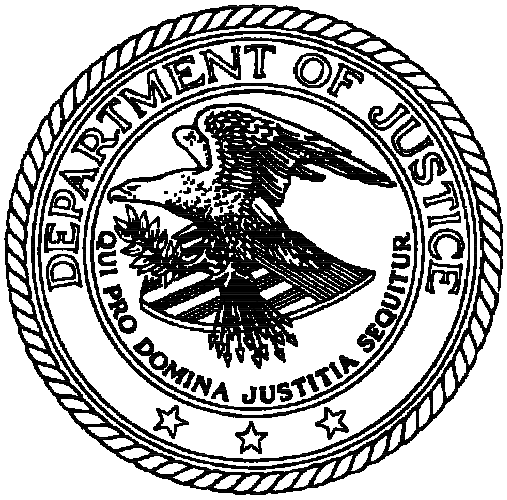
U.S. Department of Justice



A Review of FBI Security Programs

Commission for
Review of FBI Security Programs
March 2002

Commission for the Review of FBI Security Programs
United States Department of Justice
950 Pennsylvania Avenue, NW, Room 1521
Washington, DC 20530
(202) 616-1327 Main
(202) 616-3591 Facsimile

March 31, 2002

The Honorable John Ashcroft
Attorney General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Attorney General:

In March 2001, you asked me to lead a Commission to study security programs within the Federal Bureau of Investigation. Your request came at the urging of FBI Director Louis Freeh, who had concluded that an outside review was critical in light of the then recently discovered espionage by a senior Bureau official.

In discharging my duties, I turned to six distinguished citizens as fellow Commissioners and to a staff of highly qualified professionals. I want to acknowledge the diligence with which my colleagues pursued the complex matters within our mandate. The Commission took its responsibilities seriously. It was meticulous in its investigation, vigorous in its discussions, candid in sharing views, and unanimous in its recommendations.

When I agreed to chair the Commission, you promised the full cooperation and support of the Department of Justice and the FBI. That promise has been fulfilled. I would like to thank the Department's Security and Emergency Planning Staff for the expert help they gave us, and I especially commend the cooperation of Director Mueller and FBI personnel at every level, who have all been chastened by treachery from within.

I am pleased to submit the report of the Commission for the Review of FBI Security Programs.

Sincerely,

William H. Webster

Commission for the Review of FBI Security Programs

William H. Webster, *Chairman*

Commissioners

Clifford L. Alexander, Jr.

Griffin B. Bell

William S. Cohen

Robert B. Fiske, Jr.

Thomas S. Foley

Carla A. Hills

- - - - - -

Commission Staff

Michael E. Shaheen Jr.
Director and Chief Counsel

Richard M. Rogers George Ellard
Deputy Chief Counsel Deputy Chief Counsel

Charles Alliman
Joshua G. Berman
Donald R. Bailey
Steven E. Baker
Thomas E. Boyle
Robert R. Chapman
David E. Conway
David H. Cogdell
Charles W. Dixon
Kevin A. Forder
Daniel W. Gillogly
Currie C. Gunn
William B. Hackenson
Zachary J. Harmon
Alan Hechtkopf
Terry J. Ihnat
Carl Jaworski
Wilbur J. Hildebrand, Jr.
Marcia Hurtado
Willard F. Kelchner
Michael D. Kushin
Dale Long
Daniel W. McElwee, Jr.
John W. Mildner
Marie A. O'Rourke
Gail A. Ospedale
Claudia Peacock
Iqbal N. Qazi
Kevin M. Reinhard
Stephen C. Stachmus
Cinthia Trask
Wayne A. Van Dine

Norman A. Van Dam

Contents

EXECUTIVE SUMMARY

The Commission for the Review of FBI Security Programs was established in response to possibly the worst intelligence disaster in U.S. history: the treason of Robert Hanssen, an FBI Supervisory Special Agent, who over twenty-two 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 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 usually collected this material in the normal routine of an FBI manager privy to classified information that crossed his desk or came up in conversation with colleagues. Before going to some prearranged "drops" with Soviet and Russian agents, Hanssen would simply "grab[] the first thing [he] could lay [his] hands on." In preparation for other acts of espionage, which he might have months to anticipate, Hanssen was more systematic. He was proficient in combing FBI automated record systems, and he printed or downloaded to disk reams of highly classified information. 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 US intelligence services had compromised, information vital to American interests and even more immediately vital to those whose identities Hanssen betrayed.

During our review of FBI security programs, we found significant deficiencies in Bureau policy and practice. Those deficiencies 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.

Until the terrorist attacks in September 2001, the FBI focused on detecting and prosecuting traditional crime, and FBI culture emphasized the priorities and morale of criminal components within the Bureau. This culture was based on cooperation and the free

flow of information inside the Bureau, a work ethic wholly at odds with the compartmentation characteristic of intelligence investigations involving highly sensitive, classified information.

In a criminal investigation, rules restricting information are perceived as cumbersome, inefficient, and a bar to success. A law-enforcement culture grounded in shared information is radically different from an intelligence culture grounded in secrecy. The two will never fully co-exist in the Bureau unless security programs receive the commitment and respect the FBI gives criminal investigations. Even the latter, employing their own sensitive information and confidential sources, will benefit from improved security.

The focus on criminal investigations as the core function of the FBI and the perception of those investigations as the surest path to career advancement has had an important consequence: operational imperatives will normally and without reflection trump security needs. For instance, senior Bureau management recently removed certain security based access restrictions from the FBI's automated system of records, the principal computer system Hanssen exploited, because the restrictions had hindered the investigation of the terrorist attacks. This decision might make a great deal of sense operationally; however, it was made essentially without consulting the Bureau's security apparatus. One result, surely unforeseen and unintended, was general access within the Bureau to information obtained through warrants under the Foreign Intelligence Surveillance Act. The use of that information in criminal investigations is tightly restricted by Constitutional considerations and Department of Justice guidelines. Highly classified FISA information, unidentified as to source and generally disseminated to FBI investigators, violates the basic security principle that such information should be circulated only among those who "need to know."

Operational efficiency is important, especially when our country might be under terrorist siege, and tightening controls on classified information will come with a cost to efficiency and resources. With this in mind and recognizing that we cannot eliminate intelligence efforts directed against us, the Commission attempted to recommend changes

in FBI security programs that will minimize the harm those who betray us can do and shorten the time between their defection and detection. Accordingly, the recommendations we make are intended to address significant flaws in the process through which the Bureau generates and implements security policy and protocols for classified information. We believe that, if these recommendations are followed, a workplace culture will be established that recognizes security lapses as significant, restricts access to particular items of classified information to those who need them to perform their jobs, and makes disloyal employees more quickly visible. If these goals are met, the FBI will strike a sound balance between security and operational efficiency.

To this end, we focused our investigation on four areas: the structure of the Bureau's security programs and the policies and procedures designed to ensure the integrity of its personnel, information systems, and documents.

An important component of our work consisted of gathering information about security organization in other agencies so that we could incorporate into our recommendations "best-practices" within the Intelligence Community. Other agencies have substantially enhanced the responsibility and visibility of their security programs within the past few years, often as a consequence of intelligence penetrations. Although the FBI has begun to take steps to improve security, senior management has not fully embraced the changes necessary to bring Bureau security programs up to par with the rest of the Intelligence Community. In general, FBI security programs fall short of the Community norm.

To correct these deficiencies, the Bureau's security function must be given stature, resources, and visibility, and Bureau senior management must commit to a security program as a core FBI function. Accordingly, our principal structural recommendation is that the FBI establish an independent Office of Security, led by a senior executive reporting to the Director, responsible for developing and implementing all Bureau security programs. The Office of Security must have the authority to take critical security issues to the Director and

speak with the Director's support.

The Commission also recommends that the FBI consolidate its security functions, which, in sharp contrast to other agencies, are fragmented, with security responsibilities spread across eight Headquarters divisions and fifty-six field offices. Consolidating security functions under a senior executive leading the new Office of Security will prompt management to focus on security, resolve conflicts between operational and security objectives, and foster Headquarters and field coordination.

The Bureau's Office of Security must develop programs to address information system security. Presently, no unit within the FBI adequately addresses this function, a failure whose consequences can be seen in Hanssen's perfidy. Bureau personnel routinely upload classified information into widely accessed databases, a form of electronic open storage that allows essentially unregulated downloading and printing. This practice once again violates the most basic security principal: only personnel with security clearances who need to know classified information to perform their duties should have access to that information. In spite of the practically unrestricted access many Bureau employees have to information affecting national security, the FBI lags far behind other Intelligence Community agencies in developing information security countermeasures. For instance, an information-system auditing program would surely have flagged Hanssen's frequent use of FBI computer systems to determine whether he was the subject of a counterintelligence investigation.

We also recommend significant changes in the background investigations potential Bureau personnel undergo before receiving initial security clearances and in the periodic reinvestigations on-board personnel undergo for security concerns. We believe that all personnel should be subject to financial disclosure obligations and that those with access to certain particularly sensitive information and programs should take counterintelligence scope polygraph examinations during their reinvestigations.

Unlike other Intelligence Community agencies, the FBI does not foster the career development of security professionals. Security responsibilities are often foisted onto agents as collateral duties, which they eagerly relinquish to return to criminal investigations that promise career advancement. Career tracks should be developed for Security Officers to professionalize these positions and make them attractive.

Bureau security training programs for new agents and on-board personnel are also in great need of improvement. The new Office of Security must develop effective, mandatory security education and awareness programs for all personnel.

The Bureau does not have a viable program for reporting security incidents to Headquarters. Currently, several components play uncoordinated roles in detecting, investigating, and assessing security violations; no single entity has authority to coordinate, track, and oversee security violations and enforce compliance. The Bureau is unable to identify or profile components and personnel who engage in multiple security violations, even when they constitute a pattern. The new Office of Security must address these deficiencies.

The FBI's approach to security policy has been as fragmented as the operation of its security programs. Because no single component is responsible for security policy, critical gaps in security programs have developed. Some of the weakest links in security have resulted from unwritten policies and from implementation of security policies without input from security program managers. The FBI should emulate other agencies by embedding security policy development into its management structure to ensure that security programs are recognized and respected and that security is not inappropriately sacrificed to operational objectives.

Our report is critical of the FBI and with justification. However, we recognize that the Bureau has taken many steps, in light of Robert Hanssen's treason, to improve security. Furthermore, in consistently finding the Bureau's security policy and practice deficient when compared with security at other entities within the Intelligence Community, we do not mean

to single out the FBI for criticism. The security programs in most agencies to which we turned to develop a best-practices model have resulted from radical restructuring made necessary as one after another agency discovered that its core had been penetrated by disloyal employees working for foreign interests. Had the FBI learned from the disasters these agencies experienced, perhaps Hanssen would have been caught sooner or would have been deterred from violating his oath to the Bureau and his country. But it is equally true that, had those agencies learned from disturbing patterns of espionage across the Intelligence Community, other treacherous moles might have been caught or deterred. Consequently, in addition to the particular recommendations about Bureau policies we make in our Report, we also make a more global recommendation: a system should be established whereby security lapses in particular entities lead to improved security measures throughout the entire Intelligence Community.

In sum, we do not mean to gainsay the steps the Bureau has taken since Hanssen's arrest to safeguard national security information. Many of those steps have been significant, as has the Bureau's cooperation as we conducted our review. However, before the Bureau can remedy deficiencies in particular security programs, it must recognize structural deficiencies in the way it approaches security and institutional or cultural biases that make it difficult for the FBI to accept security as a core function.

INTRODUCTION

I could have been a devastating spy, I think, but I didn't want to be a devastating spy. I wanted to get a little money and to get out of it.

– Robert Hanssen

In March 2001, Attorney General John Ashcroft established a Commission for the Review of FBI Security Programs to analyze and recommend improvements to security programs within the Federal Bureau of Investigation. The review was occasioned by the discovery of espionage of perhaps unparalleled scope committed by Robert Hanssen, an FBI Supervisory Special Agent, who over a span of twenty-two years gave the Soviet Union and Russia vital information affecting United States security.[1]

Hanssen began his Bureau career in January 1976 and served continuously as an FBI agent until his arrest in February 2001. For most of this time, Hanssen worked in the Bureau's Intelligence Division, later known as the National Security Division, both at FBI Headquarters and in the New York City Office. In his capacity as an investigator and as a Bureau manager, Hanssen had access to the most sensitive classified information about the foreign intelligence and counterintelligence activities of the FBI and other agencies in the U.S. Intelligence Community.

In March 1979, Hanssen was detailed to the Soviet Counterintelligence Division within the Bureau's New York City office to help establish an automated counterintelligence data base. In the same year, he started to cooperate with Soviet intelligence after he had been assigned as a Special Agent to a Soviet Foreign Counterintelligence squad in New York. Hanssen claims that his motivation was economic: the pressure of supporting a growing family in New York City on an inadequate Bureau salary. His aim was to "get a little money" from espionage and then "get out of it."

In 1979, Hanssen "walked" a document into the offices of a company in New York

---

[1] The Commission assembled a staff of thirty-five persons, who over the course of a year conducted approximately four-hundred interviews, reviewed relevant material, and spoke with Hanssen on four occasions. The Commission met five times to take testimony, consult with staff, and prepare our report, the bulk of which can be found in classified appendices to the public report.

run by an officer in the Soviet military intelligence service. The document contained information about the Bureau's penetration of a Soviet residential complex.

Hanssen made two other "drops" during this initial period of espionage, for which he received around $20,000. In a letter to the Soviets complaining that the first of three payments was insufficient, Hanssen revealed that he was an FBI agent. During one of these drops, he gave the Soviets a list of known and suspected Soviet intelligence officers that had come to him, in his words, "in the normal course of business," which included supervising an automated data system and creating a monthly report summarizing his Division's response to Soviet intelligence operations. Hanssen also identified a Soviet officer as "Top Hat," a defector-in-place for the United States and the highest ranking military intelligence officer ever to spy for the West.[2] Hanssen disclosed Top Hat's identity because he feared that the Soviet officer might be a threat to him.

Hanssen communicated with the Soviets through encoded radio transmissions, using a "one-time pad," a practically unbreakable cipher he created.

When Hanssen was transferred to FBI Headquarters in Washington, D.C. in 1981, he cut off contact with the Soviets and told his wife, priest, and attorney about his espionage. Federal authorities were unaware of the first period of espionage before Hanssen began to cooperate with the government after his arrest.

In 1981, Hanssen was assigned to the Budget Unit in the Intelligence Division at Headquarters, where he prepared the Bureau's Congressional Budget Justification Books, covering all FBI intelligence and counterintelligence operations. In 1983, Hanssen became a Supervisory Special Agent in the Soviet Analytical Unit in the Intelligence Division, and, in 1985, he transferred to a field supervisory position in the Soviet Counterintelligence Division in the New York City Office.

In April 1985, Aldrich Ames, a CIA intelligence officer responsible for monitoring

---

[2] CIA counterintelligence officer Aldrich Ames disclosed Top Hat's identity to the Soviets after Hanssen had done so. The Soviets executed Top Hat in 1986.

the recruitment of Soviet officials, walked into the Soviet Embassy in Washington and disclosed the identities of several officials who had offered their services to the agency, thus beginning an espionage career that would span nine years. Hanssen and Ames' treason would give Soviet intelligence services important dual sources for many critical pieces of intelligence, especially the identity of Soviet intelligence officers whom American intelligence services had co-opted.

Hanssen's second period of espionage began in October 1985 and continued after he was transferred in August 1987 to the Soviet Analytical Unit within the Intelligence Division. In 1985, nine days after Hanssen had assumed his New York City position, he wrote to a senior KGB intelligence operator to inform him that he would soon receive "a box of documents [containing] certain of the most sensitive and highly compartmented projects of the U.S. Intelligence Community." Hanssen asked for $100,000 in return for the documents (he would receive $50,000), and he warned that, "as a collection" the documents pointed to him. Hanssen had particular concerns about his safety:

> I must warn of certain risks to my security of which you may not be aware. Your service has recently suffered some setbacks. I warn that Boris Yuzhin . . . , Mr. Sergey Motorin . . . and Mr. Valeriy Martynov . . . have been recruited by our "Special Services."[3]

During the second span of espionage, Hanssen surrendered a "complete compendium of double-agent operations." An internal FBI report issued in this period noted serious compromises and disruptions in the Bureau's recruitment, recruitment-in-place, and double agent operations. The report raised the possibility that the KGB had "somehow acquired inside or advance knowledge of [Bureau] operations."

Hanssen also disclosed the Director of Central Intelligence Congressional Budget Justifications for several fiscal years, the FBI's technical penetration of a Soviet

---

[3] Apparently, Aldrich Ames gave the Soviets the same information about the three Soviet defectors around the same time as Hanssen. Two of the defectors were executed; the other was sentenced to fifteen years hard labor.

establishment, U.S. penetration of Soviet satellite transmissions, U.S. attempts to recruit Soviet intelligence officers, a limitation in NSA's ability to read Soviet communications, detailed evaluations of FBI double-agent operations, and other extraordinarily sensitive intelligence operations. For instance, Hanssen revealed that U.S. State Department diplomat, Felix Bloch, was under investigation for espionage on behalf of the Soviet Union. Bloch's Soviet handlers warned him about the investigation, and he was able to avoid prosecution.

Hanssen told his handlers in a November 1985 note that "[e]ventually, [he] would appreciate an escape plan" because "[n]othing lasts forever." He later suggested that they communicate through a "microcomputer `bulletin board,'" a suggestion the Soviets apparently did not accept.

In 1987, Hanssen started to transmit information and receive payments by establishing near his home in northern Virginia several "dead drops" or pre-arranged, hidden locations for clandestine exchanges that made it unnecessary for him to meet Soviet intelligence officers.

In 1988, Hanssen gave the Soviets the first of many computer diskettes he would use to transmit information and documents. At a minimum, the information and documents were classified Secret and contained warnings like the following from the cover sheet to a comprehensive review of Soviet penetration of the U.S. Intelligence Community, a review that Hanssen compromised:

> IN VIEW OF THE EXTREME SENSITIVITY OF THIS DOCUMENT, THE UTMOST CAUTION MUST BE EXERCISED IN ITS HANDLING. THE CONTENTS INCLUDE A COMPREHENSIVE REVIEW OF SENSITIVE SOURCE ALLEGATIONS AND INVESTIGATIONS OF PENETRATION OF THE FBI BY THE SOVIET INTELLIGENCE SERVICES, THE DISCLOSURE OF WHICH WOULD COMPROMISE HIGHLY SENSITIVE COUNTERINTELLIGENCE OPERATIONS AND METHODS. ACCESS SHOULD BE LIMITED TO A STRICT NEED-TO-KNOW BASIS.

In 1989, the KGB presented several awards to the intelligence officers involved in the

Hanssen operation, including the coveted Order of the Red Banner, the Order of the Red Star, and the Medal for Excellent Service.

Hanssen left the Soviet Analytical Unit in May 1990 when he was promoted to the Bureau's Inspection staff. Among other duties, Hanssen was charged with assisting in the review of FBI legal attaché offices in embassies across the globe. Hanssen's Soviet handlers offered their congratulations on his promotion: "We wish You all the very best in Your life and career." Having assured Hanssen that their communications mechanisms would remain in place, the Soviets advised him: "[D]o Your new job, make Your trips, take Your time." Hanssen's espionage continued after he joined the Inspection staff.

At the end of his tour on the Inspection staff in July 1991, Hanssen became a program manager in the Soviet Operations Section of the Intelligence Division at Headquarters, a unit designed to counter Soviet espionage in the United States.

In December 1991, he left extremely sensitive, classified documents at a drop site, along with a note telling his Soviet handlers that he had been promoted to a position of increased authority. Hanssen also provided information about classified technical and operational matters, and he proposed a new communications plan, by which he would communicate directly with the KGB using a computer loaded with advanced technology set up in a private office not subject to electronic surveillance. Shortly thereafter, Premier Gorbachev resigned, and the Soviet Union collapsed. Hanssen, who knew of a massive internal FBI mole hunt, decided to disengage from his espionage activity, he claims, because of feelings of guilt.

In January 1992, Hanssen became Chief of the National Security Threat List Unit in the Intelligence Division. That Unit was charged with helping to re-align U.S. counterintelligence activities in light of the dissolution of the Soviet Union.

In 1993, Hanssen attempted to reestablish contact by approaching a Russian military intelligence officer in a garage in an apartment complex near Washington, D.C. Hanssen says that he wanted to understand why Russian military intelligence continued to use

operatives he had exposed as double agents. Hanssen brought to this meeting summaries of all open Russian military intelligence, double-agent cases. He identified himself as "Ramon Garcia," the pseudonym he had used during the first period of espionage. The Russian intelligence officer apparently knew nothing about Garcia and rebuffed Hanssen's attempt to start a conversation. In a protest about the incident, the Russian government asserted that the person who had approached their officer identified himself as a disaffected FBI agent. The Bureau opened a case in response to the Russian protest, which Hanssen followed on the FBI's investigative database, the Automated Case Support system.

With the exception of the unsuccessful attempt to contact the intelligence officer, Hanssen had no contact with Russian intelligence until October 1999 when he began his third period of espionage by sending the KGB an encrypted message on a computer disk. At first, there was no response to the message, but eventually a signal was given. Hanssen went to a drop site and received instructions and $50,000 in cash.

At the time, Hanssen was "running up credit card debt," some of which he had rolled into a home mortgage during two refinancings; some of his six children were in college; and "financial pressures" were creating (in a phrase Hanssen adopted during a debriefing) an "atmosphere of desperation." Hanssen has claimed that his mortgage payments had grown so high that he "was losing money every month and the debt was growing." Consequently, he set a "financial goal" for himself: obtain $100,000 from the Russians to pay down his debt.

When the third period of espionage began, Hanssen was FBI liaison to the State Department's Office of Foreign Missions, responsible for conveying highly classified information and documents between State and FBI Headquarters, among other duties. From his office at State, Hanssen continued to have complete access to the FBI's Automated Case Support system, from which he obtained most of the information he passed to the Russians during this period.

In October 1999, after the first drop in the third period of espionage, for which

Hanssen received $50,000, his Russian handlers proposed two more drops, one in November 2000, the other in April 2001. Hanssen tried to move the first drop up to June 2000, complaining that the Russians were "wast[ing]" him: Hanssen was trying to generate income. He attempted a drop in June, but retrieved the material after the Russians failed to pick it up.

In November 2000, Hanssen once again communicated concern to the KGB about his security and raised questions about the future:

> . . . Recent changes in U.S. now attach the death penalty to my help to you as you know, so I do take some risk. On the other hand, I know far better than most what minefields are laid and the risks. Generally speaking you overestimate the FBI's capacity to interdict you.

In January 2001, Hanssen, who was then under suspicion, was transferred from the State Department to FBI Headquarters so that he could be closely monitored. Shortly thereafter, Hanssen would later claim, he came to believe that a tracking transmitter had been placed in his car. Despite these concerns, he went to another drop, where he was apprehended and arrested on February 18, 2001. Hanssen brought to the final drop an encrypted letter on a disk:

> Dear Friends:
>
> I thank you for your assistance these many years. It seems, however, that my greatest utility has come to an end, and it is time to seclude myself from active service. . . . My hope is that, if you respond to this . . . message, you will have provided some sufficient means of re-contact . . . . If not, I will be in contact next year, same time same place. Perhaps the correlation of forces and circumstances will have improved.
> Your friend,
>
> Ramon Garcia

Hanssen was indicted on twenty-one counts of espionage, conspiracy to commit espionage, and attempted espionage. Fourteen counts provided for the death penalty as the maximum punishment upon conviction. The remaining counts called for life in prison as the maximum penalty. On July 3, Hanssen pled guilty to fifteen counts. He is awaiting sentencing.

In November 2000, three months before his arrest, Hanssen gave the Russians "the largest package [of documents he] ever produced," between 500 and 1,000 sheets of photocopied material. He downloaded to disks from the FBI's Automated Case Support system a great deal of the information he divulged in this final period:

> Any clerk in the Bureau could come up with stuff on that system. It was pathetic. . . . It's criminal what's laid out. What I did is criminal, but it's criminal negligence . . . what they've done on that system.

Documents – whether downloaded or printed – were reproduced in their entirety and with sufficient information on their face to identify them as Bureau documents.

Hanssen, who was known for his technical computer proficiency, had himself developed several data "systems" for the Bureau, for example, a system for up-loading FBI internal memoranda and conducting key-word searches.[4] Before leaving material at drops for his handlers, Hanssen would scan the Bureau's systems to see whether the FBI had identified the locations as drop sites. He would also run his name in the systems to determine whether he was a subject of an investigation.

Hanssen installed unauthorized software on his office computers, an action counter to Bureau regulations. While he was serving as FBI liaison to the State Department, a password-breaking program was discovered on his hard drive. When questioned about this

---

[4] When Hanssen unsuccessfully approached a Russian intelligence officer in 1993, he brought along a description of certain double-agent cases that he created using the system he had established in an earlier assignment. At the time, Hanssen was assigned to the National Security Threat List Unit. He simply walked over to his old section and generated the information about the double agents.

at the time, Hanssen explained that he had to re-configure his FBI computer system at State to install a color printer, but that he could not do so without the password of a systems administrator, who was not often available. Consequently, Hanssen said, he broke the administrator's password and solved the problem. Hanssen was not disciplined for this conduct.

On at least one occasion, Hanssen hacked into the computer of a Bureau colleague. In 1992, he downloaded a classified document from the hard drive of the Chief of the Bureau's Soviet Intelligence Section, purportedly to demonstrate security weaknesses in the computer system.[5] Hanssen attempted unsuccessfully to interest his handlers in contemporary technology. Early on, he suggested to the Soviets that they communicate by e-mail and later he urged them to purchase a personal digital assistant so that he could "beam" messages and classified documents to them. On occasion, Hanssen's handlers were unable to break through the encryption and other security mechanisms Hanssen installed on the discs he passed to them.

Hanssen also used non-technical methods to obtain the material he compromised. Sometimes he learned information at lunches with colleagues or "in passing," and he routinely reproduced documents on FBI photocopiers and walked out of Bureau facilities with them. Hanssen also habitually walked into meetings uninvited when classified information was being discussed. After he left the National Security Division, he visited former colleagues, discussed classified matters with agents and analysts, and passed this information to his handlers. He also visited former State Department colleagues, after he had

[5] In 1997, FBI debriefers asked former agent Earl Pitts, who had pled guilty to spying for the Soviets, whether he knew of anyone else working for the Russians. Pitts explained that he did not know of other spies with certainty, but he had heard that Hanssen had hacked into an FBI computer. The Bureau did not follow up on this information because it was already known.

been transferred to FBI Headquarters. His last recorded visit came nine days before his arrest.

Hanssen had no difficulty collecting sensitive information. Before going to one dead drop, he simply "grabbed the first thing [he] could lay [his] hands on." However, he "tried to stay with things that [his handlers] would find tremendously useful, immediately useful, . . . remarkably useful." On one occasion, Hanssen took a volume from Headquarters containing Top Secret and Special Access Program information about an extraordinarily important program for use in response to a nuclear attack. Hanssen photographed the material in the back seat of his automobile and returned the volume to the Bureau.

Over the course of his espionage, Hanssen received two Rolex watches and about $600,000 in cash and diamonds from Soviet and Russian intelligence services. About $800,000 was purportedly deposited in a Moscow bank on Hanssen's behalf. The FBI also recovered $50,000 from a drop site.

Hanssen led an apparently frugal life, using some of the money he received for espionage on home improvements and private schooling for his six children. He also spent a significant sum on an exotic dancer, whose life, Hanssen claims, he was trying to reform.

Over twenty-two years and more than forty passes, Hanssen turned over to Soviet and Russian intelligence an estimated twenty-six diskettes and 6,000 pages of classified information. Although we have not been called upon to conduct a damage assessment of this betrayal, the affidavit filed in support of the criminal complaint against Hanssen does not exaggerate when it describes the information Hanssen betrayed as having "extraordinary importance and value."

While Hanssen's misdeeds are so shocking as to be in some fundamental sense inexplicable, his conduct is not as rare as citizens of a free and democratic society would hope. The Commission has received testimony that since the nineteen-thirties every U.S. agency involved with national security has been penetrated by foreign agents, with the exception of the Coast Guard. Eighty employees of the federal government and companies

with which it contracted were convicted of espionage between 1982 and 1999.[6] According to open-source material, 117 American citizens were prosecuted for espionage between 1945 and 1990 or clear evidence existed of their guilt; the reported cases of espionage doubled from the 1950s to the 1970s and then doubled again in the 1980s. Of course, this data does not include espionage that has not been detected or reported. Money appears to be the major motive in these cases; and most of these spies volunteered their services to foreign intelligence agencies.[7]

The practice of tradecraft by our adversaries, including the use of defectors-in-place, should come as no surprise. Though the ancients did not have computer diskettes, they did have the means to transmit covert information vital to "national" security. Herodotus, for instance, tells us about a Greek living in Persia, who alerted Sparta to Xerxes' invasion plans by smuggling information on a piece of wood covered with wax. The Bible is also replete with instances of espionage, including Yahweh's instruction to Moses to send spies into the land of Canaan. The account of the harlot Rahab sheltering Israelite spies and betraying the city of Jericho might be the first documented instance of a "safe house."

Thus, history teaches us to expect spies among us and to anticipate that some of those spies will be of us. Espionage has not been invented by our recent adversaries, and it is not a sign of our political or moral decline. In fact, we have been beset by spies from within even before we had a Constitution to unite us. For instance, Edward Bancroft, a New England physician who served as secretary to the commission the American colonies sent to France during the Revolutionary War, was a confidant of Benjamin Franklin, an indispensable agent of John Adams, and a British spy. Bancroft sent London weekly communications written in invisible ink and placed in a hole in a tree in the Tuileries

---

[6] DOD PERSONNEL: Inadequate Personnel Security Investigations Pose National Security Risks, U.S. General Accounting Office (Oct. 1999)

[7] S. Wood & M. Wiskoff, AMERICANS WHO SPIED AGAINST THEIR COUNTRY SINCE WORLD WAR II, Defense Personnel Security Research Center (1992)

Gardens. The rebellious colonies did not have to wait long for other disastrous betrayals, and, indeed, from our Country's early history on, the name Benedict Arnold has signified a traitor from within.

Recognizing that we cannot eliminate espionage efforts against us, the Commission has attempted to recommend changes in FBI security programs that will minimize the harm that those who betray us can do to our national security and minimize the time between their defection and detection. To achieve these goals, we focused our attention on four areas: the structure of the Bureau's security programs and the policies and procedures designed to ensure the integrity of its personnel, information systems, and documents.

We also examined security programs in federal entities other than the FBI: the CIA, NSA, the Department of State, and the Air Force's Office of Special Investigations. We looked at these entities to develop a "best-practices" model we could use to assess the Bureau's security programs, and we specifically focused on the Office of Special Investigations because, like the FBI, it has intelligence and law-enforcement functions that must be carefully delineated.

We will present our findings in the chapters to come and in much greater detail in classified appendices. In sum, we found serious deficiencies in most security programs we analyzed within the Bureau. When compared with best practices within the Intelligence Community, FBI security programs fall far short. It should be noted, however, that security programs in the CIA, NSA, the Department of State, and other elements within the U.S. Intelligence Community have undergone top-to-bottom reviews and re-structuring in the relatively recent past as a result of significant, though belatedly discovered compromises. Simply naming a few of these double agents is chilling:

- Aldrich Ames, a CIA counterintelligence officer, pled guilty to spying on behalf of the Soviet Union in what has been described as the costliest breach of security in CIA history. During nine years as a spy,

Ames revealed more than one hundred covert operations and betrayed more than thirty operatives spying for Western intelligence services.

- Ronald Pelton, a former intelligence analyst at the National Security Agency, was found guilty of having given Soviet agents an incredibly detailed account of U.S. electronic espionage capabilities, which, in the words of the sentencing judge, cost our country "inestimable damage."

- Jonathan Pollard, a military intelligence analyst, was arrested for passing to Israeli agents more than 800 classified documents and more than 1000 cables. The Secretary of Defense declared that he could not "conceive of a greater harm to national security" than Pollard's betrayal.

- John Walker, a retired naval officer, operated a spy ring that included his son and brother. Using cryptomaterial Walker supplied, Soviet agents were able to receive and decode over one million communications, leading, in the assessment of the Secretary of Defense, to "dramatic Soviet gains in all areas of naval warfare."

Thus, although our report is highly critical of fundamental practices and policies governing sensitive information within the Bureau, it would be a mistake to single out that entity for criticism. The FBI has not been alone in finding itself betrayed by trusted employees willing to imperil their country for money or some other venal or twisted political consideration. Furthermore, at least some of the critical deficiencies we found in Bureau policies have been replicated in other federal agencies. For instance, we observed critical deficiencies in the process by which the Bureau conducts background checks for security clearances, a finding sadly mirrored in a 1999 GAO study concluding that ninety-two percent of Department of Defense security investigations in the period studied were deficient.[8]

[8] See note 6. More recently, the GAO criticized the Department of Energy's access controls and "need-to-know" policies in the wake of allegations that China had surreptitiously obtained U.S. nuclear warhead designs. NUCLEAR SECURITY: DOE Needs To Improve Control Over Classified Information, U.S. General Accounting Office (Aug. 2001). We will present disturbingly similar criticisms of FBI policies. Several damage assessments conducted in

Furthermore, in spite of Hanssen's purported proficiency with electronic storage systems, the methods he used to betray his country have been practiced by others with little technical knowledge. For instance, over seven years ago, the CIA Inspector General concluded that Aldrich Ames' access to computer "terminals that had floppy disk capabilities represented a serious system vulnerability":

> No specific precautions were taken by Agency officials to minimize Ames' computer access to information within the scope of his official duties. In fact, there is one instance where Ames was granted expanded computer access despite expressions of concern . . . by management . . . about his trustworthiness. Ames . . . was surprised when he signed on [the computer] and found that he had access to information about double agent cases. This allowed him to compromise a significant amount of sensitive data . . . to which he did not have an established need-to-know.[9]

National security would have been better served if deficiencies found in one agency had led other agencies to review their own practices. Unfortunately, security reform usually occurs in an agency only after it has been severely compromised. For instance, after allegations surfaced that China had obtained nuclear warhead designs from an employee of the Los Alamos National Laboratory, the Department of Energy's programs for protecting classified information were thoroughly reviewed and found severely wanting. Again, these findings are sadly similar to the deficiencies we found in the FBI's security programs. Had the Bureau taken advantage of the review of DOE procedures, had DOE taken advantage of reforms at the Central Intelligence Agency in light of Ames' defection, had the CIA taken advantage of reforms at the Department of State after a security compromise there, the entire Intelligence Community would have benefitted.

---

the wake of recent foreign espionage penetrations also recommend changes in security programs that parallel changes we suggest in our report.

[9] Abstract Of Report Of Investigation, The Aldrich H. Ames Case: An Assessment of CIA's Role In Identifying Ames As An Intelligence Penetration Of The Agency, Findings 59 & 61 (Oct. 21, 1994).

The Intelligence Community as a whole has failed to learn from history, a failure that is mirrored in the fragmented security policy governing members of that community. Each agency is responsible for implementing its own security system in compliance with government-wide mandates. The Bureau's security policies, for instance, are an amalgam of its own traditional practices and a sometimes imperfect reflection of a slough of Executive Orders, National Security Directives, Presidential Decision Directives, Director of Central Intelligence Directives, Congressional enactments, and other mandates.

We are not the first to note the lack of a system to ensure that security policy is implemented properly in the Intelligence Community and that members of that community learn from their brethren's mistakes. In 1994, a Joint Security Commission declared that:

> . . . [F]undamental weaknesses in the security structure and culture . . . must be fixed. Security policy formulation is fragmented. Multiple groups with differing interests and authorities work independently of one another and with insufficient horizontal integration. Efforts are duplicated and coordination is arduous and slow. Each department or agency produces its own implementation rules that can introduce subtle changes or additions to the overall policy. There is no effective mechanism to ensure commonality.[10]

Consequently, in a report to the Secretary of Defense and the Director of Central Intelligence, the Joint Commission recommended that a security executive committee be established to "unify security policy development; serve as a mechanism for coordination, dispute resolution, evaluation, and oversight; and provide a focal point for Congressional and public inquiries regarding security policy. . . ." Almost a decade earlier, the Senate Select Committee on Intelligence asserted that "more needs to be done to ensure that agencies learn from each other's experiences and that progress achieved in one area can have benefits for

[10] Redefining Security 2 (Feb. 1994).

others." In calling for the establishment of a comprehensive National Security Program, the Committee warned:

> If there is no national policy, . . . there is no standard against which to hold each department accountable. If national policies are fragmented, outdated or unbalanced, security becomes subordinated to other departmental priorities and interagency disputes. This has occurred far too often in recent years.[11]

And it has continued to occur in the sixteen years since the Select Committee issued its report. Consequently, in addition to the particular recommendations about Bureau policies that we make in our report, we offer a more global recommendation: a system should be established whereby security lapses in a particular entity lead to improved security measures throughout the entire Intelligence Community. Determining how this system should be structured is outside our mandate, but the need for it is obvious.

Our report contains many recommendations for changes in the FBI's policies and practices. We are pleased to see that the Bureau has already begun to examine its security programs and has independently implemented some of our recommendations. Critics often assert that the problems we have examined, as well as other well publicized missteps the Bureau has taken in recent years, are the product of a culture ingrained within the FBI that will make meaningful reform impossible. We found many instances of Bureau employees affording respect to deficient practices simply because they are Bureau practices and other instances when state-of-the-art practices in other agencies were rejected simply because they were not Bureau practices. However, the vast majority of FBI employees with whom we spoke have been shaken by Hanssen's treason; they are acutely aware of the damage he has done to the country and to the reputation of the institution they love; and they seem to understand the necessity of reforming inadequate practices. The reaction of other agencies recently betrayed from within shows that organizations that instill esprit in their members

---

[11] Meeting The Espionage Challenge: A Review of U.S. Counterintelligence And Security Programs, Report of the Select Committee on Intelligence, U.S. Senate 39 & 61 (Oct. 3, 1986).

can change when chastened to the core, and we have observed first-hand the degree to which Hanssen's crimes have shaken the Bureau as a whole, particularly those employees who are part of the Intelligence Community.

There is another "cultural" dimension to the security deficiencies we observed in the Bureau. Until the terrorist attacks in September 2001, the FBI focused on detecting and prosecuting traditional crime. That focus created a culture that emphasized the priorities and morale of criminal components within the Bureau, which offered the surest paths for career advancement. This culture extolled cooperation and the free flow of information inside the Bureau, a work ethic wholly at odds with the compartmentation characteristic of intelligence investigations involving highly sensitive, classified information.

In a criminal investigation, rules restricting information are perceived as cumbersome, inefficient, and a bar to success. However, when a criminal investigation is compromised, usually only a discrete prosecution with a limited set of victims is at risk. In sharp contrast, when an intelligence program is compromised, as Hanssen's case demonstrates, our country's ability to defend itself against hostile forces can be put at risk.

A law-enforcement culture grounded in shared information is radically different from an intelligence culture grounded in secrecy. Whether the two can co-exist in one organization is a difficult question, but they will never do so in the FBI, unless the Bureau gives its intelligence programs the same resources and respect it gives criminal investigations, which, employing its own sensitive information and confidential sources, would also benefit from improved security.

Implementation of the changes necessary to secure vital information within the Bureau's universe will require continuous dedication, not momentary attention, so that neither bureaucratic inertia nor tight focus on the latest national crisis the FBI faces will permanently divert resources from structural defects that must be cured. Consequently, we also recommend that, within six months, the Bureau submit to Congressional intelligence oversight committees, through the Attorney General, a plan addressing the weaknesses we

have discovered in FBI security programs and our recommendations. We also urge that the Bureau submit to the committees annual reports for the next three years on its efforts to implement that plan. We note that the Central Intelligence Agency, in the wake of Ames' defection, issued such reports, apparently to great effect.

The Commission wishes to thank the members of its staff, whose effort is reflected in this report. Our country will make a serious error if it does not capitalize on this effort. Neglect of the systems undergirding national security can lead to consequences so severe and so horrific that, in our view, the political structure is duty bound to respond.

RECOMMENDATIONS

The following is a compressed compilation of the recommendations in our Report. Because the recommendations addressing security weaknesses in the Bureau's information systems are often arcane, we placed them in the technical appendices and have limited the INFOSEC portions of this summary to broad policy recommendations.

GENERAL

I. A System Should Be Established So That Significant Security Lapses In An Entity Within The Intelligence Community Lead To Improved Security Measures Across The Community

II. The Bureau Should Within Six Months Submit To Congressional Intelligence Oversight Committees, Through The Attorney General, A Plan Addressing Weaknesses In Its Security Programs, And It Should Submit Annual Reports On Its Efforts To Implement That Plan

INFORMATION SECURITY

I. Comprehensive, Consistent, And Centrally Coordinated INFOSEC Policies Should Be Adopted

The FBI does not have a well-defined, comprehensive INFOSEC policy or clearly written guidance explaining how current policy is to be implemented. Responsibility for curing this problem should be vested in a new Office of Security. Having established an INFOSEC policy, the Bureau must also create security guidelines and system specific plans.

II. INFOSEC Education And Training Must Be Implemented

The FBI lacks adequate INFOSEC education and training programs. Classified information stored on some of the Bureau's most widely utilized systems is not sufficiently protected because users lack training on critical security features. Implementation of a

general INFOSEC education and training program may take some time, but the Bureau must immediately train users on the security features of the Automated Case Support system because this system poses a tremendous risk to national security information.

III. Key INFOSEC Positions Must Be Filled And Supported

Many key INFOSEC positions have not been filled, and some have been filled by persons lacking essential experience and training. Persons assigned to these positions must be given the time, authority, and support necessary to perform their duties.

IV. The FBI Must Institutionalize A Formal, Tailored Process To Certify And Accredit Computer Systems

The FBI must define a certification and accreditation process that comports with governing directives and is tailored to meet Bureau needs. This process must consider the security implications of interfaces among connected systems and between systems and other components, such as workstations. Persons tasked to certify FBI systems should have the requisite expertise; they should not review their own work product or report to system builders and operators.

V. The FBI Should Develop A Comprehensive, Prioritized Plan To Address Security Shortcomings

The Bureau must define the security environment it wants to create to protect information by identifying relevant policies, specific threats, and secure usage assumptions. The Bureau must determine threats that existing security countermeasures do not counter and information protection policies that are not being enforced, and it must select programs, tools, and technologies to sustain its security environment.

I. Security Investigations And Adjudications Should Be Consolidated In A New Office Of Security

The process by which the FBI currently conducts background investigations, adjudicates cases, and grants security clearances is fragmented, resulting in duplicative efforts, wasted resources, and unaddressed security issues.

I. The Personnel Security Process Should Be Automated

The Bureau's system for processing and tracking investigations, reinvestigations, adjudications, and clearances is paper-driven and inadequate. The FBI should create a system to track personnel so that they are identified for reinvestigations and their clearances are up-to-date.

II. BICS Investigations Should Be Thorough

The Background Investigation Contract Service (BICS) should ensure that its Special Investigators (SIs) are skilled and conduct thorough investigations. BICS should avoid a checklist approach to investigations. SI reports should be detailed, highlighting and explaining potential security problems. The SI reporting process should be automated. Responsibility for Personal Security Interviews should be removed from field offices and given to BICS SIs.

III. Adjudicator Training Should Be Improved

The Bureau should give adjudicators extensive training to ensure that they comply with Director of Central Intelligence Directives and internal mandates. Adjudicators should be trained to recognize incomplete background investigations, and they should request additional coverage when necessary.

I. Stricter Controls Should Be Placed On Interim Clearances

The interim clearance process for contract employees lacks adequate controls, resulting in interim clearances granted without full-scope investigations, a practice that can lead to high-risk personnel cleared with insufficient vetting. The Bureau should implement tighter controls on personnel granted interim clearance, limiting facility access and minimizing contact with FBI employees and assets.

VI. The FBI Should Adopt A Financial Disclosure Program And Develop A Technical Structure To Support Financial Monitoring

The FBI should comply with Executive Order 12968 by requiring employees and contractors to complete financial disclosure forms. The Bureau should also develop a personnel and technical infrastructure to support financial monitoring. Information from financial disclosure forms and an automated analysis should be available in employee reinvestigations and security investigations.

VII. The FBI Should Implement A Counterintelligence Polygraph Program And Create An Infrastructure To Support The Program

The FBI should adopt a counterintelligence polygraph examination, focused on espionage and restricted to reinvestigations of personnel with access to Sensitive Compartmented Information and special programs. The Bureau should develop a quality control program and educate personnel about the polygraph's security function and the limited nature of the counterintelligence examination.

DOCUMENT SECURITY

I. Classified National Security Documents Should Be Handled And Stored In SCIFs And Secure Areas And Available Only To Those With A Need To Know

The Bureau should train its personnel to recognize that compartmentation and need-to-know principles apply even in Secure Areas and SCIFs.

II. The Security Access Control Badge System And The FBI Police Program Should Be Strengthened

Employees should be required to "badge into" SACS areas on hardware that requires a PIN number and records the passage of every badge, including all car-pool passengers. Gold badges and executive-escorted-visitor badges should be eliminated. FBI police should match the photograph on every SACS badge entering Headquarters with the bearer of the badge and conduct aperiodic checks of vehicles and persons leaving Headquarters to emphasize the gravity of document security. The police force should be brought to full strength and given an enhanced security role.

III. The Bureau Should Enhance Protections On The Handling, Copying, And Disposing Of Classified Material

The FBI should bring its written policy statements on these matters into compliance with Director of Central Intelligence Directives and Executive Orders. The revised policy should eliminate confusion about "working documents" and copies of classified documents obtained through electronic systems. Headquarters employees should receive detailed guidance about moving classified information around the building and should be prohibited from leaving classified material unattended, except in approved Secure Areas or Sensitive Compartmented Information Facilities (SCIFs). After-hours protocols for securing computers and classified material should be established. Bureau photocopiers, particularly

in SCIFs and Secure Areas, should not be operable without PIN numbers. Photocopying classified material should be held to a minimum, and copies should be subject to the same controls as originals. A time limit for maintaining copies of classified documents should be established. Security risks in the destruction of Secret waste off-site should be eliminated.

IV. Written Guidance On Top Secret And Sensitive Compartmented Information Should Be Current, Clear, And In Compliance With Director Of Central Intelligence Directives And Executive Orders

FBI manuals and policy statements should incorporate changes made over time by Bureau Electronic Communications and should comply with Director of Central Intelligence Directives, especially in describing SCIF operations. Written policies should provide clear and specific guidance to Security Officers, who are sometimes unaware of policy because they do not know how to locate it.

V. The Operations Of The Special File Room Should Be Improved By Eliminating Unnecessary Classified Material And Enhancing Staffing, Training, And Equipment

The Bureau should destroy all documents within the Special File Room (SFR) eligible for destruction. Profiles should be adopted to control the amount of information intelligence agencies send the Bureau. SFR employees should receive improved, recurring formal training, in addition to on-the-job mentoring, and Headquarters personnel should be trained to take advantage of SFR document indexing services.

VI. SCIF Operations Must Be Improved By Promulgating Clear, Enforceable Rules And Providing Training For SCIF Tenants

The operation of Bureau SCIFs across the country is inconsistent and sometimes improper. SCIF operations should be controlled by clearly written guidelines, as Director

of Central Intelligence Directives require, and training for SCIF personnel should be improved. SCIF accreditation, daily operations, and periodic reviews require much greater resources than are currently allotted.

VII. The FBI Should Consider Adopting The Human Intelligence Control System

The Bureau should consider adopting the Human Intelligence Control System, a system of compartmenting human source information developed by the CIA. If it does adopt this approach, it should publish clear, written policies effecting those controls, and it should train personnel who will use them.

I. The FISA Process Should Be Simplified, And Access To FISA Information In ACS Should Be Restricted

The process implementing the Foreign Intelligence Surveillance Act (FISA) should be streamlined to reduce the number of persons involved and the complexity of the process. The Bureau should implement a system of electronic links with the Department of Justice to enhance the security of the FISA process and allow simultaneous review. Responsibility for FISA packages should be centralized in an FBI FISA Unit. The training of field security officers who monitor FISA carrier security should be improved, and trust receipts should be used whenever possible. Personnel handling FISA on the Automated Case Support system should be trained in the use of access restrictions. The ability to print and download FISA information on ACS should be restricted.

I. A Central Security Authority Must Coordinate And Oversee All Document And Physical Security Violations And Compliance Activity

A central security authority with the ability to profile and identify individuals and components engaging in patterns of security violations will make it easier for the Bureau to

detect habitual violators. Currently, several components play uncoordinated roles in detecting, investigating, and assessing security violations; no single entity has authority to coordinate, track, and oversee security violations and enforce compliance. A central authority responsible for coordinating security issues among all FBI entities, with the authority to rescind security clearances, will create a powerful incentive for employees to comply with good security practices. A database should be developed so that patterns of security violations by individuals or components can be detected.

I. FBI Policy Manuals Should Require Security Coordination

To bolster this central security authority, manuals addressing physical security violations should be updated and reconciled. The manuals should require that suspected, possible, and actual losses and compromises of classified information be reported to appropriate components. The manuals should explain categories of security violations and levels of punishment and specify how the Bureau components that respond to possible security violations should coordinate their efforts.

SECURITY STRUCTURE

I. FBI Security Programs Should Be Integrated In An Office Of Security That Reports To The Director

The Bureau's security programs are weak and fragmented. The Bureau should restructure an integrated security program within an independent Office of Security, reporting to the Director. All security functions should be consolidated within that Office, including security policy making. Security policies should be reviewed and implemented through a senior executive security policy board, chaired by the head of the Office, that includes DOJ's Security Officer.

II. The Office of Security Should Develop A Professional Security Staff Through Enhanced Selection, Retention, And Training Programs

The FBI does not have a professional security staff or a career-enhancing training program for security specialists. In addition to developing and training a security staff, the Bureau should introduce professional career tracks for security professionals and for information technology security specialists.

III. The Office Of Security Should Implement Comprehensive Employee Security Education And Awareness Programs

The Office should maintain a full-time professional training staff to develop and implement security education and awareness programs for all employees. The staff should disseminate information on security responsibilities and create user-friendly computer sites for security information. Security should be an integral part of the curriculum at the FBI Academy. The Office of Security and the Information Resources Division should jointly develop training programs in information-system security. Mandatory executive management training programs should be conducted. Compliance with security policies and programs should be a component of annual performance appraisals of all managers and Security Officers.

IV. The Office Of Security Should Develop A Centralized Security Violation Reporting Program

The FBI's review of security violations is fragmented and inadequate. The Bureau should develop a reporting program, which describes security violations and establishes clear procedures for investigating security violations. The program should be accompanied by recurring notice to employees and recurring security education. The program should require

written documentation of security violations and mandatory reporting of all violations to the Office of Security, where they should be tracked on a secure centralized database. Automated analytical functions for collected data should be installed.

V. The Office Of Security Should Audit Security Programs.

The FBI does not adequately review its fragmented security programs. The Office of Security should periodically review and audit all security programs and systems. Office personnel should be detailed to the Inspection Division as needed to ensure meaningful audits of security programs.

INFORMATION SYSTEMS SECURITY

(INFOSEC)

Well, if they had been [monitoring computer use], I probably wouldn't have been making the kind of queries that I was making. ..... So, it would have affected the way I used the machine. It may have prevented the disclosure of things.

– Robert Hanssen

INFORMATION SYSTEMS SECURITY
(INFOSEC)

Robert Hanssen's espionage demonstrated in a public and convincing way that the Bureau's information systems security controls are inadequate. Information under the Bureau's control is exceedingly important to national security and must be protected. The FBI must also exchange information with intelligence agencies, and intelligence sources, both current assets and prospective recruits, will play increasingly prominent roles in the Bureau's mission. Consequently, the FBI must take immediate steps to restore confidence in its ability to protect its sources and the information they disclose.

Our analysis of FBI information system security (INFOSEC) policy and practice is three-fold. This unclassified section of the Report will illustrate some of the analytic themes and recurring weaknesses discovered in our review of Bureau information systems. Appendix A, classified, expands on those themes by explaining the methodology we employed and our more interesting findings and conclusions. The remaining INFOSEC appendices are for the technical reader and provide, we hope, an expert analysis that can help the Bureau translate policy and allocation choices into improved information systems security.[12]

Our analysis is premised on a component of "best practices" in the Intelligence Community, the "Defense-in-Depth" concept, a set of principles that, instead of using all available resources to build, for example, a thirty-foot perimeter wall to protect a building, would erect a ten-foot fence, install locks on doors and windows, and purchase a safe for the most valuable assets. This layered approach mitigates the vulnerabilities in any one security feature by establishing a number of defensive layers that must be breached. By increasing the risk of detection, these layers of security act as a deterrent to espionage. Whether the

[12] Appendix B is the Technical Report, which describes our findings, the systems reviewed, the information sought, and technologies the FBI might employ to detect insider threats. Appendices C through I contain detailed findings for each system selected for in-depth review.

compromised insider is deterred by the risk of detection or actually thwarted by a security layer, the Defense-in-Depth approach restricts a compromised insider's unauthorized access to data.

In the course of our review, we identified a wide range of problems affecting the FBI's computer systems and INFOSEC programs, which we will briefly summarize, saving a detailed discussion for the appendices.

- The Bureau has failed to develop an effective strategy to identify and protect critical information. The FBI has not defined its security environment and therefore lacks the analytical framework necessary to address insider threats.

- Classified information has been moved into systems not properly accredited for its protection.

- Until recently, the Bureau had not begun to certify and accredit most of its computer systems, including many classified systems. The current approach to certification is inadequate.

- Inadequate physical protections place electronically stored information at risk of compromise.

- The FBI lacks adequate, documented INFOSEC policies.

- The Bureau's approach to system design has been deficient. It has failed to ascertain the security requirements of the "owners" of information on its systems and identify the threats and vulnerabilities that must be countered.

- Classified information stored on some of the FBI's most widely utilized systems is not adequately protected because computer users lack sufficient guidance about critical security features.

- The FBI has failed to limit user access to systems and databases that employees need to perform their jobs.

- Many key INFOSEC positions remain unfilled, and, when they have

been filled, the persons assigned often lack the time, authority, and support necessary to perform their duties.

- Some FBI systems have insufficient resources to perform required audits. When audits are performed, audit logs are reviewed sporadically, if at all.

As varied as the FBI's computer security problems may be, they all flow from a pervasive inattention to security, which has been at best a low priority in recent years. At the Bureau, security is often viewed as an impediment to operations, and security roles and responsibilities are viewed as counterproductive to career advancement. Management often does not support INFOSEC programs, which receive insufficient resources. As FBI computer systems were modified over the years to adapt to evolving operational demands, program priorities and resource allocations clearly favored operational over security needs. FBI personnel tasked with computer security were expected to gauge the security implications of these changes and modify security programs to accommodate them with few resources and minimal guidance.

This is not to fault Bureau personnel charged with building, modifying, and securing information systems. They are following well worn paths at the FBI, and much of what has been accomplished with insufficient time and resources is commendable. FBI management faces the same resource allocation issues that all large organizations face, and allocations have often been driven by external pressures and crises. Items perceived as having low priority, such as computer security, receive little attention.

This portion of our Report will concentrate on the FBI's Automated Case Support system, which Hanssen exploited almost exclusively in his last period of espionage, and on Trilogy, an ambitious, but limited plan to upgrade certain Bureau computer networks and information systems. This discussion is intended as an illustration of the broader findings we make in the appendices about the Bureau's information systems. The discussion will also illustrate the vulnerability of extraordinarily sensitive information within the FBI, the

Bureau's failure to instill security consciousness in its personnel, and the tension between operational needs and security imperatives.

THE AUTOMATED CASE SUPPORT SYSTEM (ACS)

Deployed in 1995, ACS is one of several applications residing on the Bureau's investigative mainframe and is intended to contain information ranging from unclassified to Secret. ACS is the FBI's investigative system of records and is comprised of three sub-systems: a case indexing system; a case management system; and a system to store and retrieve text documents. Information related to all FBI investigations and cases, including criminal and intelligence cases, is stored on ACS. The system allows FBI personnel to open and assign cases, set and assign leads, store text of documents (for example, investigative reports and memoranda of interview), and index, search, and retrieve these documents. ACS also contains a considerable store of administrative data, such as personnel and Office of Professional Responsibility files.

Several, nearly universal complaints about ACS relate to the general unfriendliness of the system and the perceived absence of security. Many FBI agents avoid ACS, often by delegating ACS functions to support staff. Many agents distrust ACS, and, in defiance of Bureau policy, refuse to upload into the system the most sensitive information in their possession.

Hanssen's Use Of ACS

Bureau personnel have reviewed audit logs recording Hanssen's activity on FBI computer systems and have identified thousands of files that he accessed and downloaded or displayed long enough to view or print. Almost all of these files resided on ACS. It remains unclear how many files Hanssen actually exploited by providing them or the information they contain to his contacts.

Hanssen was able to mine ACS data quite effectively. An FBI employee associated

with the preliminary damage assessment noted that Hanssen compromised over fifty FBI human sources and potential recruits and many technical sources. As a result of Hanssen's exploitation of ACS, several sources were executed or imprisoned. The Bureau also pulled other sources out of the field and terminated a number of technical programs and projects. FBI sources apparently fear that information Hanssen passed will lead to their discovery, and their handlers can do little to assuage these fears. The handlers are concerned that their credibility could never withstand another blow like the one Hanssen dealt. In addition to human and technical sources, Hanssen compromised critical information housed on ACS about U.S. intelligence capabilities. Through ACS, Hanssen also developed a particularly clever scheme to ensure that information he sent by mail to his Russian contacts was not intercepted.

Hanssen's interest was often piqued by descriptions in ACS of documents to which user access had been restricted. FBI employees uploading restricted documents to ACS often complete an unrestricted descriptive data field called "Attributes." Hanssen found the synopses in the Attribute fields for restricted documents "very revealing."

Hanssen's computer expertise also helped him exploit ACS. He mastered ACS search engines, finding ways to navigate around security restrictions. For instance, ACS administrators have created a list of "stop words," terms that are not indexed in the ACS search engine. If a user attempts to conduct a search using a stop word, for example, "Secret," the search engine will not find the term, even though it may appear in the text of many documents. To get around these restrictions, Hanssen drew on his extensive knowledge of National Security Division programs, practices, and personnel to frame queries. A Supervisory Special Agent explained that the entire Washington Field Office technical program was open to Hanssen because he was sophisticated enough to search particular files related to the program.

Hanssen employed only his ordinary ACS rights to access information. As a Headquarters Supervisory Special Agent, he had access to cases normally restricted to

personnel in the field offices in which they originated. It does not appear that Hanssen possessed system administrator access or that he hacked into any files. Hanssen successfully searched for unrestricted confidential information in ACS administrative cases, information to which access was probably restricted when placed in substantive case files. The FBI has determined that, of the many documents Hanssen accessed on ACS, about 500 should have been more restricted than they were, a failure that could have stemmed from ignorance of the restriction capabilities or misunderstanding of how they work. However, while some ACS information was accessible to Hanssen because it had not been properly restricted, much of it was generally available.

As a result of this failure to restrict cases appropriately, Hanssen was able to access an ACS counterespionage case file on an investigation of a potential spy within the U.S. Intelligence Community. Based on information in the file, Hanssen pieced together the identity of the target of the investigation. He also deduced that the Bureau had closed the case when he learned through ACS that the FBI had removed surveillance devices from the target's home. Observing that no new documents had been added to the ACS file, Hanssen confirmed that the investigation had been closed, alerting him that the Bureau might turn its attention elsewhere – and potentially to him.

Hanssen also attempted to use ACS to ascertain whether the Bureau was investigating him or his espionage. He searched for documents containing his name spelled several different ways, his home address, names of agents in FBI espionage squads, code names of espionage investigations, Russian/Soviet counterintelligence restricted cases, and terms such as "espionage." He also searched for documents pertaining to "dead drops" and for administrative files to determine if resources had been allocated to surveil the locations he used as drops. Any one of these searches might have alerted an auditor that Hanssen had at the least unusual interests, some beyond his need to know; and many of these queries (or combinations thereof) should have alerted an auditor that Hanssen was curious whether the

FBI was investigating him.[13] While it does not appear that Hanssen learned of the investigation mounted against him, these searches did not alert the Bureau to his misconduct because computer audit logs generally go unreviewed.

Access Restrictions On ACS Case Files

In the appendices, we review sophisticated INFOSEC countermeasures associated with ACS, such as identification and authentication, session controls, and audit capabilities. However, the most important security device from the perspective of the average user is the ability to restrict access to ACS case files.

Most, if not all members of the Bureau community have access to ACS, the FBI's investigative system of records, into which all case-related documents are supposed to be uploaded. However, not everyone with ACS access has access to every file in the system. While all Bureau employees have Top Secret clearances, no employee needs to know about every investigation. The need-to-know principle is often overlooked at the FBI, but it remains prominent in highly sensitive investigations, such as those involving human sources and counterespionage efforts like the one that snared Hanssen. Many Bureau personnel working on such cases believe that there is no reason to share all classified information with every ACS user in the FBI's global community. To address this reasonable concern, ACS was designed with a capability to restrict access to case files.

Access may be restricted when files are initially opened. There are two general types of access restrictions. A case may be restricted to a list of persons with roles in the case.

---

[13] Under Executive Order 12968, access of cleared individuals to classified information should be restricted to information needed "to perform or assist in a lawful and authorized governmental function." This restriction is frequently referred to as the "need-to-know" principle.

Hanssen also conducted searches targeting public figures, including the Clinton First Family. On over twenty occasions, he ran searches containing the names "Hillary Rodham Clinton," "Hillary," "Chelsea," or "Clinton." He ran at least one search on Director Freeh. Had the FBI been aware of these searches, it seems likely that auditors would have found this activity peculiar and it would have received close scrutiny.

This is referred to as a "P" restriction. A case may also be restricted to personnel in the field office where the case originated. This restriction to the office of origin is referred to as an "O" restriction.

ACS system defaults are set to designate a newly opened case as O, P, or unrestricted based on the case classification number. For instance, Office of Professional Responsibility cases are automatically opened as O cases and thus restricted to the office of origin. Asset cases, that is, cases involving human sources of intelligence, are automatically opened as P cases and thus restricted to persons with roles in the case. Until recently, Special Agents could request that a case unrestricted under its case classification be opened as an O or P case. The support person opening the case would override the default associated with that classification and restrict the case as instructed by the case agent.

If a case is O or P restricted (by default or designation), FBI employees lacking access rights who pull the case up in an ACS search will not be able to read certain information. With some case classifications, for instance, cases relating to foreign counterintelligence assets, the employee lacking access will not even know that a case exists. Instead, a "silent hit" will be generated to advise the case agent overseeing the case that an employee lacking access rights attempted to search for or view the case. When used properly, O and P restrictions appear to bar unauthorized access effectively. In fact, the Bureau has encountered difficulties when a P file is needed, but no employee with access to the case is available.

Unfortunately, the FBI has failed to train ACS users on case-file restrictions adequately. Headquarters has not implemented a comprehensive, centralized training program, and field offices have been left to piece ACS training together. As a result, users often fail to restrict investigative case files properly. As we have seen, Hanssen took advantage of this security failure to access approximately five hundred case files that had not been appropriately restricted.

Headquarters does offer some ACS training, although mostly for information

management assistants. It is unclear how widely this offering is advertised or taken advantage of. Field personnel aware of the course offerings have noted that resource limitations make it difficult to take advantage of the training. Therefore, some field offices have independently taken initiatives to increase the ACS proficiency of their users. The Washington Field Office, for instance, offers its ACS users a few hours of training to complement what they learn on the job. The training has an operational, not an INFOSEC focus.[14]

As a result of inadequate training, many users do not completely understand case file restrictions. Many, particularly at Headquarters, are unaware that the restriction capability even exists. An information management specialist at the FBI's Engineering Research Facility estimated that fifty percent of the agents she supports, many of whom have transferred from Headquarters, were unaware of this capability until she informed them. Once informed, the agents instructed her to restrict by designation approximately half their cases. Even ACS trainers, the persons most knowledgeable about ACS, have disparate views about how the restrictions operate. There is clearly a great deal of confusion about this security capability, which has likely resulted in its misapplication or at least inconsistent application.

One consequence of this confusion is that the FBI population generally has little confidence in ACS as a secure system for storing classified information. The ineffective application of ACS file restrictions has resulted in a number of horror stories about exposure of confidential files on ACS and has fueled a general apprehension about the system's INFOSEC weaknesses.

Even before the revelations concerning Hanssen's combing ACS for marketable data,

---

[14] Agents and support staff in the Indianapolis Field Office (IFO) are reputed to be among the most proficient ACS users in the Bureau, perhaps because the office trains all ACS users. While the focus of the training is operational, there is some INFOSEC guidance. However, personnel overseeing the training note that the program is not coordinated with Headquarters and may simply reflect IFO's interpretations of FBI policy.

some FBI personnel routinely chose not to upload certain information into ACS. For instance, it is common knowledge within the Bureau that the New York Field Office (NYFO) generally refuses to upload certain types of national-security information. NYFO intelligence agents have confirmed that this is the case. In 1995, NYFO personnel were asked to assess ACS as a pilot system before it was deployed, and they developed significant concerns about security. An intern from the Massachusetts Institute of Technology was given ordinary user access and challenged to discover system vulnerabilities. In an afternoon, the intern accessed a number of restricted files.

NYFO intelligence agents have also long worried that, if they were to upload all case-related information, as required, not only would restricted files be at risk of compromise, but information contained in unrestricted files viewed in the aggregate might create complete pictures that should not be disseminated throughout the Bureau. These agents also believe that it is possible to ascertain user passwords by employing ACS system tools.

Skepticism about ACS security is not limited to NYFO. At the Engineering Research Facility, a program manager operating a Top Secret/SCI program noted that his unit does not upload into ACS even sanitized versions of the unit's reports. Instead, the unit uploads only verification that a report exists and requires that prospective readers request the report in hard copy. Personnel in the Washington and Indianapolis field offices also expressed concerns about uploading classified information into ACS, particularly asset information, and often they do not upload that information.

Several ACS users described a common situation that could result in the inadvertent exposure of files intended to be restricted. Documents uploaded to ACS may be attached to multiple case files. Frequently, a document is sent to a substantive case file, which may be restricted, and to an administrative file, which often is not. Thus, the uploaded document is restricted when serialized in the substantive case file, but not when serialized in the unrestricted administrative file. For example, NYFO intelligence agents pointed out that classified information from the Washington Field Office's annual asset reports can be found

in unrestricted administrative case files. These reports provide considerable detail about foreign intelligence assets, including their identities and activities.

The FBI's counterespionage efforts have been undermined by this lack of confidence. According to a Unit Chief, personnel charged with investigating espionage allegations generally do not upload case file information into ACS. The Chief also noted that they do not even solicit help with leads on ACS because on one occasion, when a lead was sent to a field office, new agents who covered the lead – unaware of the unit's avoidance of ACS – uploaded information without restricting it. By complying with the FBI directive to upload, but apparently unaware of how ACS file restrictions operate, these agents compromised classified information. Other members of counterespionage units noted that databases have been created, separate from the FBI's established systems, to collect, analyze, and protect data. These databases, which may exist throughout the FBI, operate outside the supervision of the Bureau's security apparatus.

Hanssen's espionage has increased suspicion of ACS among Bureau personnel. Many persons interviewed suggested that the little confidence they had in ACS as a secure system of records evaporated after Hanssen. NYFO personnel feel vindicated for resisting Bureau policy that information be uploaded into ACS, and personnel in the Washington and Indianapolis Field Offices are frustrated for having sometimes uploaded information. Russian intelligence units in the Washington Field Office were apparently hard hit by Hanssen's misconduct. Many of their sources were compromised. By contrast, only two human assets operated out of NYFO were put in jeopardy. These sources were imperiled because information concerning them was extracted from NYFO hard copy documents sent to other field offices as leads and uploaded into ACS. It is not unusual for NYFO information to appear in ACS in this manner.

It is difficult to gauge whether confidence in ACS can be restored. Some persons interviewed have suggested that confidence is shattered beyond repair and that the FBI will need to deploy a new, or at least renamed, more user-friendly system. Many interviewees

asserted that the Criminal Investigation Division and the National Security Division should be given separate investigative systems to support their missions and security needs. Whatever approach the FBI takes, it must solicit input from user communities, particularly those who have resisted uploading information into ACS, to determine what is needed to restore confidence. If the user communities are willing to work with ACS and its case restrictions, the FBI must commit to defining clearly which cases should be restricted and at what level. The Bureau must also educate its users regarding the policy and procedures for restricting cases, and this policy must be enforced. Users should expect to be questioned when they access files as to which they have no apparent need to know.

Shaken confidence in ACS and skepticism about the security of information housed in it undermine the mandate that all case-related information be uploaded into ACS. As the FBI's investigative system of records, ACS is intended to store the Bureau's institutional knowledge. If case files, or even entire cases, are purposely not uploaded, the FBI's institutional knowledge is less complete and investigations may suffer because potentially helpful information is available only to the few who are aware of it.

In short, ACS's integrity as a repository for the FBI's investigative case files has been compromised. The hard and bitter fact also remains that Hanssen was able to exploit the Bureau's investigative system of records with little difficulty and was able to compromise information of incalculable value to national security.

The Decision To Remove Restrictions On ACS

In the wake of the terrorist attacks in September 2001, FBI senior management significantly altered Bureau policy on ACS case file restrictions. This decision may have extraordinary importance for national security and the Bureau's ability to construct cases that can be prosecuted. The manner in which the decision was made also confirms that, within the FBI, operational imperatives often trump security needs, which played no apparent role in the decisional calculus.

On October 3, 2001, an Electronic Communication (EC), approved by the Deputy Director and five other senior officials, was sent from the Director's office to all FBI Divisions. This EC, titled "Restricting Cases in ACS," reinforced long standing policy that all cases must be entered into ACS, and it fundamentally changed policy by mandating that no case be restricted by designation or deliberately not uploaded without approval of an Assistant Director.

To explain this policy change, the EC noted that case file restrictions had hampered PENTTBOM, the international investigation of the terrorist attacks. Apparently, agents assigned to pursue leads in PENTTBOM had been frustrated by restrictions limiting access to potentially relevant case files, and FBI senior management had determined that the agents' frustration was well grounded.

This EC was soon followed by another, dated October 10, 2001, declaring that, on the evening of October 10, the FBI's Information Resources Division would remove certain ACS case restrictions. Pursuant to the new policy, three case classifications that had been automatically restricted as P cases lost this default protection, leaving eight P case classifications. The list of O restricted case classifications was reduced to six. Sixteen previously defaulted O case classifications lost that protection, including domestic security, hostage taking, and international terrorist investigations. Existing and new cases falling within the remaining eight P and six O case classifications would remain restricted. However, all existing cases not falling within these classifications would lose their restrictions that evening, unless an Assistant Director decided otherwise. The new policy affects not only cases previously entitled to default restrictions, but also cases that agents had opened or would otherwise open with designated restrictions. Thus, ACS users were given less than a day to learn about the EC, review restrictions on their cases, and solicit approval from a Headquarters Assistant Director to maintain restrictions on particular cases.

The decision to loosen ACS restrictions was made essentially without the involvement of the Security Countermeasures Branch, the Bureau's security apparatus.

The security consequences of this policy are difficult to assess. Obviously, many cases previously restricted by default or designation are now open to the full universe of ACS users. Substantial sensitive source material is now unrestricted. For example, while informant and asset files remain restricted, it is likely that at least some of the other case files to which source information is attached are now unrestricted.

While this new policy retained restrictions on tax and most grand jury information, other confidential information was not afforded continued protection. For instance, information collected pursuant to the Foreign Intelligence Surveillance Act (FISA) historically has been housed in restricted cases. There are complicated procedures – many driven by executive policy, but some predicated on case and constitutional law – governing the use of FISA information in criminal cases. Accordingly, problems may arise in making FISA information generally accessible throughout a system employed by agents conducting criminal investigations.[15] And a point more central to our mandate is again true: highly classified information has been made available to a range of Bureau personnel far broader than those who need to know it.

Having implemented this decision, there is little the FBI can do to reverse it. For example, ACS does not have a separate case classification for investigations employing FISA information. Consequently, while a terrorism case (now unrestricted) might include FISA information, not all terrorism cases will. Therefore, it will be very difficult to identify all cases that include FISA information, particularly now that the information is generally available and may have been picked out for use in other (perhaps even criminal) cases.

Even if the Bureau were to reinstate restrictions on certain existing cases, the case files have been generally available on ACS for some time; returning these cases to their previous security status has been likened to putting toothpaste back into a tube. Even if

---

[15] On October 12, 2001, the FBI's General Counsel ordered by Electronic Communication that FISA information newly uploaded onto ACS carry a warning about its source and declaring that the information cannot be used in criminal cases without approval from Headquarters and the Department of Justice.

senior FBI officials responsible for this policy change considered all its implications before making it, they failed to solicit the input of key security personnel, whose views might have informed their decision. Although the change may be defensible, the manner in which it was made sends a clear signal that the FBI's security organization is irrelevant during an operational crisis.

TRILOGY

The Bureau's current effort to upgrade a number of its computer networks and systems reveals many of the inadequacies in its approach to information security.

For the past several years, the FBI has requested that Congress appropriate funding to upgrade its computer systems, and upgrade proposals have evolved in response to Congressional concerns. In November 2000, Congress allocated $379 million for Trilogy, the most recent proposal.

As the name implies, the Trilogy upgrade is composed of three parts. One component involves a substantial replacement of the Bureau's telecommunications and network infrastructure. Another will implement a platform of products to make FBI computers more user friendly and to provide more centralized system management capabilities. The final component will upgrade some applications, such as the Automated Case Support system.

Trilogy is not a comprehensive upgrade. A number of networks and systems will not be affected. Only the largest networks and most widely utilized systems will be improved. A senior Information Officer likened the Bureau's existing systems to "an old car broken down in a ditch." The purpose of Trilogy is to get the old car out of the ditch, not to provide the FBI with state-of-the-art information systems.

Trilogy does present a considerable opportunity for security enhancement. For example, it contemplates a separation of the telecommunication backbones of the existing networks that could greatly improve their security. Intrusion detection technologies at the network level have also been considered to enhance the ability to monitor misconduct. The

FBI contemplates that security features in existing networks and systems will migrate to their upgraded successors. New hardware and software implemented through Trilogy will come with limited built-in security features, and an effort, called Information Assurance, is underway to propose additional security features for the upgrade.

FBI Trilogy personnel originally anticipated that the upgrade would take approximately three years to implement. Because of pressures to complete the upgrade more quickly, an aggressive schedule was devised to implement Trilogy in about two years, by June 2003. The project was proceeding according to this schedule when in October 2001, the Bureau's Director ordered that the schedule be compressed. At present, two of Trilogy's three components are scheduled to be completed by July 2002, and the third, by February 2003.

A program manager has told Commission staff that security concerns have gained prominence in the Trilogy upgrade in the wake of Hanssen's espionage, although the principal focus of the program is still clearly operational. The focus on functional improvements – "getting the old car out of the ditch" – confirms that priority will be given to operational needs. In addition, given the accelerated Trilogy schedule, design and time constraints will not permit the FBI to focus on security enhancements. It is common in the computer industry for security measures to fall by the wayside when schedules are compressed. However, given the FBI's current computer security posture, the present course is problematic; even the very rush to complete the upgrade project could enable a compromised insider to introduce holes in the system that could be exploited later.

Already, the Trilogy staff has determined that key security enhancements will not be implemented through the project. Proposed Information Assurance (IA) security enhancements, which may or may not address many security needs, are not included within the plan and will have to be integrated into the Trilogy infrastructure later. Currently, these measures have not received funding, though it may be imminent, albeit at only fifty-five

percent of the amount sought. [16]

The approach to implementing IA technologies merits discussion. The IA Program will select a number of security technologies and then canvass prospective products and vendors. After evaluating products and vendors, Program managers plan to discuss with Trilogy computer scientists whether selected products are compatible with the Trilogy infrastructure in place at that point. A more effective approach would be for the Program to identify threats to information on systems upgraded by Trilogy and then select appropriate countermeasures to address the threats. This analysis should have been performed in the original Trilogy design process.

If Trilogy, IA, and Security Countermeasures program managers do not coordinate effectively, the FBI faces a considerable threat of disjointed security countermeasures and wasted resources. The introduction of Trilogy alone will not improve the FBI's security posture and will offer little to reduce the time between defection and detection of compromised employees. If the FBI decides to implement security countermeasures after Trilogy has been designed and deployed, it will face the difficult task of assessing whether the new security countermeasures comport with Trilogy system design and the security requirements of data owners. Moreover, subsequent security additions likely will require that the FBI re-certify and re-accredit computer systems, an expensive and time consuming operation.[17]

---

[16] The IA Program requested approximately $114 million and expects to receive roughly $64 million. Accordingly, a number of security tools originally sought will not be implemented.

[17] As of September 2000, the FBI had certified and accredited eight computer systems. Bureau and DOJ security components were unaware that the FBI was operating more than these eight systems until a representative of the Information Resources Division testified before the Senate Select Committee on Intelligence in September 2000 that the FBI was operating at least fifty computer systems, of which approximately thirty processed classified information. The Bureau has since identified numerous additional systems, many of which contain classified information.

RECOMMENDATIONS

This section of the Commission's Report will not contain specific recommendations that the FBI should implement. Recommendations for improving information security tend to be arcane, and we have reserved them for the technical appendices that accompany this report. Instead, we offer five broad INFOSEC recommendations, which flow, not simply from the shortcomings in ACS and Trilogy, but from the many specific recommendations and findings about the other systems and programs discussed in the appendices.

First, the Bureau must establish comprehensive, consistent, and centrally coordinated INFOSEC policies. To implement these policies, the FBI also must create guideline-level documentation and system-specific security plans.

Second, the Bureau must implement adequate INFOSEC education and training. Classified information stored on some of the FBI's most widely utilized systems is not sufficiently protected because users lack guidance on critical system security features. While implementation of a comprehensive INFOSEC education and training program will take time, the Bureau must find a way to educate users immediately on ACS security features. As Hanssen's betrayal has shown, ACS poses a tremendous risk to information affecting national security.

Third, the Bureau must fill key INFOSEC positions, and the persons assigned to these roles must be given the time, authority, and support necessary to perform their duties.

Fourth, the Bureau must define and institutionalize a formal process to certify and accredit all computer "systems," as that term is defined in Director of Central Intelligence Directive 6/3.

Finally, the Bureau must perform the analysis necessary to develop a comprehensive, prioritized plan to address security shortcomings. The framework for this analysis is straightforward. The FBI must define the information security environment it wants to create by identifying information policies, specific threats, and secure usage assumptions. The Bureau must assess threats that existing security countermeasures do not counter and

information security policies that are not being enforced. The FBI can then select programs, tools, and technologies to sustain its security environment.[18]

Only the Bureau has sufficient information about its mission, threats, security objectives, and resources to perform this critical analysis and select security countermeasures suited to its needs. In this section of the Report and in the appendices, the Commission highlights numerous security shortcomings the FBI may need to address. Some of these problems are egregious, and corrective actions are straightforward and urgently needed.

The Bureau will have to make policy decisions about the nature of its mission and the amount of resources that will be devoted to security at each stage in the INFOSEC analysis that we recommend. Those decisions will open some avenues and close others. Certain programs, tools, and technologies will become wise investments; others, inappropriate or beyond fiscal reach. Again, the important point is not that any particular INFOSEC technology be adopted, but that the Bureau develop and follow an INFOSEC plan consonant with its mission and resources. We hope that our assessment will help the Bureau accomplish this task.

CONCLUSION

The FBI's INFOSEC problems flow from a pervasive inattention to security. Given a culture that views security as an impediment to operations, it is unsurprising that FBI computer security programs receive insufficient resources and management support. This neglect is evident at all levels, from the absence of clear, documented INFOSEC policy to the failure to educate and train computer users in the security features of their systems.

Currently, the Bureau is redefining its mission to reflect a heightened need for intelligence. Until the FBI develops and commits to a protection strategy that reflects basic security principles, such as "Need to Know" and "Defense in Depth," other intelligence

[18] We discuss many of these tools in the appendices; for example, intrusion detection and monitoring programs are discussed in Appendix A and in the Technical Report (Appendix B).

agencies and sources may question its ability to protect critical information, which will in fact remain vulnerable to espionage. Hanssen's crimes exposed the FBI's internal weaknesses. It is essential that the Bureau take rapid but appropriate steps to restore confidence in the security of its information and to protect that information from compromise.

We hope that this analysis of the Bureau's INFOSEC posture illuminates how security penetrations like Hanssen's are possible and how disastrous they can be, especially when operational imperatives hold unquestioned sway over security needs. With this analysis as a backdrop, we will now review the Bureau's personnel and document security programs and then turn to the Bureau's security structure.

PERSONNEL SECURITY

I think that [my security reinvestigations] were fine, adequate. I mean, not adequate enough to stop my espionage. . . .

– Robert Hanssen

PERSONNEL SECURITY

The Commission conducted a detailed review of the Bureau's personnel security programs, focusing on the initial investigation of applicants for employment, the process by which access and security clearances are granted, and the reinvestigation program for on-board personnel. We also examined the Bureau's financial disclosure and polygraph programs.

Detecting compromised employees and preventing penetration by hostile outsiders are the paramount goals of personnel security programs. A comprehensive personnel security system must allocate substantial resources to assess applicants and monitor employees and other personnel, focusing on those with access to critical information. Set forth below and in greater detail in the Personnel Security Appendix are a series of findings and recommendations, aimed at improving personnel security within the Bureau.

INVESTIGATION, ADJUDICATION, AND CLEARANCE PROGRAMS

The FBI uses a complex background investigation process to make determinations or "adjudications" of whether past and current conduct of employees and contractors suggests future unreliability. Under federal regulations, the Bureau employs this process in determining whether employees and contractors should have security clearances and access to FBI facilities. Failure to comply with these regulations and flaws in the investigation and adjudication process can lead to imprudently granted clearances and access and to devastating security weaknesses.

All employees are initially cleared at the Top Secret level, and every member of the workforce is supposed to undergo a reinvestigation and clearance determination every five years. Interim clearances are also granted for those who need immediate facilities access, including non-Bureau personnel, such as task-force members and contractors.

The FBI conducts a dual adjudication of its applicants. First, a determination is made as to the suitability of applicants for hiring. Individuals are evaluated on their character and

integrity, as well as their professional skills. A separate determination is made on security questions. Suitability and security issues are reviewed in different entities, the Administrative Services Division for the former and the National Security Division for the latter.

Before October 1, 2001, the investigation, adjudication, and clearance process operated as described below. After October 1, the FBI began to implement a series of changes in its personnel security programs. We support these efforts, but believe that the Bureau must fully acknowledge structural weaknesses in the program it is attempting to revamp before it can be successfully modified.

Applicants

The Bureau Applicant Employment Unit (BAEU) in the Administrative Services Division administers the applicant program and makes suitability determinations. Special Agent and support personnel applicants submit applications to field offices and must complete skill tests, drug tests, and polygraph examinations before background investigations are initiated.

Field offices conduct Personal Security Interviews and "scope" applicant cases for investigative coverage, that is, they determine the extent of the investigation necessary. The scoping is forwarded to the Background Investigation Contract Service at Headquarters, which distributes the work among Special Investigators, who conduct an investigation described later in this section.

When field work, name traces, and record checks have been completed, a BAEU analyst determines the applicant's suitability for employment. If an applicant is found suitable, the case is sent to the Personnel Security Unit (PSU) in the National Security Division for clearance adjudication.

On-Board Personnel

The PSU is also responsible for administering the reinvestigation program for FBI employees. A 1994 inspection found that the FBI reinvestigation process, which consisted of a file review, local record checks, and credit report review, was not in compliance with Intelligence Community standards. The reinvestigation process now includes full-field background investigations back to the time of the last investigation. Polygraph testing became a component of reinvestigations after Hanssen's arrest.

Before Hanssen's arrest, PSU handled reinvestigations and clearance adjudications for all employees. Since then, problematic reinvestigations, particularly cases involving employees who hold particularly sensitive positions or have access to Sensitive Compartmented Information, are diverted to the Analytical Integration Unit, created in response to Hanssen's arrest to provide deeper analysis to cases posing heightened security issues.

Personnel Security Assistants scope the re-investigative work and send leads to field offices where record checks, Personal Security Interviews, and polygraph examinations are conducted. The Background Investigation Contract Service conducts the background investigation.

Completed investigative reports are sent for adjudication to Personnel Security Specialists, who do not have investigative experience and receive only on-the-job training. The specialists rely on adjudication guidelines that summarize relevant Executive Orders and Director of Central Intelligence Directives. The analysis underlying adjudications is often superficial.

Non-FBI Personnel

The Industrial Security Unit (ISU) within the National Security Division adjudicates security clearances for a wide range of non-FBI personnel, such as task-force members, contractors, chaplains, and private attorneys, who need access to facilities or classified information.

Because time is sometimes critical, field Security Officers complete certain checks and conduct Personal Security Interviews before Headquarters security processing begins. If initial checks are favorable, Headquarters ISU may grant interim security clearances.

Of particular note are contract linguists the FBI hires to meet operational demands. Linguists involved with counterintelligence matters receive a full-field background investigation and a polygraph examination before they receive access to FBI facilities or classified information. The majority of linguists are used solely in criminal matters and may be granted escorted access to facilities before receiving security clearances.

ISU also grants interim clearances, if initial checks are favorable, to contractors, such as janitors and vendors, who need access to FBI facilities but not to classified information. These individuals, known as "unclassified contractors," are cleared at the Secret level because FBI facilities often permit open storage of classified material.

Executive Order 12968 mandates that background investigations be completed within 180 days after an interim clearance has been granted. Until recently, investigations for the majority of contractor interim clearances were overdue, and, thus, many contractors working in FBI facilities did not have final security clearances**.** An estimated fifty percent of the contractors end their FBI association before background investigations have been completed. Field offices are responsible for alerting Headquarters when non-FBI personnel are due for reinvestigation, but often they do not. ISU has no system to track non-FBI personnel due for reinvestigation. Because of an inadequate tracking system, many reinvestigations are missed completely.

The Background Investigation Contract Service (BICS)

BICS was established in 1991 to conduct background investigations and reinvestigations. It is a component of the FBI, which hires and manages around 1,700 Special Investigators (SIs), mostly retired FBI agents, throughout the country.

Once BICS receives work from a "customer" -- the Bureau Applicant Employment

Unit for new applicants, the Personnel Security Unit for employee five-year reinvestigations, and the Industrial Security Unit for non-FBI personnel -- BICS scopes leads and assigns work to SIs, along with work orders setting out the investigation and the time it will take.[19] SIs are instructed not to deviate from the work order. They must inform Case Managers of derogatory information they develop and seek approval for additional interviews in response to that information.

Although most SIs are former criminal investigators, many have limited experience in background investigations. Since they are contractors, they receive no formal training, but are given an investigative procedures manual and a four-hour orientation.

In conducting investigations, SIs must use the FBI reporting format and a procedure known as CARLABFAD, an investigative approach introduced during J. Edgar Hoover's tenure as Director, covering nine topics: the subject's Character, Associates, Responsibility, Loyalty, Ability, Bias and prejudice, Financial responsibility, Alcohol use, and Drug use. SIs, who are former FBI agents, sometimes simply ask interviewees, who are current agents, whether subjects of investigations are CARLABFAD.

When SIs complete their investigations, they usually dictate reports to one of four typing centers around the country. BICS Case Managers review SI reports for completeness and may request that missed coverage be completed. They have no adjudicative responsibilities; they only see a small part of the investigative process, and they rarely deal directly with adjudicators, who can request expanded coverage.

For the most part, BICS background investigations and reinvestigations meet the standards set down in Executive Orders and Director of Central Intelligence Directives and in some respects surpass them. Problems exist, however. Hanssen's 1996 reinvestigation highlights a number of deficiencies in BICS investigations and the Bureau's adjudication

---

[19] Staffing Assistants in the field office where the case originates also scope local record investigations, such as police and court checks. BICS Personnel Security Specialists review this coverage for thoroughness and contact the field, if coverage is insufficient.

process. One supervisor told an SI that Hanssen was in the "doghouse" with an Assistant Director about an issue related to a foreign intelligence service. The SI did not follow up on this comment or determine whether it referred to a counterintelligence issue. A co-worker described Hanssen as a "maverick," who had his "own ideas on things" and did not always "toe the line" with management. The SI failed to probe these comments. Another reference described Hanssen as "intense" with a "mixed reputation," and a supervisor stated that he was an "unusual" character. In neither case did the SI pursue these comments. Foreign travel and contacts were not addressed, although a reference commented that Hanssen was a friend of a Soviet defector. Hanssen's Personal Security Interview conducted by an NSD Security Officer also lacked depth in its coverage of counterintelligence issues. The Personnel Security Interview did not refer to foreign contacts or financial matters.

Hanssen's background reinvestigation also failed to develop details about his finances, an area that Hanssen himself identified to Commission staff as critical. Two references commented that Hanssen's children attended college on academic scholarships, and another asserted that Hanssen's wife came from a wealthy family who assisted the Hanssens. A fourth reference stated that Hanssen had money troubles. BICS did not ask that these disparate comments be explored, and PSU made no effort to determine Hanssen's true financial condition.

RECOMMENDATIONS

I. Security Investigations and Adjudications Should Be Consolidated In A New Office Of Security

Security clearance decisions are governed by Executive Orders and Director of Central Intelligence Directives that are extensive and detailed. Background investigations must comply with these mandates and fully develop issues as to character and trustworthiness. The process by which the FBI currently conducts background investigations, adjudicates cases, and grants clearances is fragmented; responsibility for

various elements is spread throughout Headquarters and the field, with no entity in control. For instance, scoping is currently performed by field security officers, Headquarters analysts, and BICS managers. This fragmentation results in duplicative efforts and wasted resources, missed leads, and unaddressed security issues.[20]

Security adjudications should occur in the new Office of Security detailed later in this Report.

II. The Personnel Security Process Should Be Automated

The system for processing investigations, reinvestigations, and adjudications is paper-driven and barely automated. For the most part, forms, investigative reports, summaries, and adjudicative material are distributed in hard copy. Lack of automation creates inefficiencies that can add weeks to the investigation process.

FBI investigation and adjudication processes should be automated. Personnel should be able to submit applications and investigation and reinvestigation material electronically. The BICS process should also be automated and integrated with the application, investigation, and reinvestigation programs, and a reliable system for tracking contractor clearance statuses should be developed.

III. BICS Investigations Should Be Thorough

Special Investigators (SIs) sometimes fail to investigate issues thoroughly, as is evident in Hanssen's reinvestigation. This results in adjudicators having less than complete information or ignoring some issues altogether.

BICS must improve the quality of its SIs. Inexperience in background investigations and, in some cases, inability lead to incomplete and inadequate investigations that do not cover adjudicative guidelines or comply with regulations. SIs frequently employ a checklist

---

[20] Scoping is also hampered by the large, confusing lead-setting manual the FBI uses to establish coverage. We recommend that the manual be simplified.

approach, content to touch upon subject areas, rather than explore them comprehensively. Case Managers, supervisors, and quality control specialists must insist that BICS SIs go beyond the CARLABFAD approach and conduct thorough interviews. Contracts with SIs who do not perform well should not be renewed.

I. The BICS Process Should Be Revamped

Fault does not lie entirely with the SIs. Institutional problems also exist. For example, BICS gives SIs only a portion of the investigative file, which often does not include the application, names of SIs conducting other portions of the investigation, or sensitive issues requiring investigation. SIs often do not have access to record checks or Personal Security Interviews and sometimes are unaware of information that could assist the investigation. SIs should be given as much information as possible about the subject of the investigation. SI contracts, work orders, and the BICS payment system discourage development of additional references, critical components of background investigations that provide adjudicators with independent sources of information.

Some Case Managers often employ the same checklist approach to reports as SIs: As long as a CARLABFAD issue is mentioned, that portion of the report is complete. Reports should be more than technically compliant with requirements; they should be sufficiently detailed to highlight and explain potential problems in conformity with the mandatory "whole person" approach to adjudications and investigations.[21]

Flaws in the way that Personal Security Interviews (PSIs) are conducted must also be

[21] Under Security Policy Board Federal Government Adjudicative Guidelines, the adjudicative process should involve a careful weighing of a set of traits, known as the whole person concept, including unquestioned loyalty to the U.S., strength of character, trustworthiness, honesty, reliability, discretion and sound judgment, freedom from conflicting allegiances, potential for coercion, and willingness and ability to abide by regulations governing sensitive information. Adjudications should be predicated on a comprehensive collection of favorable and unfavorable information from a variety of sources. Unfavorable information will not in and of itself disqualify a person from a security clearance, but is judged from the perspective of the person as a whole, about whom mitigating circumstances and conduct may be known.

addressed. These interviews are essential components of the adjudication process and are seen within the Intelligence Community as a source of significant information. Some field Security Officers do not give these interviews proper attention and employ a checklist approach. In smaller offices, where security functions are collateral duty, PSIs are sometimes delegated to staffing assistants with no investigatory experience, who often interview co-workers from their own office, a likely conflict. Responsibility for conducting PSIs should be removed from field offices and given to BICS SIs.

II. The Bureau Should Develop Professional, Well-Trained Adjudicators

Security adjudicators receive insufficient training. Some receive training from the Department of Defense, and a smaller group has attended an advanced adjudication course. However, training is not continuous and is not a priority. Some adjudicators are aware of Bureau guidelines, but others have difficulty articulating the adjudicative process and the standards governing it.

Some adjudicators lack skills necessary to conduct thorough adjudications. They also rely on CARLABFAD in checking reports for thoroughness and in determining adjudications. Adjudicators practice check-box analysis, simply making sure that investigative requirements have been mentioned, without conducting a comprehensive analysis of the information. Often adjudicators do not analyze the information at all. Some adjudicators are reluctant to request additional information or pursue missed coverage and adjudicate cases with incomplete information.

Adjudicators should receive training, and they should contact BICS SIs about coverage and reports and contact Case Managers if additional coverage is needed.

III. Stricter Controls Should Be Placed On Interim Clearances

Interim clearances are frequently granted to non-employee personnel without full scope investigations, a practice that can lead to high-risk persons being cleared without sufficient vetting. ISU sometimes fails to require full investigations after interim clearances

have been granted. In accordance with the governing Executive Order, adjudications should be completed within 180 days after interim clearances are granted. The Bureau should also implement tighter controls on personnel granted interim clearances, limiting facility access and minimizing contact with FBI employees and assets.

THE FINANCIAL DISCLOSURE PROGRAM

Financial gain is a primary factor motivating espionage. Thus, most agencies within the Intelligence Community have systems in place to detect personnel with unexplained financial gain, excessive debt, and financial vulnerabilities.

In the aftermath of the Ames case, the President and Congress took steps to enhance financial monitoring of cleared personnel. For instance, Executive Order 12968 provides for financial disclosure, expanded use of Bank Secrets Act databases, and broad financial waivers and releases from certain government employees. The Order sets guidelines for determining who must make financial disclosures and requires that all employees with access to classified information consent in writing to disclosure of financial records.

The FBI is not in compliance with Executive Order 12968. With the exception of certain senior personnel and members of the Senior Executive Service, the Bureau does not require employees or contractors to complete a Financial Disclosure Form (FDF). Financial information provided by non-SES personnel is in response to a limited series of questions on a standard form, which has little adjudicative value.

The FDF is a means of identifying persons with unexplained affluence or excessive debt. Studies have shown that most spies do not hoard their illicit gains, but purchase assets that are difficult to hide, such as real estate and automobiles. The FDF can deter potential spies by reminding filers annually that resources are devoted to identifying those who engage in espionage. The FDF can also serve as valuable documentary evidence in criminal prosecutions for espionage or false statements. The form can identify employees on a path toward serious financial difficulties and, thus, potentially vulnerable to espionage. Once

identified, these individuals can be given financial counseling. Finally, the FDF can assist in determining which employees should be polygraphed, and it can help polygraphers focus polygraph examinations, SIs conduct reinvestigations, and adjudicators make clearance decisions.

Pursuant to Congressional mandate, the CIA requires that all employees and contractors cleared for staff-like access submit FDFs annually, which are made available to financial investigators, adjudicators, and counterintelligence specialists. Initially, some CIA employees opposed the financial disclosure program as an invasion of privacy. To address this concern, the Agency began extensive briefings on the necessity for financial information in light of the Ames case.

Most CIA employees file financial information electronically and have electronic access to past years' data. Filings are processed by computer and, if certain thresholds are reached, they are reviewed by financial analysts for mistakes, omissions, and explanations for problem areas. If the analysts cannot explain the data, the employee is interviewed and databases may be checked. If this does not resolve the issues, the case is sent to the Financial Investigations Branch or referred to the Counterintelligence Center.

The Financial Investigations & Analytical Units

Many Intelligence Community studies and personnel security specialists have concluded that the ability to "follow the money" is an essential component of personnel

security programs. Thus, many agencies have established specialized units to conduct financial analyses. Hanssen himself gave us grounds to support that decision:

> No one knew of my espionage activities except the Russians, and it was done anonymously. The only thing that possibly could have uncovered my espionage activities was a complete investigation of my financial positions and deposits to bank accounts.

Before Ames' arrest, CIA investigators used financial tools to determine that he had received $1.3 million from unexplained sources. By examining currency transaction records, investigators discovered three large transactions by Ames. Investigators also took advantage of rarely utilized National Security Letters available to intelligence organizations conducting espionage investigations to gain access to Ames' bank accounts, credit card transactions, and loans. The financial analysis uncovered that Ames had made large cash expenditures for a car, a house, and home renovations. Ultimately, this financial information formed the predicate for an FBI investigation.

In 1994, as a direct response to the Ames case, the CIA created a Financial Investigations Branch to focus on personnel identified as potential security risks because of financial anomalies. The branch is staffed by analysts, including Security Officers, auditors, and former IRS Special Agents, who receive extensive specialized training.

Recommendation

The FBI Should Adopt A Financial Disclosure Program And Develop A Technical Infrastructure To Support Financial Monitoring

There are several reasons for the FBI to adopt a financial monitoring program beyond the need to comply with Executive and Congressional mandates. Financial disclosure and monitoring are effective tools in reinvestigations, adjudications, and espionage investigations. Financial disclosure can identify unexplained wealth and personnel who are financially

overextended and potentially at risk.[22]

The FBI should create a Financial Investigations and Analytical Unit and develop a financial monitoring system into which employees can enter data electronically, encrypted to ensure security. The automated system should be able to apply algorithms to identify unusual financial patterns and compare employee generated data with external sources to determine whether the employee has unreported or unexplained wealth or excessive indebtedness. Information from the FDF and the automated analysis can be used in adjudications.

The financial disclosure system will depend on the skill and experience of those who conduct financial investigations. Thus, the Bureau must recruit and develop a well-trained, experienced group of investigators and analysts.

The CIA's experience suggests the possibility that the FBI workforce will not initially have a positive reaction to the financial disclosure program. Consequently, the Bureau should educate its workforce about the financial disclosure and analysis programs and the ways in which financial information will be used. The FBI should be able to benefit from programs recently implemented at the CIA, Air Force Office of Special Investigations, and Customs.

THE POLYGRAPH PROGRAM

The polygraph examination is perhaps the most controversial tool in personnel security programs. Proponents of polygraph examinations for security screening advance three arguments in its favor. First, they assert that the polygraph is a source of important adjudicative information that often cannot be obtained through other investigative methods. Second, advocates contend that the polygraph is a deterrent: Undesirable candidates will not

[22] Hanssen has told Commission staff that he would have sought financial counseling from the Bureau's Employee Assistance Program, had he been assured of confidentiality. We recommend that the FBI make sure that sufficient resources have been allocated to that program to develop a strong financial counseling component.

apply for employment, fearing disqualification, and employees will avoid misconduct, fearing detection. Finally, polygraph supporters insist that it is a cost-effective tool for gathering information and deterring espionage.

Opponents question the scientific validity of testing, claiming that it produces an unacceptably high incidence of false positives and inconclusive results. Opponents also claim that the polygraph examination can be a highly intrusive invasion of privacy and that there is a tendency to base decisions solely on test results.

Polygraph examiners compare physiological measurements recorded in response to relevant questions to physiological measurements recorded in response to control questions. Although polygraphy has scientific components, it is not a science; it is a discipline dependent on the training, skill, and experience of the polygrapher. Physiological responses are scientific aspects of this discipline, and a properly calibrated instrument will register very accurate readings. However, the etiology of these reactions can be extremely complex. Thus, the polygraph is not a "lie detector." Test subjects may register measurable physiological responses for a variety of reasons. The most significant contribution of the polygraph is its success in eliciting information and its value as a deterrent; however, the polygraph should be but one of several investigative tools.

Polygraph examinations are utilized in personnel security screening and in security, criminal, and operational investigations. The full-scope test, the more controversial and broader of the two forms of personnel screening polygraphy, covers a wide range of topics and personal matters. It is not restricted to individuals suspected of misconduct. Opponents of full-scope tests assert that they are highly intrusive, unjustifiable invasions of privacy subject to error. Proponents contend that full-scope examinations can be narrowly focused, eliciting only information relevant to trustworthiness, national security, and adjudicative criteria.

The FBI's polygraph program was implemented in 1978 almost exclusively as an interrogation tool in criminal cases. In the mid-1980s, the FBI began to mandate polygraph examinations for agents in sensitive positions, although enforcement of the policy was rare and selective. In 1994, FBI Director Freeh authorized an applicant polygraph screening program to verify information and determine trustworthiness. Agents already on duty were not required to be polygraphed. The applicant testing format has been extended to cover espionage and terrorism.

When Hanssen was arrested in February 2001, most employees who entered on duty before 1994, Hanssen among them, had never taken a polygraph examination. A handful of Special Agents in sensitive positions had been tested, but only when detailed to organizations like the CIA, where a counterintelligence polygraph test is required. After Hanssen's arrest, Director Freeh ordered polygraph testing for the "top 500 managers," addressing contacts with foreign intelligence services and unauthorized disclosures of classified information. This effort was accomplished quickly, with four unresolved cases referred to the Washington Field Office for investigation.

The FBI's current polygraph program seems to be well managed and monitored. Adequate quality control procedures appear to be in place. The FBI is considering expanding the polygraph program to include five-year reinvestigation examinations and random testing for all personnel.

Use of the polygraph in other entities within the Intelligence Community is instructive. The CIA has utilized the polygraph as a screening tool since 1948. Over the years, the Agency expanded the program beyond applicant screening to include testing of industrial contractors and validation of operational assets. The goal of the CIA reinvestigation program is to test at least every five years persons with the most sensitive access and those with staff or staff-like access. The remaining population is tested every ten years.

In the aftermath of Ames' espionage, the CIA undertook a comprehensive review of

the use of the polygraph in its counterintelligence program. The Agency implemented a Quality Assurance Program to review polygraph results and ensure consistency in test application, interpretation, and instrumentation.[23]

The CIA went through a difficult period after the Ames case and implementation of the new screening program. Tightened procedures and attention to counterintelligence testing led to increased reliance on the polygraph and increased scrutiny of cases with significant physiological responses. The result was the so-called "A to Z cases," several hundred unresolved polygraph cases referred to the CIA's Counterintelligence Center and ultimately to the FBI. Some of these cases were open for years, causing delays in assignments and promotions. The practical suspension of these officers, or "ghosts" as they were known throughout the CIA, had a devastating effect on morale and undermined confidence in the polygraph. Ultimately, all but a few of these cases were closed as unrelated to counterintelligence concerns.

The CIA and the National Security Agency have kept up with technological enhancements in the field and use specialized tools to standardize the technical aspects of the discipline. Computerized polygraph instruments and the digital transfer of files and charts between headquarters and the field through secure connections have drastically improved efficiency. The new technology allows for seamless case management of a widely dispersed work force, near real-time quality control from headquarters, and the reduction of time and storage space. These agencies also spend considerable resources on employee

---

[23] CIA examiners, as well as FBI examiners, are trained at the Department of Defense Polygraph Institute (DoDPI), a recognized center for polygraph training, research, and development. DoDPI emphasizes criminal testing, the most common use of the polygraph within the government. DoDPI has also implemented a counterintelligence training module taught by CIA personnel.

After the three-week CI module at DoDPI, new CIA examiners continue CI training at the Agency because of the complexity of counterintelligence and security examinations. Likewise, NSA examiners, upon completing DoDPI training, receive extensive additional training and are closely monitored until they become proficient in counterintelligence polygraphy.

awareness programs relating to polygraph examinations. Educational briefings are held regularly, as well as one-on-one sessions when requested, so that the concerns of polygraph candidates can be addressed before the examination.

RECOMMENDATION

The FBI Should Implement A Counterintelligence Polygraph Program And Create An Infrastructure To Support The Program

The FBI should continue to conduct full-scope tests on applicants and should adopt a counterintelligence test in reinvestigations of employees and non-FBI personnel with SCI and special access clearances. This approach focuses on personnel who may pose the greatest risk to national security and minimizes the risk of false positives.[24]

Bureau training is currently insufficient for counterintelligence testing, which requires technical skills for eliciting information, developing themes, and understanding CI issues, skills that differ from criminal or full-scope testing skills. As the Bureau moves into specific-issue CI testing, it should develop quality control and assurance programs for this discipline.

The Bureau should upgrade the technical instruments used in its polygraph program. Improved technology and computer driven systems will ease data storage and transmission of results for Headquarters review. The systems will also permit the FBI to keep statistics and conduct audits.

Adverse personnel actions should not be taken solely on the basis of polygraph results. This judgment is consistent with current FBI policy, which establishes a procedure for reviewing examinations that produce "no opinion," inconclusive, or "deceptive" results.

---

[24] Our recommendations concerning polygraphy for the most part comport with changes the Bureau made following the detection of Hanssen's espionage. However, those changes are often embodied in interim or draft policy statements, which we believe should receive final approval.

That procedure appears to comport with the due-process rights that Executive Order 12968 affords federal employees who have been denied access to classified information.

The FBI should anticipate employee concerns by developing an education program to explain the polygraph's security role and alleviate concerns about "lifestyle witch hunts" and intrusive screening.

CONCLUSION

FBI personnel security programs, with some important exceptions, comply with governing laws and regulations. Nonetheless, they often fall short of best practices observed in agencies across the Intelligence Community. The Bureau should look to programs in those agencies as models to enhance security.

DOCUMENT SECURITY

Security was lax . . . [in] that you could bring documents out of FBI Headquarters without . . . ever having a risk of being searched, or looked at, or even concerned about.

– Robert Hanssen

DOCUMENT SECURITY

Much of Robert Hanssen's espionage involved compromising FBI document security by photocopying or downloading classified material and carrying it out of Bureau facilities. Thefts by a trusted employee entitled to read most of what he stole are difficult to prevent, short of invasive searches. No document security system can unfailingly prevent employee theft. However, reasonable measures can be taken to make theft more difficult and easier to detect.

FBI employees working with classified material operate in a culture that unduly emphasizes operational efficiency at the expense of document security. As a result, classified information, spread throughout the Bureau on paper and on widely accessible computer networks, is inadequately secured.

To access classified information, an FBI employee must have a security clearance and need to know that information. Since every FBI employee has a Top Secret clearance, the clearance alone becomes essentially irrelevant as a tool to control access to classified material within the Bureau. That leaves enforcement of the need-to-know principle as the linchpin of access control. The principle purposely slows down information flow to ensure that personnel actually need to know the information they receive to perform their jobs. This is sometimes inconvenient and at odds with the criminal investigative culture dominant at the Bureau. The overarching solution to document and related physical security problems at the FBI will require a profound realignment of culture to emphasize that classified information should be shared only to the extent necessary for successful operations. FBI employees must be taught and regularly reminded why the need-to-know principle is worth the inconvenience it can cause and how the principle can be employed in such a way that operations are not impaired.

Operational efficiency is important, and tightening controls on classified information will come at a cost in resources and efficiency. Moreover, additional controls will not

prevent disloyal employees from memorizing information that could harm national security. Accordingly, the recommendations we make are intended to accomplish three relatively modest goals: spur the FBI to address significant gaps in protocols for handling classified information; create a central authority for coordinating security violations and compliance activity; and create a workplace culture that minimizes security lapses and makes disloyal employees more quickly visible. If these goals are met, the FBI will strike a sound balance between operational efficiency and document security.[25]

CLASSIFIED DOCUMENT PRACTICES

It is impossible to determine the number of classified documents the FBI receives, generates, and handles each year because production and copying of Secret documents are not regulated.[26] Some sense of the volume of classified material can be gleaned from the fact that, in the year 2000, Headquarters received 35,956 Top Secret/Sensitive Compartmented Information (TS/SCI) documents, almost all of which were processed through a Special File

---

[25] Appendix K covers in much greater detail the material reviewed in this section of the Report. Appendices L through T provide reference material to explain and support our recommendations. Appendix L sets out the rules governing Secret document security; Appendix M describes the FBI's use of SCIFs and Secure Areas for handling national security information; Appendix N provides the rules governing Top Secret and Sensitive Compartmented Information security; Appendix O is a flow chart illustrating the movement of TS and SCI documents at FBI Headquarters; Appendix P is a comparison of FBI and Intelligence Community classified document handling policies; Appendix Q explains the process for obtaining FISA orders; Appendix R describes the rules for reporting and investigating information security violations; Appendix S collects in charts SEPS security compliance review results, damage assessments, security violations reported to OPR, and security deficiencies noted in Inspection Division Reports; Appendix T describes other physical security issues noted by Commission staff.

[26] This Report will cover Secret and Top Secret (TS) information and an access control called SCI or Sensitive Compartmented Information. Secret information is material whose unauthorized disclosure may cause serious damage to national security. TS information is material whose unauthorized disclosure could cause "exceptionally grave" damage to national security. SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Room. In the same year, the FBI Mail Services Unit received 7,212,388 pieces of mail, 125,000 FedEx packages, and 713,306 courier deliveries, of which about fifteen percent was classified Secret, TS, and/or SCI. More than 500,000 files containing TS/SCI material are stored in the Special File Room. In addition, the FBI receives about 30,000 classified teletypes per month from other government agencies. In 2000, the FBI itself classified Secret or higher around 185,000 internally generated documents.

Secret Information

The FBI receives, generates, and stores a vast amount of material classified Secret, including counterintelligence, counterespionage, and counterterrorism information. Secret documents need not be individually tracked as TS/SCI material is.

The Bureau considers Headquarters and field offices Secure Areas appropriate for open storage of Secret material, even though the process of approving Headquarters as a Secure Area in compliance with DOJ regulations began only after the Commission requested documents supporting the designation of Headquarters workspace as Secure. Because these spaces are considered Secure Areas for open storage, Secret material can travel within Headquarters, be left out during working hours, and be minimally secured at night. The FBI also routinely uploads Secret material to its ACS databases, a form of electronic open storage that allows essentially unregulated downloading and printing. Open storage also means that hard drives that contain Secret material need not be stored in a security container after working hours.

As a result of this approach to Secret material, FBI employees without a need to know have relatively easy access to the material. Non-employees inside FBI facilities, such as contractors, can potentially observe or collect classified material, at least in document form. Anyone gaining unauthorized entry to Headquarters would also gain access to openly stored classified material. At Headquarters, most components dealing with classified national security material reside in Sensitive Compartmented Information Facilities (SCIFs) or in

Secure Areas.[27] However, access to those areas is not always well-controlled, and classified material moving to and from them may be vulnerable. At field offices, openly stored material may be accessible to personnel who do not need to know that information.

Training in transporting and storing Secret material comes typically on-the-job, and document security practices vary widely from component to component. The FBI imposes no physical controls on disseminating and copying most categories of classified material within FBI space. Few units heed directives about placing classified material face-down when persons not authorized access are nearby, using cover sheets, destroying unneeded working copies, classifying and safeguarding needed copies, and maintaining protocols for securing computers, waste, notes, and security containers. Secret documents are often destroyed off-site in a fashion that does not completely protect against loss or theft. Security Officers assigned to assist with classified document issues are frequently undertrained and do not receive management support.

FBI uniformed security police, who provide the primary line of defense against unauthorized entry at Headquarters and other facilities are understaffed, insufficiently trained, and ill equipped to deter improper removal of classified material. The authority of these officers is undercut by providing FBI executives with "gold badges" that allow them and visitors they escort to bypass normal security and by "executive escorted visitor badges" that allow uncleared visitors repeated escorted access.

RECOMMENDATIONS

I. Classified National Security Documents Should Be Handled And Stored In SCIFs And Secure Areas Segregated From Other Components And Available Only To Those With A Need To Know

---

[27] A SCIF is a facility that has been constructed according to DCID standards and has received CIA accreditation. A Secure Area is an area with enhanced physical security protections, such as continuous protection by guards or alarm systems.

Given the ubiquity of ACS, Headquarters should immediately undergo the formal review required for open storage of Secret material. The Bureau should train employees that compartmentation and need-to-know principles apply even in Secure Areas. Those principles should be enforced by ensuring that all components handling classified material operate in Secure Areas or SCIFs. Employees in those areas should be well trained and supported in maintaining security. Headquarters SCIFs and Secure Areas should be located on the same floor or in the same part of the building, segregated from components that do not routinely use such information. Access to these areas should be closely controlled. Field squads that handle classified material should be segregated in Secure Areas that cannot be routinely accessed by personnel with no need-to-know.

II. The SACS Badge System And The FBI Police Program Should be Strengthened

Access to Secure Areas and SCIFs should be controlled by Secure Access Control System (SACS) key-card scanning devices. Every employee entering a SACS area should be required to "badge in." The SACS system should require personal identification numbers in addition to a badge scan. All passengers in car-pools entering Headquarters should be required to badge into the building.

The FBI uniformed security police should be brought to full strength and trained to identify unauthorized and inadequately secured classified material being removed from Headquarters. The police should also be trained in security protocols and should conduct aperiodic checks of vehicles and carrying cases leaving Headquarters to emphasize the gravity of document security. They should also examine the photograph on every SACS badge entering Headquarters for a match with the bearer. The badges of non-employees with unescorted access should clearly note that the bearers are not FBI employees. "Gold badges" and "executive escorted visitor" badges should be eliminated.

III. The FBI Should Enhance Protections On Handling, Copying, And Disposing

Classified Material

Classified information should be placed face down when persons not authorized access are nearby. Cover sheets should be required; working copies of classified documents no longer needed should be destroyed; if they are needed, they should be classified and safeguarded. An after-hours protocol for securing computers, waste, notes, and security containers consistent with DOJ's mandates should be established in all Secure Areas and SCIFs.

Headquarters employees should receive guidance about moving classified information about the building. At a minimum, Secret and higher classified material should be placed under cover sheets and sealed in addressed, opaque envelopes. Employees should be prohibited from leaving classified material unattended in any part of the building that is not a SCIF or an approved Secure Area.

Photocopying Secret material should be held to a minimum, and copies of classified documents should be subject to the same controls as originals. FBI manuals should establish a time limit for maintaining working copies of classified documents so that managers can better monitor retention of copies. Photocopiers, particularly in SCIFs and Secure Areas, should not be operable without personal identification numbers, or copying centers should be created and staffed by employees trained in classified document security. The FBI should study the feasibility of bar coding particularly sensitive classified material, such as asset files, to facilitate control and tracking.

Security risks in the off-site destruction of Secret waste should be eliminated by ensuring that all units that handle classified material have sufficient shredders and by greatly enhancing central destruction capabilities at Headquarters.

Top Secret and Sensitive Compartmented Information

Director of Central Intelligence Directives and FBI regulations prescribe requirements for access to and handling, storing, and destroying Sensitive Compartmented Information

(SCI). Before being given access to SCI, FBI employees and contractors must have appropriate clearances, access approval, and a clearly identified need to know the information; they must also be "read in," that is, undergo a briefing, and sign a non-disclosure agreement. SCI cleared individuals are subject to additional security procedures such as a more vigorous adjudication of background re-investigations, and they are obliged to report foreign contacts and travel.

Security programs designed to safeguard TS and SCI material at the FBI are problematic. The provisions in Bureau manuals controlling security are incomplete and cumbersome to access, and their importance day-to-day is not stressed.

The need-to-know requirement seems to be generally observed in the dissemination of documents, and SCIF accreditation procedures are followed, but security requirements are sometimes sloppily observed and casually enforced. Knowledge of the requirements for handling TS/SCI and sensitivity to this material must be enhanced across the board.

A huge amount of TS/SCI arrives at Headquarters every year, and a substantial amount remains there indefinitely, creating a practical problem of allocating limited space to dated, but sensitive information.

Information profiling, the description of TS/SCI information that other intelligence agencies should send the FBI, is not effectively employed. Once the Special File Room disseminates TS/SCI information, it is not routinely protected by cover sheets, and there are no effective controls on copying. Safes where TS/SCI is stored in operational units are not routinely audited for classified material no longer needed.

Few Unit and Section Chiefs are familiar with manual provisions relating to TS/SCI, although they are aware that this material must be given greater protection than other classified material. Most learned this from on-the-job training. At the operational level, most Unit and Section Chiefs rely on Security Officers in the component to protect classified material. The knowledge and experience of these Officers varies markedly.

While FBI employees who routinely work with TS/SCI information are generally

aware of the procedures for receipt, storage, dissemination, and disposition of that information, most do not have detailed or consistent knowledge about those procedures and are not aware of the written authorities governing them. Our own observations corroborate employee anecdotes about security lapses, such as SCIF doors propped open with no access controls, SCI material faxed on non-secure machines and incorporated into unclassified documents on uncleared word processors, and SCI material transported without proper protection.

RECOMMENDATIONS

IV. Written Guidance On TS/SCI Should Be Current, Clear, And In Compliance With DCIDs

FBI manuals and other written policy statements should incorporate changes made over time by Bureau Electronic Communications and should comply with Executive Orders and Director of Central Intelligence Directives. Written policies should provide clear, specific guidance to Security Officers, who are sometimes unaware of policy because they do not know how to locate it. Policy amendments and clarifications should be routed to Security Officers. The manuals should also be revised to remove widespread confusion about controlling TS/SCI documents obtained through electronic systems and working documents that have not been incorporated into official files. Manuals and other written guides should be revised to address SCIF operating procedures.

V. The Operations Of The Special File Room Should Be Improved By Eliminating Unnecessary Classified Material And Enhancing Staffing, Training, And Equipment

The Bureau should undertake the difficult, labor-intensive task of reviewing the hundreds of thousands of files within the Special File Room to destroy all documents eligible for destruction, especially if the Bureau decides to maintain the large amount of TS/SCI

received in the wake of recent terrorist attacks.

While statutes and regulations limit the Bureau's authority to destroy TS/SCI material that is part of an FBI file, two steps can be taken to reduce the amount of unnecessary paper. One is to develop a more effective profile to control the amount of information sent to the Bureau by NSA, CIA, and other agencies. Tailored descriptions of the material FBI personnel need will reduce the large volume of marginally useful information coming to the FBI and warehoused in SFR space. The second step is prompt destruction of unneeded material. Some FBI personnel assert that the failure to destroy unneeded TS/SCI is rooted in a concern about potential personal or institutional embarrassment if destruction of particular documents is challenged in the future. However, warehousing thousands of documents to ward off possible future criticism is unproductive because forgotten and unindexed SCI is of no greater use than destroyed material.

VI. SCIF Operations Must Be Improved By Promulgating Clear, Enforceable Rules And Providing Training For SCIF Tenants

The operation of Bureau SCIFs across the country is inconsistent and sometimes improper, for example, doors are propped open, visitors are unchallenged or unescorted, and end-of-day inspections do not occur. SCIF operations should be consistent across the Bureau and should be controlled by clearly written guidelines, as the DCIDs require. This will also require improved training for SCIF personnel.

SCIF accreditation, daily operations, and periodic reviews require much greater resources than are currently allotted. When briefed into SCI operations, FBI personnel should receive clear and complete instructions about proper SCIF operations.

VII. The FBI Should Consider Adopting The Human Intelligence Control System

The FBI's failure to give human intelligence more protection than it does is somewhat at odds with its traditional desire to protect human sources.

The Bureau should carefully consider adopting the Human Intelligence Control System, a system of compartmenting human source information developed by the CIA, so that this particularly sensitive information receives more protection than comes with the Secret classification the FBI typically applies to human intelligence. If it does adopt this approach, it should publish clear, written policies effecting those controls and train those who will use them.

FISA DOCUMENTS

The Foreign Intelligence Surveillance Act (FISA) establishes a procedure by which intelligence about the actions and intentions of foreign powers and their agents can be collected in the United States through electronic surveillance and physical searches. FISA is a process reserved for the most important FBI counterintelligence and counterterrorism cases. Applications for FISA warrants and for renewals are made through DOJ's Office of Intelligence Policy And Review; they have grown steadily since 1978 from about 200 annually to more than 1,000.

The use of FISA warrants and the information collected through them are extremely sensitive. Applications for court-ordered surveillance, supporting affidavits, and the orders themselves are at a minimum Secret. They also frequently contain TS/SCI information. A breach of security in the FISA process may result in a target becoming aware of FISA coverage and ceasing the forms of communications that FISA collects. As a consequence, security is essential in acquiring FISA coverage, implementing and storing FISA orders, and handling the product of FISA warrants. The FISA process is long and cumbersome; it involves large amounts of classified documents in constant motion through the FBI and DOJ

under minimum security controls. The present process constitutes a security risk.

There are three key security weaknesses in the FISA process: 1) the absence of secure computer links between the FBI and OIPR requires that classified FISA documents be carried by hand between DOJ and Headquarters, creating risks to the physical security of the documents; 2) Within the FBI, Secret FISA material circulates, typically on paper, with insufficient controls and with no method for determining who has had access to it; and 3) Once classified FISA orders have been served, the FBI and DOJ do not consistently or completely verify that carriers (telecommunications and internet service providers) maintain proper security for those orders.

RECOMMENDATIONS

VIII. Secure Electronic Links Should Be Established Among Participants In The FISA Process

A FISA process completed through electronic links among the participants will enhance security and allow the parties to consult and agree to changes simultaneously and without the risk of lost or misplaced classified documents. The technology would permit system audits to reveal individuals who attempt to access FISA material without a need to know.

I. The FISA Process Should Be Simplified

Many studies have concluded that the FISA process should be streamlined by reducing the number of people who review FISA packages. These studies also point to redundancies in the review process: multiple reviews of documents by the same entities for the same purpose and by different entities for the same purpose. Our review has confirmed that these criticisms of the FISA process are valid. Redundancy in the current FISA process threatens security.

X. The FISA Unit Should Be Responsible For The Security And Tracking Of FISA Packages

Until FISA applications are processed purely electronically, precise tracking of documents through the process is essential to prevent unauthorized exposure of FISA information and to identify all persons who have had access to FISA documents. Responsibility for the security and tracking of FISA packages and orders as they move through the FBI should be centralized in an FBI FISA Unit. The Unit should emphasize security through the use of a computerized tracking system and other measures mentioned in the appendices. The Unit should coordinate with FBI components controlling carrier clearance and monitoring to ensure that FISA orders are not forwarded to insufficiently secure telecommunications and internet service providers.

XI. Access To FISA Information In ACS Should Be Restricted

Knowledge about particular FISA warrants and the information they collect is too sensitive to be made available to all FBI personnel through the ACS database. Such exposure is a clear violation of the need-to-know principle and may result in FISA information leaking into criminal prosecutions, thereby potentially compromising intelligence collection, revealing sensitive techniques, and threatening successful prosecutions. As soon as possible, access to FISA-related information in ACS must be restricted. Personnel with access to that information should be trained in the use of access restriction functions in the ACS database. Steps should also be taken to control, if not eliminate the ability to print and download FISA information from ACS.

XII. Carrier Clearance, Compliance, and Monitoring Must be Ensured Through Strengthened FBI Security Programs.

FBI management must vigorously support security procedures necessary to ensure that

carriers receive timely security clearances, store and handle classified FISA information properly, and are regularly inspected.

FISA security programs at Headquarters and in the field must be fully staffed by trained personnel. Current carrier clearance practices should be amended to allow rapid interim clearances of carrier personnel when operational emergencies require dealing with uncleared carrier personnel. In those instances, trust receipts (unclassified documents replacing FISA Orders) must be mandated until full clearances and appropriate security protections can be implemented at those carriers. The FBI should devise a strategy to employ trust receipts exclusively. An aggressive security compliance program should ensure that common carriers are cleared and handling FISA material appropriately.

COMPLIANCE AND DISCIPLINE

Document security improvements will be short lived absent a means of ensuring compliance with policy. The Bureau needs a central authority to coordinate and track security compliance and discipline programs, which now reside in three FBI components, the Inspection Division, the Office of Professional Responsibility (OPR), and the Security Countermeasures Section (SCMS), and one DOJ component, the Security and Emergency Planning Staff (SEPS). The Inspection Division conducts detailed inspections of Headquarters components and field offices to ensure compliance with FBI programs, including security. OPR is charged with investigating allegations of misconduct by FBI employees and imposing discipline. SCMS conducts damage assessments when classified material is lost or not secured and is responsible for accrediting Sensitive Compartmented Information Facilities, approving Secure Areas, and coordinating between Headquarters and field Security Officers. DOJ's SEPS conducts periodic compliance reviews of certain FBI security programs.

Executive Orders, federal regulations, and internal written policies control the reporting and investigation of security violations involving classified information. This

framework gives the Bureau considerable authority to police internal classified information security violations. However, this authority is not exercised aggressively or cohesively, in large part because reporting information about potential security violations to the Inspection Division, OPR, and SCMS is governed by overly general and insufficiently clear manual provisions. The manuals do not require that OPR, the Inspection Division, and SCMS share information about actual or potential security violations.

OPR records for roughly the last five years reflect 84 security related disciplinary matters, of which 31 appear to involve classified material security breaches. In approximately the same period, SCMS conducted about 360 damage assessments and concluded that classified information security had been breached in 149 instances. Inspection reports addressing the nine field offices inspected in the last three years contain 84 negative findings about breaches of classified information security. SEPS compliance reports from 1993 to 2001 reflect approximately 300 violations of security and approximately 160 security recommendations. Because the FBI lacks a central repository for collecting and analyzing security violations, it is impossible to ascertain whether these events overlap and whether OPR, the Inspection Division, and SCMS considered every matter potentially within their jurisdiction.

Interviews reveal that FBI personnel scrupulously follow rules when performing duties subject to OPR enforcement. One senior agent well versed in these issues reported that, as a result, the Bureau has historically fixed problems by assigning them to OPR as high priorities. Components slated for periodic inspection by the Inspection Division are also extremely attentive to issues and programs under inspection.

The absence of a central collection point for security breaches is a serious problem. Lack of coordination among OPR, the Inspection Division, and SCMS gives the FBI little capacity to identify or profile individuals and operational components engaged in patterns of security violations. This, in turn, increases the possibility that habitual security violators will remain undetected and that punishment for a discrete violation will not be commensurate

with the true scope of improper activity. At a minimum, this security infirmity means that the FBI has no central data base that would enable these components to cross-reference their work and ensure that each is aware of all reported potential violations within its jurisdiction.

RECOMMENDATIONS

XIII. A Central Security Authority Must Coordinate And Oversee All Document and Physical Security Violations and Compliance Activity

Currently, the Office of Professional Responsibility, the Inspection Division, the Security Countermeasures Section, and DOJ's Security and Emergency Planning Staff have separate roles in detecting, investigating, and assessing security violations or imposing discipline; no single entity has responsibility to coordinate, track, and oversee security violations and enforce compliance. A central authority for coordinating security issues among all FBI entities, with the power to rescind security clearances, will create a powerful incentive for employees to comply with good security practices. The authority will be afforded the same institutional deference that OPR and the Inspection Division now receive.

A database should be developed so that patterns of security violations by individuals or components can be detected.

XIV. FBI Policy Manuals Should Require Security Coordination

To bolster this central security authority, manuals addressing SCMS, OPR, and Inspection Division security referrals should be updated and reconciled. They should require initial reports to the Security Programs Manager of all suspected, possible, and actual losses or compromises of classified information. They should also require that allegations of loss, suspected loss, and compromise of classified information be referred to OPR.

The manuals should clearly and in detail explain categories of security violations and levels of punishment. The present system, which simply puts security violators on notice that their actions can lead to discipline, is inadequate. Lastly, the manuals should require input from SCMS into OPR, field office, and Headquarters investigations of security issues. Currently, OPR can authorize Assistant Directors and Special Agents-in-Charge to investigate serious classified information security breaches within their components. SCMS should review the results of delegated investigations before final adjudication to ensure that investigators understand the scope and impact of potential security breaches and to enhance centralized collection of information about security breaches.

CONCLUSION

This section has outlined particular steps that should be taken to ensure document security or at least make it much more difficult for disloyal employees to compromise material that undergirds national security. Those steps and the reasons for them are explained in greater detail in the appendices. However, the detail should not obscure the broader point that security will never be effective unless Bureau personnel are trained to appreciate the importance of the information that goes through their hands and the necessity for tight controls.

SECURITY STRUCTURE

. . . [I]f I had been a more malevolent spy than I was, [the FBI] would have had a very difficult time finding me.

– Robert Hanssen

In addition to the security programs previously described, the Commission reviewed the Bureau's security structure, focusing on how the FBI organizes security functions at Headquarters and in the field and how responsibility for security policy is delegated. We reviewed staffing levels and the criteria used in selecting personnel for security positions. We examined the Bureau's programs for security education, awareness, and compliance, as well as its training programs for new agents, Security Officers, and other key security personnel. Finally, the Commission reviewed the Bureau's procedures for reporting, investigating, and disciplining security violations and the procedures for inspecting security programs.[28]

The Commission also gathered information about security organization in other agencies so that we could incorporate "best-practices" into our recommendations. We focused on security programs at the CIA, NSA, and Department of State, as well as the Air Force's Office of Special Investigations, which, like the FBI, has law-enforcement and intelligence missions. Many of these agencies place much greater emphasis than the FBI on security, in part to correct program deficiencies discovered during their own internal espionage investigations. The lessons they have learned should be invaluable to the Bureau as it assumes an enhanced role in combating terrorism and ensuring national security.

---

[28] During our review, Headquarters officials responsible for security and their staffs provided detailed briefings on Bureau security structures, describing shortcomings in the security program, programmatic changes underway, and suggestions to strengthen the program. We interviewed dozens of other Bureau personnel with security responsibilities. During a training program at the FBI Academy, we spoke with many Security Officers about their job functions and suggestions for change. Appendix J explains in more detail the results of our review of the Bureau's security structure.

In general, we found serious weaknesses in the structure of Bureau security programs, arising from several organizational defects:

- Security functions are dispersed across eight Headquarters divisions and many field offices, resulting in a lack of uniformity and accountability
- No single group is responsible for developing and implementing security policy
- The Bureau has not designated security as a core function critical to its mission
- FBI management often slights the security program in favor of operational functions
- The security program has not been professionalized

A comparison of the Bureau and other agencies in the Intelligence Community reveals numerous similarities, but significantly different programs and results. The information needing protection and the external regulatory structures are almost identical. Each agency has implemented security programs based on organizational threats and has established countermeasures based on risk assessments. Nonetheless, the FBI's security program falls short.

The FBI has not dedicated sufficient resources to security. Other agencies have substantially enhanced the responsibility and visibility of their security programs within the past few years, but the Bureau has lagged behind. Although the Bureau has begun to take steps to improve security, it has failed to follow the Intelligence Community in designating security as a core function. Senior management has not successfully integrated security into the FBI's operational mission. Simply put, security is not as valued within the Bureau as it is in other agencies. As an FBI Internal Security Task Force noted, "[s]ecurity policies are too often viewed as a nuisance to negotiate around, rather than [as] edicts with which to

comply."[29] Until recently, the security program was buried within the National Security Division, with no immediate reporting relationship to the Director. The Security Programs Manager has little or no authority over security programs in other Headquarters divisions or in the field. Few personnel are dedicated to security, and it is widely recognized that security assignments are not career-enhancing. These facts and perceptions diminish the role and importance of what should be one of the FBI's most critical functions.

Despite efforts to improve security, staffing and funding for FBI security programs are deficient. Funding for the security program has been part of the National Security Division budget, and NSD management has often shortchanged the program or used security personnel for operational functions. Between 1994 and the beginning of fiscal year 2000, the number of personnel assigned to the Security Countermeasures Branch declined by eighteen per cent. As of August 2001, 174 employees or 0.64 per cent of the Bureau's staff were assigned to security programs. Other agencies within the Intelligence Community devote significantly more personnel resources to security.

With this background and considering the lessons learned in our review of particular Bureau security programs, the Commission advances the following recommendations to improve FBI security structure.

I. FBI Security Programs Should Be Integrated In An Office Of Security That Reports To The Director

Bureau management must commit to a security program that receives markedly greater stature, resources, and visibility. The Commission recommends that the FBI establish an independent Office of Security, led by a senior executive reporting to the Director. The head of the office should be responsible for developing and implementing Bureau security programs, with authority to take critical security issues to the Director so that the Office speaks with the endorsement of the Director. Consolidating security functions under a senior

[29] Recommendations of the Internal Security Task Force, Apr. 17, 2001, 4.

executive will ensure constant focus on security by senior management, promote resolution of conflicts between operational and security imperatives, strengthen the security program at Headquarters, and foster coordination with the field.

The elevation of the security program to a senior management level is consistent with the best practices we observed at other federal agencies. In recent years, the CIA, NSA, and State centralized security functions in a single office at the senior executive level. These reorganizations have been accompanied by funding and staffing enhancements and management commitment to robust security programs. For instance, three years ago, the CIA consolidated its security programs into an Office of Security to eliminate security gaps that had resulted from uncoordinated programs. Today, the CIA's Director of Security participates in all senior management board meetings.[30]

The Commission's recommendation for the establishment of an independent security organization is consonant with several internal assessments of Bureau security programs.[31] In December 2001, the Bureau responded to these assessments by creating a Security Division, reporting to the Executive Assistant Director for Administration and by transferring the security function from the Security Countermeasures Branch of the National Security Division.[32] The realignment of the security function into an independent Security Division

---

[30] The State Department has recently undergone a similar reorganization of its security office in response to significant security lapses. The Assistant Secretary of State for Diplomatic Security and Foreign Missions is now Principal Advisor to the Secretary of State for Security Matters. At NSA, the Associate Director of the Directorate for Security reports to the Director.

[31] 2002 - 2006 Security Countermeasures Program Plan (Sept.10, 2001); FBI Information Security: Report of the Information Security (Infosec) Working Group to the Internal Security Task Force, (Aug. 2001); Recommendations of the Internal Security Task Force (Apr. 2001).

[32] Under the restructuring, most security functions will be consolidated in a Security Division with three principal sections: Personnel Security, Physical and Technical Security, and Information Assurance. The Division is responsible for developing security policy, issuing clearances, approving access to Bureau information and facilities, overseeing programs to protect SCI, approving space as secure areas or SCIFs, certifying and accrediting information systems, developing and delivering security awareness briefings and materials, conducting on-site security evaluations, and delivering these services to Headquarters components and field offices. The

is a good first step toward enhancing the role and visibility of the security program. The Bureau must, however, fully staff and implement the proposed program.[33]

The Commission recommends that the FBI consolidate in the Office of Security all security functions now spread across Headquarters and the field. The FBI's security program, in sharp contrast to other agencies' security organization, is fragmented, with responsibilities residing in eight Headquarters divisions and fifty-six field offices. Many agencies within the Intelligence Community have consolidated their security programs to effectuate a Defense-in-Depth strategy, under which all aspects of security (for example, personnel and INFOSEC programs) are part of an integrated program.

Best practices in the Intelligence Community separate information systems security from day-to-day computer operations. The Office of Security is the logical focal point for efforts to ensure the security of the Bureau's information systems. It should be responsible for validating security measures to ensure the confidentiality, integrity, and availability of intelligence information and for all operations that protect information and information systems, including intrusion detection, vulnerability assessments, real-time auditing and monitoring, and incident response.[34]

The Commission also recommends that the Office be responsible for security at Headquarters and Quantico, including responsibility for FBI police, access control, construction design security, technical surveillance countermeasures, and physical and

---

Security Division also represents the Bureau on multi-agency committees on security.

[33] Under the restructuring, the Security Division and the Counterintelligence Division, which is responsible for conducting counterespionage investigations, will report to different Executive Assistant Directors. It is critical that these Divisions work together on current and proactive internal espionage investigations.

[34] DOJ's Security and Emergency Planning Staff (SEPS) is responsible for developing security policy and overseeing its implementation in Department components, such as the FBI. Although we have not examined SEPS in detail, the program seems to suffer from many of the structural weaknesses that led us to recommend creation of an Office of Security in the Bureau, weaknesses such as inadequate resources and insufficient stature within the Department's structure. We recommend that the Department address this issue.

technical security countermeasures.

The FBI should follow the lead of other agencies and consolidate within the Office of Security responsibility for initial background investigations for new employees, contractors, and linguists, as well as periodic re-investigations. The polygraph component of the clearance process should be placed within the Office of Security.

Finally, the FBI must enhance within the Office integrated information tracking and analytical capabilities. Unlike other federal agencies, the Bureau is unable to conduct in-depth analyses of personnel data to identify potential counterintelligence concerns or anomalies that could result in the compromise of sensitive information. The ability to perform this function depends on the creation and maintenance of databases to collect security information, as well as automated tools to extrapolate and interpret that data.

The Analytical Integration Unit (AIU) established by the Security Countermeasures Branch in May 2001 is a positive first step toward developing this capability. The Unit was initially created to analyze potential derogatory information about personnel with access to the Bureau's most sensitive information. Eventually, the AIU will be responsible for integrating security information with counterintelligence, resolving anomalies, analyzing problem cases and performing detailed financial analysis. Bureau management anticipates that the AIU will be responsible for reporting programs covering financial disclosures, foreign travel, foreign contacts, outside employment and roommates. We endorse the enhancement of this Unit.

II. Responsibility For Security Policy Should Be Vested In The Office of Security And Managed By A Security Policy Board

The FBI's approach to security policy has been as fragmented as its security programs. Because no single component is responsible for policy, critical gaps in security programs have developed. Some of the more severe weaknesses result from unwritten security policies, often implemented without input from the Security Countermeasures Branch. The Office of Security should be responsible for ensuring that FBI components

comply with government security standards and that all employees are aware of security policy.

Other agencies have built into management structures processes for coordinated security policy development and have appointed senior officials to implement policy. At the CIA, for example, the Chief of the Security Policy Staff within the Office of Security oversees a staff of professionals who coordinate draft policies with affected components before final approval. A Security Policy Board of senior agency officials from each Directorate meets every other month to review security policy.

The FBI should adopt a similar approach to security policy to ensure that groups with divergent interests do not work independently and that security is not inappropriately sacrificed to operational objectives. Participation by senior management in security policy formulation will enforce a commitment to security programs.

A Security Policy Board should be established, chaired by a member of the Office of Security, with senior executives from Headquarters divisions, field offices, and other mission areas appointed by the Director. The Department of Justice Security Officer, or a designee, should also be a member of the Board.

I. The Office of Security Should Develop A Professional Security Staff Through Enhanced Selection, Retention, And Training Programs

Failure to designate security as a core function has led to a demoralized, poorly trained group of Special Agents and support personnel, expected to fulfill security responsibilities for which they have little or no expertise. Security has taken a backseat to operational missions, fostering the belief that one can advance within the Bureau only through success in investigative work. Efforts to change this perception will be unsuccessful unless senior management designates security as a critical function and professionalizes the Security Officer program.

The FBI has over 160 primary and alternate Security Officers in Headquarters and field offices, many of whom have been assigned security functions as collateral duties.

Eighty-five percent of those officers have less than five years security experience. Security duties are often secondary to investigative responsibilities, and agents tend to spend as little time as possible fulfilling those duties. Security Officer performance reviews are usually not based on security duties, but on investigations. Security Officers are usually eager to return to investigative work, leading to high turn-over. Assignment to the security program at Headquarters or appointment as a field Security Officer is not career enhancing. The most common complaint Security Officers voiced to Commission staff is that their function is not respected within the Bureau: they are sometimes seen as "poor performers" or as "retired in place." The stature of Security Officers is also weakened by the fact that they sometime report to field supervisors who themselves do not support Bureau security programs.

Unlike other federal agencies, the FBI does not have a career track for security specialists. This has hindered efforts to develop and retain security professionals. The Bureau has no program for recruiting employees with the experience, education, and skills required of professional Security Officers. Job descriptions and performance plans for the position do not exist. A security career program would allow for advancement and career development, contribute significantly to the professionalization of the security staff, and ensure that security skills that take years to develop are not lost through attrition when Special Agents return to criminal investigations.

The Commission recommends that the FBI establish career tracks for Security Officers and technical support staff. This is the norm at other agencies, which devote significant resources and time to developing professional staffs. The CIA, for instance, has established six career security tracks and fosters professional, career development through training and rotation of assignments. The CIA Office of Security assigns Area Security Officers (ASOs) to components for two-year rotations; they are responsible for physical security, background investigations and security clearances, and security incident reporting. The Office also assigns Information Systems Security Managers (ISSMs) to interpret and enforce information system policy and to supervise forensic programs, network computer security, and information security incident responses. Although the ASOs and ISSMs report

directly to the Office of Security, they are supervised day-to-day by mangers in the components to which they have been assigned.[35]

With the assistance of the Personnel Management Branch of the Administrative Services Division, the FBI's Office of Security should formulate career paths, defined by function and grade, that enhance career skills through training and rotation through offices and disciplines.[36] Qualifications should be established for levels within career tracks, and timelines should be set for obtaining specific skills and demonstrating accomplishments. Performance appraisals should be evaluated against specialized, documented standards.

The Office of Security must identify the training needs of its security professionals, who should broaden their experience by rotating assignments at Headquarters and in the field. Training must be mandatory and continuous throughout security careers. The FBI should also consider training programs leading to certification in security disciplines to enhance skills and undergird career paths. In contrast to the limited training the FBI gives its Security Officers, other agencies dedicate tremendous resources to training security personnel. The CIA, for instance, has a comprehensive training program for career, security professionals. Newly hired security personnel, working with mentors, receive six to eight

---

[35] NSA has developed a two-track career program for security professionals: Security Officers are responsible for counterintelligence and for protecting facilities, personnel, and information; Security Specialists are responsible for day-to-day operations. Career tracks are designed around three occupational specialities. Security Officers rotate through disciplines and offices and report directly to the Office of Security. A Security Career Panel manages professional certifications. NSA has created within the Office of Security a Technical Specialist program for polygraphy, counterintelligence, and security systems, with mentoring programs that enable security professionals to remain in technical fields without sacrificing career opportunities.

[36] For instance, the Commission recommends that the Bureau follow other Intelligence Community agencies in creating specialized career track positions for information systems security professionals, similar to the position of Information System Security Manager at the CIA. An internal review recently recommended that the FBI establish full-time Information Technology Security Specialists to assume duties now assigned to Computer Systems Security Officers (CSSOs), such as ensuring that components adhere to INFOSEC programs. These new positions eliminate conflicts that arise when computer specialists, who install hardware and develop software, assume the CSSO duty of ensuring that computer systems comply with information security policy.

months training in investigations, polygraphy, adjudications, and other security matters. During their careers, security personnel receive additional training. At NSA, security professionals receive three months initial training in signals intelligence, security systems, counterintelligence, and other subjects, reinforced by on-the-job mentoring programs, periodic refresher courses, and specialized training.

If career tracks are not adopted, the FBI should establish other measures to professionalize the Security Officer position. At a minimum, security duties should be full time, not collateral. Performance plans must be established for security disciplines, and performance appraisals must be evaluated based on security duties. Security Officer selection criteria should be formalized and subject to approval by the Office of Security. In-service training programs must be developed to teach skills that remain relevant in changing environments.

Unlike other agencies in the Intelligence Community, the FBI depends on Special Agents, that is, on law enforcement personnel, to serve as security officers. Should the FBI conclude that its security needs are best addressed by Special Agents serving as Security Officers, management must make these positions more attractive. Many Security Officers have recommended that, if the position were established at the GS-14 level, it would be more competitive and attract more qualified agents. Some have suggested that service as a Security Officer should be a stepping stone to Supervisory Special Agent status or other management positions. However the Bureau structures the position, the security program

will fail unless Special Agents acting as Security Officers are key elements in a core function.

I. The Office of Security Should Implement Comprehensive Security Education And Awareness Programs

Bureau programs for employee security education and awareness are in great need of improvement. While other federal agencies have implemented sophisticated security training programs, FBI employees generally receive insufficient training. Funds have not been budgeted for security awareness and education, even though Executive Orders and Director of Central Intelligence Directives require periodic training. Security education receives little support from senior management; it is often targeted for budget cuts and is a part-time responsibility of only one or two persons in the Security Countermeasures Branch.

Security is the topic of a one to two hour program during new agent training at the Academy that is not covered on the final examination. Security information for the workforce is presented in a small handbook, bland in presentation and insufficiently broad. Retraining programs do not exist.

Almost without exception, security personnel throughout the Intelligence Community concur that aggressive education and awareness initiatives are the most important components of security programs. They provide a significant return on investment because preventing security compromises is more cost effective than repairing the damage they cause. With strong management support, education and awareness efforts at other agencies instill security sensitivity in the workforce.

CIA, NSA, and State have developed security awareness programs with Power Point presentations, web sites, brochures, and other features to ensure that security awareness is attractively presented and reinforced by constant reminder. At the CIA, for instance, employees are informed of security matters through agency-wide bulletins and message boards and are notified of mandatory, security awareness training by e-mail. Employees who do not participate in this training may have their security badges revoked and computer

accounts cancelled. A six-hour security orientation for new employees and contractors stresses security awareness, including proper handling of classified information, need-to-know restrictions, computer security, and recent espionage cases. A mandatory refresher designed for those who have not been in a classified environment for two years reminds employees of proper procedures for handling classified information. An information security course is mandatory for all personnel with access to CIA information systems, and a mandatory training program covers counterintelligence and security responsibilities, highlighting current threats and reminding employees of available resources.[37]

The FBI's Office of Security must adopt effective, mandatory security education and awareness programs for all employees. Security should become an integral part of the new-agent curriculum at the FBI Academy, and it should be included in the final examination. Employees should be given thorough security briefings upon arrival at their first duty station and mandatory annual refresher training thereafter. Security education and awareness should be promulgated through a variety of media, such as a web site, newsletters, computer-based programs, and briefings tailored to specific audiences. The Office should invest in state-of-the-art training methodology and maintain a database of training resources available in-house and externally.

---

[37] State has adopted equally strong security training. After learning that many newly hired employees had not attended orientation or had skipped the security portion, State's Security Office ordered that employees not receive building passes unless they had attended the security briefing. In 2000, State implemented security awareness and training programs after the Secretary, in response to a missing laptop, directed that all employees and contractors authorized to handle classified information be briefed on protecting sensitive information. State has developed an information security web-site, and employees worldwide can consult security professionals by e-mail. In the near future, State will implement a mandatory, annual computer-based security awareness program.

V. The Office Of Security Should Develop A Centralized Security Violation Reporting Program

Unlike other intelligence agencies, the FBI does not have a viable program for reporting security incidents to Headquarters. There is no Bureau-wide definition of what constitutes a security violation, and there is no standard process for investigating potential security incidents. Currently, security incidents and violations need not be documented. Typically, Security Officers report violations to local Special Agents-in-Charge, resulting in disparate responses throughout the field and in Headquarters. Egregious violations are sometimes referred to the FBI's Office of Professional Responsibility; less severe violations are often overlooked.

Department of Justice regulations require that the Bureau report to the Department Security Officer (DSO) information about employee eligibility for access to classified information and the possible loss or compromise of that information. Department regulations also require that the FBI Security Program Manager (SPM) report to the DSO when employees knowingly or willfully violate security policies covering national security information. Upon receiving a report of a security violation, the SPM must initiate an inquiry, the results of which, if the violation is confirmed, are to be forwarded to the Department's DSO for action.

With the exception of violations involving Legal Attachés in U.S. embassies, few FBI security violations are reported to security, in spite of the fact that the FBI's Manual of Investigative Operations and Guidelines provides that employees who know about the loss or possible compromise of classified information "shall immediately report the circumstances" to the Headquarters SPM and the field Security Officer, who must initiate an investigation and a damage assessment and forward the results to Headquarters.[38]

[38] At FBI offices overseas, Marine security guards ensure that classified information is properly stored. Reports of security violations are made to State Department Regional Security Officers, who forward the results of investigations to State for adjudication. The adjudicated report is forwarded to DOJ for resolution. Although security violations have resulted in the removal of Legal Attachés, the FBI does not maintain permanent records of these violations.

Unfortunately, reporting to security is inconsistent. Security Officers also report that minor violations have no consequences. Few are even aware that an FBI manual mandates discipline for security lapses: losing or mishandling classified or sensitive information can result in sanctions ranging from oral reprimand to termination of employment.

The FBI does not track employee security violations or report them to a security clearance adjudication authority. As a result, the Office of Security is unable to monitor violations or search for patterns. Thus, the Counterintelligence Division, security clearance adjudicators, and the SPM do not have a clear picture of the state of security at Headquarters or in the field; employees who habitually violate security regulations can still receive favorable assignments and promotions and pass reinvestigations for security clearances.

Other federal agencies have implemented rigorous programs for reporting, investigating, and disciplining security violators. Those programs are reinforced by centralized automated tracking of security violations and by robust security education and awareness training to advise employees of their security responsibilities and the consequences of noncompliance. Many programs encourage collaboration between human resources staff and security personnel. Most important, security violation programs at other agencies receive the support of senior management.

As a result of several embarrassing security incidents, notably, a missing laptop containing classified information, missing classified information from the Secretary's office, and discovery of a listening device planted in a conference room, the Department of State re-structured its security program in 2000 to include mandatory reporting of violations and increased penalties.[39] Security Officers are now required to report security incidents to Headquarters for adjudication and inclusion in security files so that the human resources unit has complete personnel records. State has adopted a point system for security incidents,

[39] Former Secretary Albright set the stage for change in an address to Foreign Service officers: "I don't care how skilled you are as a diplomat, how brilliant you may be at meetings, or how creative you are as an administrator; if you are not a professional about security, you are a failure."

judged from the perspective of a "three year window" from the date of the first security violation. Successive infractions within that window have increasingly serious consequences until, finally, they are referred for disciplinary action and review of security clearances.[40]

The FBI should implement a security violation program that includes, at a minimum, mandatory reporting by Security Officers of all incidents to the Office of Security and uniform procedures for handling and documenting investigations and security adjudications. Security Officers should record security incidents in a report that includes a summary of the investigation, findings as to persons responsible, mitigating circumstances, a damage assessment, a determination as to whether the violation was deliberate or part of a pattern, and a recommendation for remedial actions including possible suspension or revocation of clearances. Final actions should be documented and reports retained on a secure database. Employees should receive training that explains the violation program and the consequences of noncompliance.

The Bureau should strengthen disciplinary procedures for security violations. The FBI should define minor incidents and serious violations and encourage self-reporting by applying lesser sanctions to minor violations. Those who engage in multiple or patterns of

---

[40] State maintains files on security incidents until the personnel involved leave the Department. Information in the files is provided to Human Resources for consideration in assignments, promotions, and other personnel actions. Employees with a history of security incidents may have assignments suspended or denied.

The CIA uses an automated program to process and track security incidents. Security Officers investigate security incidents and file reports that include a finding as to the persons responsible for the violation, the risk of compromise, and determinations as to whether the violation was deliberate and part of a pattern. The report can recommend remedial action. Because the CIA encourages individuals to self-report, minor violations are not always placed in the automated database, and violations are placed in personnel files only if administrative or disciplinary action has been taken. Performance appraisals include only egregious security violations. Administrative actions can range from oral reprimand to dismissal. After two years without a security violation, the record of infraction is deleted from the database.

security violations should be subject to additional discipline, including, at a minimum, mandatory attendance at security courses.

The Office should track security violations to determine whether an employee's access to sensitive information poses an unacceptable risk. The database should include information on all employees and contractors, including background information, initial and re-investigation information, results of polygraph examinations, financial disclosures, foreign contacts and travel, and other matters.

The Office of Security and the Office of Professional Responsibility should develop a process for delineating responsibilities and coordinating investigations of security violations. OPR should give the Office its findings so that they can be entered on a centralized database.

VI. The Office of Security Should Audit Security Programs

Primary responsibility for inspecting security programs and systems at Headquarters and in the field now rests with the Office of Inspections in the Inspection Division. The Department of Justice also conducts periodic security compliance reviews of FBI field offices. The Office of Security is given the results of these inspections, as they pertain to security, but does not participate in the inspections.

The Inspection Division conducts inspections, rating the effectiveness of programs and management, and audits, measuring compliance with specific goals. On-site inspection teams are augmented, as needed, by subject-matter experts from Headquarters and the field. If an inspection team is unable to secure an Inspector with security or counterintelligence experience, the security component of the inspection is often cursory, consisting of pro forma use of audit checklists. Security Officers told Commission staff that most Inspectors with whom they dealt during audits had no background in security and did not "have a clue" as to what they were auditing.

Security programs are not given high priority during inspections, which evaluate compliance with goals set in the Annual Field Office Report each office develops. Security is not a component of the report. As a result, security inspections are usually completed in a day or less and are often scheduled during the last week or day of the review. Special Agents-in-Charge (SACs) are not evaluated on the basis of compliance with security programs. Field Security Officers and the SACs to whom they report do not respect security inspections because there are no significant consequences for noncompliance. Some Security Officers assert that SACs have requested that they accept criticisms of security issues during these inspections, in lieu of the office receiving negative findings on critical programs included in the Annual Field Office Report.

The Office of Security should periodically review security programs and systems in Headquarters and the field, independent of reviews conducted by the Inspection Division. Teams of security specialists from the Office, as well as security experts from field offices, should initially focus on offices with documented security concerns or high security risks. The on-site review should be comprehensive. The Office should be given authority to rate security programs and their management, and the rating should be a critical element in SAC performance appraisals. Office of Security personnel should also be detailed to the Inspection Division as needed to ensure meaningful audits of security programs.

CONCLUSION

Because Bureau security functions are dispersed across eight Headquarters divisions and many field offices, no one has traditionally been responsible for developing, implementing, and enforcing consistent security policy and practices.

Because the Bureau has failed to designate security as a core function, management continues to slight the security program in favor of operational functions and to deny security programs the resources needed to succeed.

The key to effective security programs within the FBI is an adequately funded Office of Security, reporting to the Director and responsible for security policy, implementation,

and training.

CONCLUSION

[T]here is no way that I can justify what I have done. It's criminal and deceitful and wrong and sinful.

– Robert Hanssen

Robert Hanssen's treachery is heinous, but, when compared with natural events, it is like a five-hundred year flood: an incredible assault that should not be taken as the norm in developing disaster preparedness plans. Of more importance is the history of domestic espionage outlined in the Introduction to this Report, of which Hanssen's crimes are an instance.

History shows that espionage and security breaches are inevitable. Nonetheless, we can end our review on a guarded note of comfort: It is possible to react rationally to the inevitable by implementing steps to deter espionage, reduce the time between defection and its detection, and minimize the harm traitors can do.

We hope that our efforts will contribute to this goal.

GLOSSARY

Glossary of Acronyms

Acronym	Term
ACS	Automated Case Support (system)
AD	Assistant Director
ADPT	Automated Data Processing and Telecommunication
ADPTSO	Automated Data Processing and Telecommunication Security Officer
AES	Advanced Encryption Standard
AFGE	American Federation of Government Employees
AFOR	Annual Field Office Report
AFOSI	Air Force Office of Special Investigations
AFSA	American Foreign Service Association
AISC	Agency Information Course Security
AITU	Audio/Intercept Technology Unit
AIU	Analytical Integration Unit
ASAC	Assistant Special Agent-In-Charge
ASD	Administrative Services Division
ASO	Area Security Officer
ATM	Asynchronous Transfer Mode
BI	Background Investigation
BIGOT	Controls on Information (The acronym originated in WWII)
BICS	Background Investigation Contract Service
BPMS	Bureau Personnel Management System
C&A	Certification and Accreditation
CA	Computer Associates
CAA	Controlled Access Area
CARLABFAD	Character, Associates, Responsibility, Loyalty, Ability, Bias and prejudice, Financial responsibility, Alcohol use, and Drug use
CCA	Codename/Codeword Application
CCB	Configuration Control Board
CCF	Central Clearance Facility
CFR	Code of Federal Regulations
CEAU	Cryptographic and Electronic Analysis Unit
CI	Counter Intelligence
CIA	Central Intelligence Agency
CIPA	Classified Information Procedures Act
CIRT	Computer Incident Response Team
CJIS	Criminal Justice Information Services
CLEA	Criminal Law Enforcement Application
CM	Configuration Management
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOP	Concept of Operations

Acronym	Term
COOP	Continuity of Operations Plan
COR	Central Office of Record
COTS	Commercial Off the Shelf
CQR	Career Qualification Review
CRC	Cyclic Redundancy Check
CS	Computer Specialist
CSSO	Computer System Security Officer
CT	Counter Terrorism
CTD	Counter Terrorism Division
DAAS	Double Agent Analysis System
DAD	Deputy Assistant Director
DBMS	Database Management System
DCI	Director Of Central Intelligence
DCID	Director Of Central Intelligence Directive
DEA	Drug Enforcement Administration
DIA	Defense Intelligence Agency
DICAST	Defense and Intelligence Community Accreditation Support Team
DIR	Daily Intelligence Review
DIS	Defense Intelligence Service
DISA	Defense Intelligence Systems Agency
DISCO	Defense Industrial Security Clearance Office
DM	Data Mining
DOD	Department of Defense
DOJ	Department of Justice
DS	Data Signal (level)
DSO	Department Security Officer
DVD	Data Video Disk
EAP	Employee Assistance Program
EC	Electronic Communication
ECF	Electronic Case File
EKMS	Electronic Key Management System
ELSUR	Electronic Surveillance
EO	Executive Order
ERF	Engineering Research Facility
ETA	Education Training and Awareness
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FCI	Foreign Counterintelligence
FINCEN	Financial Crimes Enforcement Network, Dept of Treasury
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FO	Field Office
FOIA	Freedom of Information Act
FOIPA	Freedom of Information and Privacy Act

Acronym	Term
GSR	Galvanic Skin Response
HERU	Historical Executive Review Unit
HIT	Hostile Intelligence Threat
HCS	HUMINT Control System
HQ	Headquarters
HUMINT	Human Intelligence
IA	Information Assurance
IAU	Intelligence Analysis Unit
IBM	International Business Machines
IC	Intelligence Community
ICM	Investigative Case Management (system)
ICO	Intelligence Community Officer
ID	Identification
IDCS	Integrated Data Communication System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IG	Inspector General
IIIA	Integrated Intelligence Information Application
IIISNET	Investigative Intelligence System Network
IMA	Information Management Assistant
INFOSEC	Information Systems Security
IOB	Intelligence Oversight Board
IOS	Intelligence Operations Specialist
IP	Internet Protocol
IPC	Interface Presentation Component
IPS	Intrusion Protection System
IPX	Internet Packet Exchange
IRD	Information Resources Division
IS	Information System
ISD	Investigative Service Division
ISO	International Standards Organization
ISOO	Intelligence Security Overview Office
ISSAM	Information Systems Security Assessment Methodology
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSU	Information Systems Security Unit
ISU	Industrial Security Unit
IT	Information Technology
ITS	Information Technology System
ITSS	Information Technology Security Specialist
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
KG	Key Generator
KSA	Knowledge, Skill, and Ability
LAC	Local Agency Checks

Acronym	Term
LAN	Local Area Network
LD	Laboratory Division
LEGAT	Legal Attaché Office
LEO	Law Enforcement Online
LHM	Letterhead Memorandum
LOU	Limited Official Use
LPAR	Logical Partition
LSU	Language Service Unit
MAOP	Manual of Administrative Operations and Procedures
MBI	Minimum Background Investigation
MIOG	Manual Of Investigative Operations and Guidelines
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NACIC	National Counter Intelligence Center
NACLC	National Agency Check with Law and Credit
NARA	National Archives and Records Administration
NIACAP	National Information Assurance Certification and Accreditation Process
NIAP	National Information Assurance Partnership
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NOCONTRACT	Not Releasable to Contractors or Consultants
NOFORN	Not Releasable to Foreign Nationals
NRO	National Reconnaissance Office
NSA	National Security Agency
NSD	National Security Division
NSI	National Security Information
NSLU	National Security Law Unit
NSPR	No Significant Physical Response
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSM	National Security Telecommunications and Information Systems Security Manual
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NSTL	National Security Threat List
NT	New Technology
OADR	Originating Agency's Determination Required
OCA	Original Classification Authority
OGA	Other Government Agencies
OIPR	Office of Intelligence Policy and Review
OMB	Office of Management and Budget

Acronym	Term
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
OPSEC	Operations Security
ORCON	Dissemination & Extraction of Information Controlled by Originator
OSI	Office of Special Investigations
OSTO	Operational Support Tracking Office
PAR	Performance Appraisal Review
PASSAU	Pay Administration and Support Staffing Unit
PC	Personal Computer
PDD	Presidential Decision Directives
PDS	Protected Distribution System
PENTTBOM	Investigation of the September 11, 2001 Terrorist Attacks on the Pentagon and the Twin Towers
PIN	Personal Identification Number
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PRI	Periodic Reinvestigation
PROPIN	Caution - Proprietary Information Involved
PSI	Personnel Security Interview
PSS	Personnel Security Specialist
PSU	Personnel Security Unit
QCMSU	Quality Assurance, Configuration Management, Methods and Standards Unit
RA	Resident Agent
RSO	Regional Security Officer
SA	Special Agent
SAC	Special Agent-In-Charge
SACS	Security Access Control System
SAPS	Special Access Programs
SARS	System Account Request System
SBI	Special Background Investigation
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCMB	Security Countermeasures Branch
SCMPM	Security Countermeasures Program Manager
SCMS	Security Countermeasures Section
SDIS	Secure Data Information System
SES	Senior Executive Service
SFR	Special File Room
SI	Special Investigator
SIMP	Security Incident Management Program
SIOC	Strategic Information and Operations Center
SIPRNet	Secret Internet Protocol Router Network

Acronym	Term
SO	Security Officer
SOP	Security Operating Procedure
SPM	Security Programs Manager
SPOM	Security Programs Operating Manual
SSA	Supervisory Special Agent
SSAA	System Security Authorization Agreement
SSBI	Single-Scope Background Investigation
SSRP	Sensitive Source Reporting Program
STU	Secure Telephone Unit
TCP	Transmission Control Protocol
TDM	Time Division Multiplexers
TNC	Telecommunications Network Component
TS	Top Secret
TSCL	Top Secret Contract Linguists
TSCM	Technical Security and Countermeasures
TTAP	Technical Threat Analysis Program
UAC	User Application Component
UNI	Universal Index
USG	United States Government
WNINTEL	Warning Notice - Intelligence Sources and Methods Involved
XML	eXtensible Markup Language

COMMISSION CHARTER

CHARTER
COMMISSION FOR THE REVIEW OF
FBI SECURITY PROGRAMS

I. OFFICIAL DESIGNATION

This Charter relates to the Commission for the Review of FBI Security Programs (Commission).

II. OBJECTIVES AND SCOPE OF ACTIVITY

The objective of the Commission is to review and analyze the adequacy of the Federal Bureau of Investigation security policies and procedures and to make recommendations to the Attorney General on ways to improve their effectiveness.

III. DURATION

The Commission will exist until March 31, 2002, but is subject to renewal.

IV. REPORTING

The Advisory Group shall report to the Attorney General or the Attorney General's designee.

V. SUPPORT SERVICES

The Department of Justice will provide all necessary support services for the Advisory Group.

VI. DUTIES

The duties of the Commission are advisory and are to carry out the objectives listed in the section of this Charter entitled OBJECTIVES AND SCOPE OF ACTIVITY. The Commission may also appoint ad hoc committees, with the Department of Justice approval, to assist it in carrying out its duties. Ad hoc committees will research and prepare recommendations to the Commission.

VII. OPERATING COSTS

The estimated annual operating cost of the Commission, including working groups and ad hoc committees, is expected to be approximately $1.2 million. The cost includes 1.0 full

time equivalent government personnel to support activities of the Commission as well as the travel expenses for the meeting attendees.

VIII. MEETINGS

The Commission will meet as often as necessary at the call of the Chairperson. The Designated Federal Official approves the call of the Commission meetings and agenda in advance and is present at all meetings. The Attorney General has determined that Commission meetings will not be open. Meetings will be conducted and records of the proceedings kept as required by the Federal Advisory Committee Act. Ad hoc committees will meet, as required and agreed to by the Chair of the Commission and the Designated Federal Office, to research and prepare recommendations to the Commission.

I. ESTABLISHING AUTHORITY

This Commission is established under the authority of the Attorney General.

J. DELEGATION OF AUTHORITY TO APPOINT MEMBERS

The Attorney General or the Attorney General's designee has the authority to approve members to the Commission.

K. TERMINATION

This charter expires on March 31, 2002, but is subject to renewal.

L. DATE OF CHARTER

The date of this charter is August 17, 2001.

John Ashcroft
Attorney General
Department of Justice

THE COMMISSION FOR THE REVIEW

OF

FBI SECURITY PROGRAMS

WILLIAM H. WEBSTER, the Commission's Chair, served as Director of Central Intelligence from 1987 to 1991. He also served as U.S. Attorney for the Eastern District of Missouri from 1960 to 1961 and, in 1970, was named a U.S. District Court Judge for that District. In 1973, Judge Webster was elevated to the U.S. Court of Appeals for the Eighth Circuit, a position he held until1978 when he became Director of the Federal Bureau of Investigation, a position he held until 1987. Judge Webster is a graduate of the Washington University School of Law, and he served as a lieutenant in the U.S. Navy in World War II and in the Korean War. Judge Webster is currently a partner in the law firm, Milbank, Tweed, Hadley & McCloy.

CLIFFORD L. ALEXANDER, Jr. has served as Chairman of the U.S. Equal Employment Opportunity Commission and as a Special Consultant on Civil Rights to President Lyndon Johnson. In 1977, he became Secretary of the Army. Secretary Alexander has also served as Chairman of the Board of the Panama Canal Company and as a member of the Board of Overseers of Harvard University. He is a graduate of the Yale Law School and is currently President of Alexander & Associates.

GRIFFIN B. BELL served in the U.S. Army from 1941 to 1946, attaining the rank of Major. In 1953, he joined the law firm, King & Spaulding, where he became managing partner. In 1961, President Kennedy appointed him to the U.S. Court of Appeals for the Fifth Circuit, on which he served until 1976. Judge Bell became the Attorney General of the United States during the Carter Administration in 1977 and served until 1979 when he returned to King & Spaulding and became Chairman of its Policy Committee. He has also served as President of the American College of Trial Lawyers and as a Director of the American Enterprise Institute. Judge Bell is a graduate of the Mercer University Law School.

WILLIAM S. COHEN began a career of public service in 1973 as a U.S. Congressman from the State of Maine, which he also represented as a U.S. Senator from 1979 to 1996. After leaving the Senate, he accepted President Clinton's request in 1996 to lead the Department of Defense and became the first elected member of a political party to serve in the cabinet of another party in modern American history. Secretary Cohen was responsible for reversing a decade-and-a-half decline in the defense budget and the defense procurement budget, which he increased by nearly 50%, the largest military pay raise in a generation, and adoption of electronic commerce and other best business practices in the Defense Department, the largest business enterprise in the world. Secretary Cohen is currently Chairman and Chief Executive Officer of the Cohen Group.

ROBERT B. FISKE, Jr. was U.S. Attorney for the Southern District of New York from 1976 to 1980 and chairman of the Attorney General's Advisory Committee of U.S. Attorneys. In 1994, Mr. Fiske served as an Independent Counsel in the Whitewater

investigation and recently served as chairman of a New York State Judicial Commission on Drugs and the Courts. He is past President of the American College of Trial Lawyers and of the Federal Bar Council and currently practices law with Davis Polk & Wardwell. Mr. Fiske is a graduate of the University of Michigan Law School.

THOMAS S. FOLEY represented a Congressional district in the State of Washington for thirty years. He served as majority leader of the U.S. House of Representatives from 1987 until his election as speaker in 1989. After his retirement from the House, Ambassador Foley practiced law until his appointment as U.S. Ambassador to Japan. He is currently chairman of the Trilateral Commission, a member of the Council on Foreign Relations, and a partner in the law firm, Akin, Gump, Strauss, Hauer & Feld. Ambassador Foley is a graduate of the University of Washington's School of Law.

CARLA A. HILLS has served as Assistant Attorney General for the Civil Division of the U.S. Department of Justice and as Secretary of the U.S. Department of Housing & Urban Development. Ambassador Hills was Chairman of the Urban Institute from 1983 to 1988 when she became U.S. Trade Representative, the nation's chief trade negotiator. She has served on several presidential and congressional commissions and is a graduate of the Yale Law School. Ambassador Hills is currently Chairman and Chief Executive Officer of Hills & Company.