U.S. Department of Justice

A Review of FBI Security Programs

Commission for Review of FBI Security Programs
March 2002

William S. Hein & Co., Inc.
Buffalo, New York
2002

Library of Congress Cataloging-in-Publication Data

A review of FBI security programs / Commission for Review of FBI Security Programs.
p. cm.
"U.S. Department of Justice".
Includes index.
ISBN 1-57588-732-0 (alk. paper)
1. United States. Federal Bureau of Investigation. 2. Internal security--United States. 3. National security--United States. 4. Intelligence service--United States. I. United States. Commission for Review of FBI Security Programs.

HV8144.F43 R48 2002
327.1273--dc21

2002032860

Printed in the United States of America

The quality of this reprint is equivalent
to the quality of the original work.

This paper meets the requirements of
ANSI/NISO Z39.48-1992 (Permanence of Paper).

William S. Hein & Co., Inc.
Buffalo, New York
2002

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

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.