UNCLASSIFIED EXECUTIVE SUMMARY

A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen

Office of the Inspector General
August 2003

UNCLASSIFIED EXECUTIVE SUMMARY

I. Introduction

In this report, the Office of the Inspector General (OIG) of the Department of Justice (DOJ) examines the performance of the Federal Bureau of Investigation (FBI) in deterring, detecting, and investigating the espionage of Robert Philip Hanssen, a former FBI Supervisory Special Agent. Hanssen's espionage began in November 1979 – three years after he joined the FBI – and continued intermittently until his arrest in February 2001, just two months before his mandatory retirement date. In addition to its management responsibility to detect espionage among its employees, the FBI is the lead agency for detecting and investigating espionage committed in the United States.

Hanssen became an FBI agent in 1976. During his 25-year FBI career, he principally served in Soviet counterintelligence assignments in New York City and Washington, D.C. In the 1980s and 1990s, Hanssen held positions at FBI Headquarters and the State Department that gave him access to a broad range of highly sensitive counterintelligence and military information. On February 18, 2001, after a three-month investigation of Hanssen, he was arrested and charged with committing espionage on behalf of the KGB (Komitet Gosudarstvennoy Bezopasnosti, the intelligence service of the former Soviet Union) and its successors. On July 6, 2001, Hanssen pled guilty to espionage charges pursuant to a plea agreement in which he agreed to cooperate with the U.S. government and submit to debriefings. On May 10, 2002, Hanssen was sentenced to life imprisonment.

Hanssen's espionage spanned three separate time periods: 1979-81, 1985-91, and 1999-2001. Over more than 20 years, Hanssen compromised some of this nation's most important counterintelligence and military secrets, including the identities of dozens of human sources, at least three of whom were executed. Hanssen gave the KGB thousands of pages of highly classified documents and dozens of computer disks detailing U.S. strategies in the event of nuclear war, major developments in military weapons technologies, information on active espionage cases, and many other aspects of the U.S. Intelligence Community's Soviet counterintelligence program.

Shortly after Hanssen's arrest, the Senate Select Committee on Intelligence (SSCI) and the Attorney General asked the OIG to review the

FBI's performance in connection with the Hanssen case. This report details the results of the OIG's investigation.

II. Summary of the OIG Investigation and Structure of the Report

The OIG assembled a team of three Special Investigative Counsel, a project director, three OIG Special Agents, two analysts, and a consultant to conduct this review. The team reported directly to the Inspector General.

The team obtained, reviewed, and analyzed more than 368,000 pages of material from the FBI, the Central Intelligence Agency (CIA), the Justice Department, the National Security Agency (NSA), and the State Department. The team also conducted more than 200 interviews in 12 states and the District of Columbia. We interviewed Hanssen's former colleagues and supervisors at the FBI and State Department, as well as family, friends, and acquaintances who knew Hanssen throughout his life. We interviewed much of the operational hierarchy of the FBI's Intelligence/National Security Division (NSD) during the 1979 to 2001 period. In addition, we interviewed CIA and Justice Department personnel who had substantial involvement with the FBI regarding "penetration" matters – that is, investigating whether a foreign intelligence service has infiltrated or recruited agents within U.S. organizations. The team also interviewed Hanssen extensively.

Our full 674-page report is classified at the Top Secret/Codeword level because it contains extremely sensitive classified information regarding sources involved in the Hanssen case and FBI counterintelligence activities. We also produced a 383-page report, classified at the Secret level, which does not contain the detailed information on the sensitive sources that is included in the Top Secret/Codeword version. In addition, we produced this 31-page unclassified executive summary to provide a public summary of the main findings in the more extensive classified reports. We previously provided a copy of all three reports to the FBI for its comments on their factual accuracy and classification, and we made changes where appropriate.

In our reports, we divide Hanssen's FBI career into three phases that roughly correspond with the three periods of his espionage and with key FBI penetration-related efforts. One chapter is devoted to each phase, and within each chapter there are three parts: Hanssen's career, Hanssen's espionage, and the FBI's penetration efforts.

Chapter One covers the time period between 1976, when Hanssen joined the FBI, and 1985, when he completed his first tour in the Soviet Analytical Unit at FBI Headquarters. This chapter also includes background information

concerning Hanssen's childhood, education, and employment prior to becoming an FBI agent. Hanssen's first espionage – conducted on behalf of the GRU (Glavnoye Razvedyvatelnoye Upravleniye, the Soviet Union's military intelligence arm) – took place between 1979 and 1981. The FBI's investigation of Soviet-related penetration leads during this time period was minimal.

Chapter Two covers the time period between 1985 – when Hanssen became the supervisor of an FBI technical surveillance squad in New York and volunteered to the KGB – and 1992. Hanssen's FBI career progressed normally during these years, which also constituted his most active period of espionage. With respect to the penetration issue, both the CIA and the FBI suffered catastrophic and unprecedented losses of Soviet intelligence assets in 1985 and 1986, which suggested that a mole was at work in the Intelligence Community. The FBI conducted several analytical efforts – including a major joint project with the CIA – that were unsuccessful at determining the cause of these compromises.

Chapter Three begins in 1992 and ends with Hanssen's arrest in February 2001. In January 1992, Hanssen became the Chief of the National Security Threat List Unit at FBI Headquarters, the highest ranking position he held at the FBI. Hanssen's failings as a supervisor and his inability to properly handle classified information led the FBI to remove Hanssen from his Unit Chief position, and he was subsequently detailed to the State Department as the FBI liaison to the Office of Foreign Missions (OFM). He served for six years in the OFM, until shortly before his arrest. With respect to espionage, Hanssen made a clumsy and aborted approach to the GRU in 1993 and then successfully re-volunteered to the KGB in 1999. Hanssen's espionage – which during this period relied heavily on his improper use of the FBI's Automated Case Support (ACS) computer system – continued until his arrest in February 2001.

The FBI's penetration-related investigations increased dramatically in the 1992 to 2001 period. The FBI substantially increased the resources it devoted to the penetration issue and successfully identified and prosecuted several individuals who spied for Russia, including CIA officer Aldrich Ames. The most significant espionage investigation that the FBI pursued after the 1994 arrest of Ames, however, was the search for the penetration of the U.S. Intelligence Community who was later determined to be Hanssen. The FBI believed early on that the mole worked at the CIA and subsequently pursued a lengthy investigation of a CIA employee. We now know that from the outset the FBI was focused on the wrong suspect at the wrong agency.

Chapter Four of our report examines deficiencies in the FBI's internal security that were apparent during our investigation of the Hanssen matter. This chapter discusses how flaws and deficiencies in the FBI's programs and policies concerning background reinvestigations, financial disclosures, polygraph examinations, computer security, classified document handling, and procedures for reporting and documenting security violations made it easier for Hanssen to commit espionage and more difficult for the FBI to detect him. It also describes the changes that have been made, or not made, to the FBI's internal security program since Hanssen's arrest in 2001.

Lastly, Chapter Five summarizes our principal factual findings and sets forth our recommendations for changes in the FBI's counterintelligence and security programs.

III. Principal Findings of the OIG Investigation

In the following paragraphs, we summarize the report's principal findings concerning Hanssen's career at the FBI, his espionage, and the FBI's penetration-related efforts from 1978 to 2001.

A. Hanssen's FBI Career

During his 25 years with the FBI, Hanssen was a mediocre agent who exhibited strong technical abilities but had weak managerial and interpersonal skills. Despite his failings as a supervisor, Hanssen was on the FBI's promotional track for much of his FBI career, and he generally received average to favorable performance evaluations. While Hanssen's day-to-day behavior did not suggest that he was engaged in espionage, he continually demonstrated an unwillingness to properly handle classified information. His indiscretions and security violations were largely ignored and wholly undocumented, however, and he was allowed to remain in positions offering him broad access to highly sensitive counterintelligence information. Ultimately, Hanssen's inability to effectively interact with subordinates and colleagues derailed his FBI career.

Hanssen received minimal supervision in most of his positions, was not required to produce significant work product, and had ample time to plan and commit espionage while on duty. Hanssen also encountered few security checks at the FBI. He was never asked to submit to a polygraph examination or to complete a financial disclosure form, and he received only one background reinvestigation during his 25-year FBI career.

To his FBI co-workers, Hanssen's personal life appeared completely inconsistent with that of a spy. He was married with six children, and appeared to be a devout Catholic who attended mass every day and who was actively involved in Opus Dei, a conservative Catholic lay organization. He also espoused politically conservative and anti-Communist views. Hanssen had no alcohol, drug, or gambling problems, and did not engage in ostentatious spending.

Hanssen was an only child whose father, a lieutenant in the Chicago Police Department, emotionally abused him throughout his life. Starting from a young age, Hanssen enjoyed spy-related entertainment, especially James Bond books and movies, collected items associated with espionage, such as a Walther PPK pistol, a Leica camera, a shortwave radio, and opened a Swiss bank account. Hanssen was an average student in college, majoring in chemistry. He drifted through dental school and business school – and became a certified public accountant – before joining the Chicago Police Department. After four years, Hanssen left the police department to join the FBI in January 1976.

Hanssen appeared to be an appropriate candidate for the FBI, in light of his college education, master's degree in business administration, experience as a certified public accountant, and service in the Chicago Police Department. The FBI's initial background investigation and interviews did not indicate that Hanssen was likely to commit espionage. While Hanssen came to the FBI with serious personal insecurities, low self-esteem, and a fascination with espionage, these characteristics did not emerge during the application process.

Once in the FBI, Hanssen's personality traits set him apart from his FBI colleagues. He had poor interpersonal skills and a dour demeanor, and was an awkward and uncommunicative loner who conveyed a sense of intellectual superiority that alienated many of his co-workers. Early in his career, however, Hanssen demonstrated significant initiative and organizational skills, developing, for example, a case prioritization system that remains in use today at the FBI. He also had an interest in and aptitude for computer work that was highly unusual at the time, and a number of his early supervisors regarded him as smart, technically proficient, and analytical.

After graduation from the FBI Academy at Quantico, Virginia, Hanssen served an initial two-year tour as a Special Agent in Gary, Indiana. While Hanssen sought out counterintelligence assignments in Gary, there was little such work available. At the end of his tour, Hanssen requested a transfer to the FBI's New York Office. Within six months of his arrival in New York,

Hanssen arranged to be transferred from a Criminal Division squad to Soviet counterintelligence work, which remained his assignment for most of his FBI career. Hanssen quickly began exploiting weaknesses in the FBI's internal information security. While still assigned to a Criminal Division squad in the FBI's New York Office, Hanssen took advantage of the unrestricted and unmonitored access to the closed file room and spent hours reading Soviet espionage files – without any conceivable "need to know" – managing to identify some of the FBI's most significant Soviet sources in the process. Hanssen – who appeared to have little aptitude for operational work – demonstrated a strong interest in computers and in administrative assignments, and was given responsibility for managing the New York Office's counterintelligence database, a position that put him at the center of the information flow.

In the early 1980s, Hanssen served in the Budget Unit and in the Soviet Analytical Unit at FBI Headquarters – positions that provided him with broad access to sensitive information and an opportunity to use his technical and computer skills, but did not require operational work. Because the Budget Unit was responsible for preparing materials justifying the FBI's budget requests to Congress, Hanssen obtained access to sensitive information from all components of the Intelligence Division, and worked closely with the NSA and the CIA to secure joint funding for certain projects. In the Soviet Analytical Unit, Hanssen gained access to the FBI's most sensitive human assets and technical operations against the Soviet Union. He also began a noticeable pattern of mishandling classified information, primarily by disclosing the existence of Soviet sources and investigations to people with no "need to know," such as FBI employees in other divisions and personnel from other agencies. While Hanssen's tours in the Budget and Soviet Analytical Units showed that he was an intelligent, analytical agent with significant computer skills, his performance also revealed that he lacked the interpersonal skills to communicate effectively and perform supervisory duties. Nonetheless, Hanssen's career at the FBI continued to advance.

In 1985, Hanssen returned to the New York Office as the supervisor of a technical surveillance squad. Hanssen was a lackadaisical manager who did not interact effectively with his subordinates. Because the squad largely "ran itself," however, Hanssen's limited interpersonal skills did not become a significant issue. Similarly, Hanssen's mishandling of classified information was obvious to his subordinates but was not brought to the attention of his superiors.

In 1987, Hanssen returned to the Soviet Analytical Unit in FBI Headquarters as a supervisor, a position that he told the OIG he found "overwhelmingly attractive" because of the extremely broad access to sensitive information it offered. Although Hanssen received very favorable performance evaluations during his second tour in the Unit, his supervisor regarded him as the "strangest person" he had ever worked with in the FBI – a "kind of cipher who was rigid, dour, and a religious zealot." As was the case during his first tour in the Unit, Hanssen produced little work product, and his subordinates regarded him as distant and arrogant. Shortly after his return to the Unit, Hanssen committed a serious security breach by disclosing sensitive information to a Soviet defector he was debriefing. Hanssen's colleagues recognized that he could not be trusted with highly sensitive information and informally attempted to restrict his access. Although this security breach was reported to an FBI supervisor, it was not documented, and no formal action was taken against Hanssen, whose access to sensitive information remained largely unchecked.

In 1990, Hanssen became an Inspector's Aide in the Inspection Division, a position that was considered a prerequisite for advancement at the FBI. In this position, Hanssen traveled to FBI field offices to help rate their overall performance. In June 1991, Hanssen became a program manager in the Soviet Section at FBI Headquarters, where he supervised operational programs designed to counter Soviet efforts to acquire scientific and technical information. This assignment was brief and uneventful.

In January 1992, Hanssen became chief of the National Security Threat List (NSTL) Unit, a new unit at FBI Headquarters that dealt with economic espionage, theft of trade secrets and critical technologies, and nuclear proliferation. This position required significant management skills and an ability to work effectively with the FBI's field offices, and Hanssen's deficiencies in these areas quickly became apparent. Hanssen's subordinates found him disinterested in the Unit's work and were frustrated by his failure to provide guidance and direction. Rather than engage in the daily work of the Unit, Hanssen frequently sat in his office listening to foreign language tapes for hours at a time. Hanssen also had poor relations with the FBI's field offices, which complained that he rejected an inordinately high percentage of their proposals for investigations.

While in the NSTL Unit, Hanssen committed two serious and flagrant security breaches. First, he hacked into the FBI's computer system and accessed highly sensitive Soviet counterintelligence documents located on the

hard drives of his colleagues and supervisors in the National Security Division. Hanssen grew nervous about what he had done and decided to report it to FBI management in the guise of revealing a flaw in the FBI's computer security. Hanssen's ruse succeeded, and no one questioned his breach of computer security. Hanssen's second significant breach occurred when, in direct contravention of a decision made by FBI management, he disclosed to the British intelligence service information about a highly sensitive FBI investigation. At about this time, Hanssen also came under investigation by the FBI's Office of Professional Responsibility because of a physical altercation with a female FBI support employee. The investigation resulted in a letter of censure and a five-day suspension. The physical altercation, the improper disclosure to British intelligence, and Hanssen's poor performance in the NSTL Unit doomed his chances for further advancement at the Bureau.

As part of an FBI-wide program in which Headquarters personnel were reassigned to FBI field offices, Hanssen was involuntarily removed from his position as NSTL Unit Chief in April 1994 and transferred to the FBI's Washington Field Office (WFO), where he was assigned to a computer squad in a non-supervisory capacity. While not an official demotion, Hanssen was no longer on the management track for higher supervisory positions at the Bureau. Hanssen largely ignored his new assignment in the field office and soon began seeking work at FBI Headquarters. For several months, Hanssen worked on computer-related projects for senior NSD officials.

In late 1994, FBI management began considering Hanssen as a candidate to fill an FBI position in the Office of Foreign Missions (OFM) at the State Department. OFM regulates selected activities of foreign missions in the United States to protect U.S. foreign policy and national security interests, and also helps foreign missions protect their diplomats and facilities. Hanssen's FBI superiors saw the OFM liaison position as a good "out of the mainstream" job for Hanssen, a supervisory agent who had proven incapable of supervising others. Hanssen started at OFM in February 1995 and remained at the State Department for the next six years.

Hanssen's work responsibilities at OFM consumed no more than a few hours a day, and he was wholly unsupervised by either State Department or FBI personnel. The job carried no significant operational or managerial responsibilities, and once Hanssen was at OFM, FBI management largely forgot about him. No one checked on him or his work – or even ensured that he was at work. No performance evaluations concerning Hanssen were completed during the entire six years that he served at OFM. Hanssen took full

advantage of the light workload and complete lack of supervision, spending hours each day out of the office, surfing the Internet and watching movies on his personal laptop computer, and visiting friends and acquaintances.

During Hanssen's detail to the State Department, the FBI provided him with a desktop computer that was connected to the FBI's ACS computer system. The ACS system gave Hanssen access to thousands of internal FBI classified documents for which he had no "need to know." To determine whether he was under investigation by the FBI, Hanssen also frequently searched the ACS system for references to his own name and address. In addition, he successfully mined the system for information concerning the FBI's most sensitive espionage investigations. While the ACS system had audit capability, Hanssen's improper searches went undetected because the FBI did not conduct audit trail reviews absent an allegation of wrongdoing.

Hanssen continued to commit security violations while at the State Department. He improperly disclosed classified information to others – including NSA and State Department employees, close friends, and members of the press. Hanssen's most egregious security breach at OFM – an attempt to install password breaker software on his FBI computer – was discovered by the FBI's computer specialists, who documented the incident and referred it to the FBI's Security Programs Manager. Hanssen told the Security Programs Manager that he had installed the hacking program in order to connect to a color printer, however, and he suffered no negative consequences as a result of this misconduct. As with Hanssen's other security violations, nothing about the matter was recorded in either his personnel or security file.

In late 2000, after the FBI received information identifying Hanssen as a Russian mole, the FBI offered him a Senior Executive Service position at FBI Headquarters, where he could be closely monitored. Hanssen was arrested on February 18, 2001.

B. Hanssen's Espionage

Hanssen was the most damaging spy in FBI history, and he betrayed some of this nation's most important counterintelligence and military secrets, including the identities of dozens of human assets, at least three of whom were executed. Hanssen committed espionage intermittently, starting and stopping several times during his 25-year FBI career. He engaged in three discrete periods of espionage – 1979-81, 1985-91, and 1999-2001 – and unsuccessfully attempted to renew his espionage on behalf of the GRU in 1993. The reasons why Hanssen initially began committing espionage, and repeatedly returned to

it, are complex and, as we explain below, changed over time. Many of the factors that have motivated or influenced traitors in the past – such as greed, ideology, career disappointments and resentment, and drug and alcohol abuse – do not apply to Hanssen or do not fully explain his conduct.

Our review of the Hanssen case revealed that there was essentially no deterrence to espionage at the FBI during the 1979 to 2001 time period and that the FBI's personnel and information security programs presented few obstacles to Hanssen's espionage. His removal of hundreds of classified documents from the FBI – including original and numbered Top Secret documents – and improper searches of the Bureau's computer system for references to himself and to the Bureau's most sensitive espionage investigations went unnoticed. Because of lax supervision, Hanssen felt free to conduct many of his espionage-related activities while on duty, including creating encryption devices for communicating with the Russians, servicing dead drops, and counting his cash payments from the Russians. These deficiencies in deterrence, detection, and supervision played a major role in Hanssen's willingness and ability to commit espionage over a more than 20-year period.

1. First Period of Espionage: 1979 – 1981

Hanssen first began spying for the Soviets in November 1979, just eight months after he transferred to a counterintelligence squad in the FBI's New York Office. While on duty, Hanssen volunteered his services to the GRU by delivering a package to a GRU officer at a Soviet trade organization. In his correspondence with the GRU, Hanssen revealed that he was an FBI agent, but offered no other identifying information. Over the next year and a half, Hanssen conducted clandestine exchanges with the GRU, receiving cash payments totaling at least $21,000.

Hanssen's initial decision to commit espionage arose from a complex blend of factors, including low self-esteem and a desire to demonstrate intellectual superiority, a lack of conventional moral restraints, a feeling that he was above the law, a lifelong fascination with espionage and its trappings and a desire to become a "player" in that world, the financial rewards he would receive, and the lack of deterrence – a conviction that he could "get away with it." We believe that the personality flaws and background that Hanssen brought with him into the FBI likely played a more significant role in his decision to commit espionage than anything that happened to him after he became an agent.

Hanssen's first period of espionage ended in the spring of 1981, when his wife Bonnie inadvertently discovered him reviewing a GRU communication in the basement of their home. Although Hanssen minimized his espionage in discussions with his wife, he says that he confessed his espionage to an Opus Dei priest within days of Bonnie's discovery. According to Hanssen, the priest granted him absolution and told him that he did not have to turn himself in, but suggested that he donate the money he had received from the GRU to charity. Hanssen said that he broke off contact with the GRU and made multiple $1,000 donations to Mother Teresa's "Little Sisters of the Poor."

The most significant information that Hanssen passed during this period concerned the identity of a long-time FBI asset in the GRU. Hanssen's first period of espionage was less damaging to the U.S. intelligence effort than his next two periods of espionage.

2. Second Period of Espionage: 1985 – 1991

Hanssen remained a dormant spy from 1981 until October 1985, when he volunteered to the KGB, the Soviet Union's principal intelligence service. In his letter to the KGB's Washington Residency, Hanssen was careful to maintain his anonymity and did not disclose his prior espionage on behalf of the GRU. Using the alias "Ramon" or "Ramon Garcia," Hanssen provided the KGB with information concerning the Intelligence Community's most important Soviet counterintelligence and military secrets, much of which he had learned while assigned to the Soviet Analytical Unit. Although Hanssen was working in New York from September 1985 to August 1987, all of his operational espionage activity during this period took place in the Washington area. According to Hanssen, he chose to volunteer to the KGB because he believed it was more professional, had a longer-term outlook, and paid more money than the GRU.

We believe that Hanssen's decision to resume espionage was motivated by many of the same factors at play in 1979. His obsession with espionage (which he referred to as an "addiction"), his lack of self-esteem and desire for recognition, his belief that he could commit espionage without being detected, and the lack of effective deterrence all played a role. The fact that Hanssen had done it before made it easier for him to do it again. Hanssen's return to espionage also was likely fueled by his knowledge that he had successfully evaded detection in the past and was in a position to demand a large payment from the Russians for the highly sensitive information he had obtained in the Soviet Analytical Unit.

During the next six years – the last stages of the Cold War – Hanssen delivered thousands of pages of highly classified documents and dozens of computer disks to the KGB detailing U.S. strategies in the event of nuclear war, major developments in military weapons technologies, identities of active and historical U.S. assets in the Soviet intelligence services, the locations of KGB defectors in the United States, analytical products from across the Intelligence Community, comprehensive budget and policy documents, and many other aspects of the Soviet counterintelligence program. He passed some of the most damaging information within his first two months of espionage, including the true names of the FBI's most significant Soviet sources at the time, KGB officers Sergey Motorin and Valeriy Martynov. Other significant operations that Hanssen compromised during this period included the FBI's espionage investigation of Felix Bloch, a senior State Department official suspected of providing information to the KGB, and an FBI analytical report regarding possible Soviet penetrations.

Toward the end of Hanssen's second period of espionage, he became increasingly careless, passing documents that clearly marked him as an FBI employee. For example, when he was assigned to the Inspection Division, he gave the KGB FBI inspection reports and documents that he took from field offices while on inspection assignments. Hanssen also compromised Foreign Intelligence Surveillance Act (FISA) wiretap applications prepared by the FBI. In a particularly reckless move, Hanssen suggested to the KGB that it attempt to recruit Jack Hoschouer, Hanssen's closest friend, who was then serving as a military attaché at the U.S. Embassy in Bonn.

Hanssen's second period of espionage contributed to the execution of at least three human sources – including Motorin and Martynov – and caused hundreds of millions of dollars worth of damage to U.S. intelligence programs. In return, the KGB gave Hanssen cash payments of at least $500,000, as well as three diamonds. He stored the cash, as much as $100,000 at a time, in a gym bag in his bedroom closet. He also deposited large amounts of the KGB's money into a passbook savings account in his own name at a bank located a block from FBI Headquarters. While Hanssen has not accounted for much of the money he received from the KGB, it is clear that he spent some of it on an addition to his home, cars, tuition payments for his children's private schools, gifts, a loan to his brother-in-law, and at strip clubs. In late 1989, Hanssen began a year-long relationship with a stripper, Pricillia Sue Galey. Hanssen paid for Galey to accompany him on an FBI Inspection Division trip to Hong Kong, bought her a Mercedes Benz, provided her with an American Express card, and gave her jewels, cash, and other gifts.

In August 1990, Hanssen's brother-in-law, FBI Special Agent Mark Wauck, heard that Hanssen's wife Bonnie had found $5,000 in unexplained cash in Hanssen's dresser drawer. Wauck reported this and other incidents he found suspicious to a supervisor in the FBI's Chicago Field Office. Although Wauck and the supervisor now have significantly different recollections of their conversation, we believe that Wauck provided the supervisor with enough information to warrant some follow up. Instead, the supervisor readily dismissed Wauck's concerns, in part because there was no policy or procedure mandating that he pass the information on for analysis and possible investigation. This incident highlights deficiencies in the FBI's protocol for the receipt and investigation of derogatory information about an agent. There was no standard procedure for reporting and collecting such information, nor was there a central repository at the FBI responsible for collecting this information.

After picking up a $12,000 KGB payment in December 1991, Hanssen again broke off contact with the Soviets. Hanssen told us that he took this action because of his increasing guilt and after confessing his espionage to Catholic priests. We are skeptical of this explanation, however, because Hanssen's decision to halt his espionage coincided with the fall of the Soviet Union, as well as with the initiation of a new FBI/CIA molehunt effort that Hanssen knew about. Both events increased the risk that Hanssen's espionage would be detected or disclosed.

3. Unsuccessful Approach to the GRU: 1993

A year and a half after breaking off contact with the KGB in late 1991, Hanssen made an awkward and unsuccessful attempt to reestablish contact with the GRU. The risks Hanssen took in approaching the GRU in 1993 far outweighed any he had taken during his first two periods of espionage. In July 1993, Hanssen approached a GRU officer in the garage of the officer's apartment building. Hanssen identified himself as an FBI agent, explained that he had worked for the KGB under the name Ramon Garcia, and tried to give the officer a package containing summaries of double agent cases that the FBI was running against the GRU. The GRU officer refused to accept the package, and then reported the approach to his superiors. The Russians filed a protest with the U.S. government – apparently believing that the approach had been an officially sanctioned provocation – and the FBI opened an investigation. Although Hanssen's approach to the GRU officer was reckless in a variety of ways, the FBI's investigation of this incident – which Hanssen monitored through the FBI's computer system – was unsuccessful.

Hanssen claimed that two factors motivated this approach to the GRU. First, he wanted an explanation as to why the GRU was still running double agent cases that he had previously compromised to the KGB. Second, he "felt pity" for the GRU and wanted to ensure that it knew which of its sources were actually double agents. Although Hanssen denied that this approach was motivated by a need for money, he sought funds from a wide variety of sources at about this time. Indeed, the day of the failed approach, Hanssen asked his mother for $10,000. In addition, even though Hanssen made this approach the day after his father died, he claimed not to remember the proximity of these two events during his debriefings and OIG interviews.

Hanssen's 1993 approach to the GRU was remarkable for its recklessness and self-destructive quality. Unlike his prior periods of espionage, Hanssen had face-to-face contact with a Russian intelligence officer, asked other FBI employees to conduct computer searches concerning this officer, and demonstrated virtually no regard for his personal security. Hanssen told the OIG that when the approach failed, it "shocked [him] back out of that mental state."

4. Third Period of Espionage: 1999 – 2001

In 1999, Hanssen revolunteered to the KGB. Over the next two years, Hanssen provided the Russians with information concerning some of the FBI's most significant KGB sources and most sensitive espionage investigations. Hanssen had obtained most of this information from improper searches of the FBI's ACS computer system. As with his second period of espionage, Hanssen used the pseudonym "Ramon Garcia" and communicated through dead drop exchanges, but passed many documents that were unmistakably FBI products. Hanssen's decision to resume espionage in 1999 was driven by two factors: (1) his discovery – through the ACS system – of the FBI's effort to identify a significant KGB mole believed to be a CIA officer; and (2) his deteriorating finances.

While searching the ACS system in the spring of 1999, Hanssen stumbled upon the FBI's most significant ongoing Russian espionage investigation. This case was a search for the KGB mole who turned out to be Hanssen. At the time, however, the FBI's investigation was focused on a CIA officer. Although the FBI did not intend for documents related to this highly sensitive investigation to be uploaded into the ACS system – because of widespread concerns about the system's security – many such documents were uploaded due to failures in training, simple human error, and insufficient

concern about maintaining operational security. Within a day of discovering the existence of the investigation, Hanssen obtained the CIA suspect's true name. Hanssen decided to warn the KGB about the investigation and thereby "save" the CIA suspect. Hanssen also stated that the case offered him all of the "excitement" and "stimulation" from espionage that he craved.

At the same time, Hanssen's financial situation was the worst it had ever been. Although Hanssen was close to the top of the FBI pay scale, his spending continually outstripped his income. He had significant credit card debts, car loans, bank loans, and tuition payments for his children. While Hanssen's mother had previously supplemented his income, giving him more than $94,000 in the mid-1990s, she told Hanssen in 1997 that she was running out of money. Hanssen claimed that he set a goal of obtaining approximately $100,000 from the KGB, believing that this amount would stabilize his finances, at least until he retired from the FBI and entered the private sector.

When Hanssen reestablished contact with the KGB in July 1999, he did so as "Ramon Garcia." Hanssen indicated that he needed money and provided a communications plan using a drop site from his second period of espionage. In August 1999, the KGB paid Hanssen $50,000. Over the next year, Hanssen made several attempts to pass information through dead drop exchanges, but the KGB failed to retrieve his packages. Accordingly, Hanssen resorted to mailing the KGB a disk and a letter which provided the true names of several individuals under investigation for espionage, as well as information concerning two FBI assets in the Russian intelligence services and two significant FBI technical operations. Hanssen's last successful dead drop exchange occurred in November 2000, when he gave the KGB a large stack of classified documents from the ACS system that he had been collecting for over a year.

In late 2000, the FBI identified Hanssen as a spy and lured him back to FBI Headquarters – where he could be more easily monitored – with the offer of a temporary Senior Executive Service position involving computer security. Hanssen began his new position on January 13, 2001. On February 12, 2001, the FBI discovered a package containing $50,000 that the KGB had left for Hanssen in a dead drop site. Six days later, on February 18, 2001, after Hanssen had left a package for the KGB in a different dead drop site, he was arrested and charged with espionage offenses.

Although Hanssen escaped detection for more than 20 years, this was not because he was a "master spy." While Hanssen took some important steps to maintain his security – such as refusing to reveal his identity to his Russian

handlers – and used his knowledge of the FBI's counterintelligence practices and poor internal security to his advantage, much of Hanssen's conduct when committing espionage was reckless. For example, Hanssen (1) set up an FBI camera on a drop site he used for exchanges with the GRU during his first period of espionage; (2) used an FBI telephone line and answering machine for communications with the KGB in 1986; (3) deposited much of the KGB's cash directly into a passbook savings account in his name in the late 1980s; (4) suggested to his Russian handlers in 1991 that they attempt to recruit Jack Hoschouer, his best friend; (5) directly approached a GRU officer in 1993 and revealed that he was an FBI agent who had previously committed espionage for the KGB – an approach that led to a diplomatic protest from the Russians and an FBI investigation that could have identified Hanssen as a mole; and (6) searched the FBI's computer system, during his last period of espionage, for references to his own name, address, and drop and signal sites – conduct that would have been difficult to explain if the FBI had utilized the computer system's audit feature. In sum, Hanssen escaped detection not because he was extraordinarily clever and crafty, but because of longstanding systemic problems in the FBI's counterintelligence program and a deeply flawed FBI internal security program.

C. FBI Analytical and Investigative Penetration Efforts: 1978 – 2001

The FBI's penetration efforts in the late 1970s and 1980s suffered from a lack of cooperation with the CIA and from inattention on the part of senior management. In 1985 and 1986, the CIA and FBI lost nearly every significant human asset then operating against the Soviet Union. These losses were unprecedented in scope, quantity, significance, and timing, yet the FBI undertook no sustained effort to determine their cause. Senior management was almost entirely unaware of the scope and significance of these losses, and throughout the 1980s the FBI failed to work cooperatively with the CIA to resolve the cause of these losses or to thoroughly investigate whether an FBI mole could be responsible for these setbacks. We now know that Hanssen compromised many of the assets and operations lost during the mid-1980s.

The early 1990s saw significant improvement in FBI/CIA cooperation, with the two agencies undertaking a joint investigation concerning the cause of the 1985-86 asset losses. The FBI drastically increased the number of squads and personnel devoted to espionage investigations, and the FBI's senior management took a much more active role in supervising penetration investigations. The energized penetration efforts led to successful espionage

prosecutions of CIA officers Aldrich Ames and Harold Nicholson, FBI Special Agent Earl Pitts, and NSA detailee David Boone. While the FBI worked closely with the CIA's Special Investigations Unit (SIU) on most of these cases, the SIU was not an equal partner. The FBI's failure to keep the CIA apprised of information concerning non-CIA espionage investigations – such as the case involving FBI agent Earl Pitts – undermined the effort to identify Hanssen.

In attempting to identify the mole who turned out to be Hanssen, the FBI intensively pursued a CIA suspect. This investigation culminated in the submission of a report to the Justice Department that appeared to seek the prosecution of that CIA suspect, despite the fact that some senior FBI managers had serious reservations about the conclusions of the report and doubted whether the officer – who has since been exonerated by the FBI – was the correct target.

Although the FBI pursued penetration leads in the 1990s that we now know related to Hanssen, he received no investigative scrutiny until late 2000. Indeed, the FBI never opened even a preliminary inquiry on any FBI employee in connection with the search for the mole ultimately identified as Hanssen. This was true even though the FBI had access to information suggesting that the mole might be an FBI employee, and believed that the mole had compromised certain FBI assets and operations.

Longstanding systemic problems in the FBI's counterintelligence program played an important role in the FBI's failure to uncover Hanssen. Most importantly, the FBI demonstrated a reluctance to consider itself as a possible source for a penetration in the absence of leads identifying a specific FBI target. Thus, the FBI maintained a focus on the CIA as the mole's employer despite information indicating that the mole might be an FBI employee.

Ineffective oversight by FBI management and poor coordination with the Justice Department also contributed to the length of the FBI's investigation of the wrong suspect and the failure to pursue alternative avenues. The FBI managers with supervisory authority over the investigation often deferred to line personnel – even when the managers harbored serious doubts about the progress of the investigation – resulting in a tacit endorsement of erroneous analysis and conclusions. This problem was compounded by the FBI's poor coordination with the Justice Department components responsible for overseeing intelligence investigations – the Office of Intelligence Policy and Review (OIPR) and the Criminal Division's Internal Security Section (ISS).

Because the FBI did not provide the Justice Department with complete information about its investigation – omitting crucial information about weaknesses in proof and investigative setbacks – the Justice Department could not properly evaluate the strength of the FBI's case against the CIA suspect.

1. Ad Hoc Analytical and Investigative Efforts from the 1970s to 1993

In the 1970s and early 1980s, the FBI investigated several source reports of Soviet penetrations of the FBI and CIA. None of the leads from this time period appears to have any connection to Hanssen's espionage.

In the 1980s and early 1990s, the FBI's response to learning that an important FBI Soviet asset was compromised or to receiving information indicating that a human penetration was at work was often to create an ad hoc team to examine the issue. These efforts were typically analytical rather than investigative. While each study considered the possibility of an FBI mole, none involved an actual investigation of this issue, and none resulted in an investigation being opened on a specific FBI employee. Likewise, none of these efforts concluded that a penetration of the FBI was responsible for the ongoing compromises that the FBI's Soviet program experienced from the mid-1980s to early 1990s.

In late 1986, the FBI learned that its two most significant Soviet assets – KGB officers Motorin and Martynov – had been arrested for espionage within the previous year. This appears to be the first notice the FBI received concerning compromises attributable to Hanssen, who we now know compromised both assets in October 1985, confirming information that CIA officer Aldrich Ames had provided to the KGB in June 1985.

After learning that its two most important KGB assets had been arrested, the FBI formed a six-person task force to determine how they had been compromised and whether an FBI mole was responsible. In the course of its review, the Task Force discovered that because of poor document controls and violations of the "need to know" principle it was impossible to determine who within the FBI had had access to the Motorin and Martynov cases. Accordingly, no FBI employee with knowledge of these assets was investigated. Nonetheless, in September 1987 the Task Force issued a final report stating that there was no evidence of a Soviet spy in the FBI. The Task Force, however, did not resolve how the assets had been compromised.

During the Task Force effort, the FBI learned that the CIA had likewise suffered catastrophic and unprecedented losses in its Soviet program. Yet, the

FBI failed to work cooperatively with the CIA to resolve the cause of these losses.

Between 1987 and 1991, the FBI suffered continuing losses of Soviet human assets and technical operations that it could not explain. During this period, the FBI conducted two analytical studies that considered the penetration issue, but neither study led the FBI to investigate the possibility of an FBI mole. The first study was a two-year effort aimed at resolving historical allegations of an FBI penetration. The project proceeded chronologically, and by late 1988 the team had analyzed leads only from the 1950s and 1960s. In an interim report, the team concluded that two penetrations of the FBI existed before 1964, but the team never reached the time period relevant to the FBI's more recent and unprecedented losses. The project was abandoned in the summer of 1989.

The second study systematically examined more than 50 FBI operations that had been compromised since 1986, including human assets, technical operations, double agent programs, and recruitment operations. The final report, issued in November 1988, described the continuing, across-the-board problems within the FBI's Soviet operations, but was equivocal with respect to the possibility of an FBI mole. The report suggested that a CIA penetration was a more likely explanation for the FBI's losses. We now know that Hanssen compromised most of the significant operations discussed in the report.

In 1991, the FBI and the CIA formed the SIU, which was directed to analyze the numerous FBI and CIA cases lost after 1985 and to prepare a list of suspects who could account for the losses. Simultaneously, the FBI created a new investigative squad at WFO to pursue investigative leads generated by the SIU and, in the meantime, to reanalyze many of the same FBI compromises and penetration leads considered during the FBI's earlier analytical efforts. By the end of 1992, after reviewing numerous FBI and CIA historical compromises without any investigative progress, the squad began to disband while awaiting new leads from the SIU.

While the SIU obtained compelling evidence that CIA officer Aldrich Ames was a Russian mole and was likely responsible for many of the compromises at issue, the team's March 1993 final report merely stated that there was a KGB penetration in the CIA who began his espionage in 1985. The report failed to highlight Ames as a suspect worthy of special investigative attention. Instead, Ames was presented simply as one of 40 CIA employees who had access to the Soviet operations compromised in the 1985-86 period. The report did not include a comparable list of FBI employees. Although the

SIU's final report raised the possibility of a KGB penetration of the FBI, the team did not undertake or recommend any meaningful action concerning this possibility.

2. Penetration Investigations and the Search for Hanssen: 1993 – 2001

The years between 1993 and 2001 marked one of the most active and productive periods for espionage investigations in the FBI's history. The FBI greatly expanded its counterespionage effort and successfully apprehended a number of significant Russian spies. This period was dominated, however, by the search for a KGB mole who was reportedly more damaging than Ames. The FBI poured enormous resources into this search. The FBI believed early on, however, that the mole was a CIA employee and did not change that view. We now know that the FBI was on the wrong track from the beginning, because the mole the FBI was looking for was Hanssen, an FBI employee.

As the investigation unfolded, the FBI focused on a specific CIA employee. Given the information it had at the time, the FBI's initial selection of this CIA employee as the lead suspect was understandable. Although an extensive investigation of this CIA suspect failed to yield any conclusive evidence of espionage, the FBI became convinced that he was a KGB mole. This was due in part to the suspect's ambiguous and sometimes suspicious behavior and in part to a belief that this individual had emerged as the lead suspect as the result of an objective and scientific process. Despite its lack of success in the investigation, the FBI, in a 70-page Investigative Report, informed the Justice Department that the CIA suspect was a significant KGB mole, and sought an opinion as to whether he could be prosecuted for espionage.

The FBI should have seriously questioned its conclusion that the CIA suspect was a KGB spy and considered opening different lines of investigation. The squad responsible for the case, however, was so committed to the belief that the CIA suspect was a mole that it lost a measure of objectivity and failed to give adequate consideration to other possibilities. In addition, while FBI management pressed for the investigation to be completed, it did not question the factual premises underlying it. Similarly, the CIA's SIU did not serve as an effective counterbalance to the FBI, because it was not an equal partner in the molehunt.

The supervisory failures in connection with the espionage investigation of the CIA suspect are most apparent in the context of the Investigative Report

that the FBI presented to the Justice Department. Although several senior FBI managers had serious doubts that the CIA suspect was the correct target, and expected the Justice Department to decline prosecution for a lack of evidence, the Investigative Report was written as if the FBI had no doubt that the CIA suspect was a KGB mole who was the most damaging spy since Ames.

Fortunately, the Justice Department never brought charges against the CIA suspect, because while prosecutors were reviewing the case the FBI determined that Hanssen was in fact the KGB mole. In late 2000, the FBI opened an investigation of Hanssen, and on February 18, 2001, he was arrested for espionage. The FBI later exonerated the CIA suspect.

IV. Summary of the FBI's Security Programs During Hanssen's Career

The Hanssen case highlighted significant, longstanding deficiencies in the FBI's internal security program, many of which were brought to the attention of FBI management over the years but were not corrected. Historically, the FBI has not been in compliance with Executive Orders, Justice Department regulations, and Intelligence Community standards regarding internal security. Although we found that the FBI has taken many important steps to improve its internal security program since Hanssen's arrest – including the implementation of a counterintelligence-focused polygraph examination program, the development of a financial disclosure program, and the creation of a Security Division – some of the most serious weaknesses still have not been fully remedied. These weaknesses expose the FBI to the risk of future serious compromises by another mole.

Before Hanssen's arrest, the FBI's security program was based on trust. Rather than taking the sort of proactive steps adopted by other Intelligence Community components – such as requiring regular counterintelligence polygraph examinations, financial disclosures, and meaningful background reinvestigations, and utilizing audit functions regarding computer usage – the FBI trusted that its employees would remain loyal throughout their careers. The Hanssen case shows the danger of that approach.

In our review, we observed serious deficiencies in nearly every aspect of the FBI's internal security program, from personnel security, to computer security, document security, and security training and compliance. These deficiencies led to the absence of effective deterrence to espionage at the FBI and undermined the FBI's ability to detect an FBI mole. Moreover, the absence of deterrence played a significant role in Hanssen's decision to commit espionage. As he explained during debriefings: "[I]f I had thought that the risk

of detection was very great, I would never have done it." Hanssen also exploited many of these weaknesses – particularly in document and computer security – to pass sensitive information to the KGB.

With respect to personnel security, Hanssen was never subject to a wide variety of basic security techniques and procedures that could have deterred or perhaps uncovered his espionage. For example, Hanssen was never asked to submit to a polygraph examination during his 25-year FBI career, despite his extraordinarily broad access to extremely sensitive human and technical intelligence information from across the Intelligence Community. After Ames's 1994 arrest, FBI National Security Division managers argued for an aperiodic, random polygraph program, but the FBI's most senior management rejected that request, largely because of concerns regarding false positives. Hanssen's arrest in 2001 finally prodded the FBI to make a polygraph examination part of the standard five-year background reinvestigation. According to the FBI, by June 2003 it had also expanded its polygraph program by implementing aperiodic, random polygraph examinations.

Hanssen likewise was never asked to complete a detailed financial disclosure form during his FBI career. During our interviews, Hanssen identified meaningful financial disclosure as the security technique that would have provided the greatest deterrence to his espionage. As it was, Hanssen felt comfortable depositing thousands of dollars of the KGB's cash in a passbook savings account – listed in his own name – at a bank located a block away from FBI Headquarters. He also safely invented stories about family wealth and successful investments to explain his spending. The FBI reported in July 2003 that a financial disclosure program "will be implemented within the next month." Given that financial gain is often an important motive for committing espionage, developing a credible financial disclosure program is a critical element in improving the FBI's personnel security with respect to both deterrence and detection.

Hanssen received his first – and only – background reinvestigation in 1996, 20 years after he had joined the FBI. The FBI has conceded that a number of "red flags" emerged during Hanssen's reinvestigation that were not resolved. The FBI's perfunctory background reinvestigation of Hanssen was not atypical, however. The system in place for background reinvestigations discouraged thoroughness. The principal investigators were not given access to the necessary source materials, such as the employee's personnel file, security file, and credit reports, and they primarily interviewed references supplied by the employee. They did not interview the employee. Moreover,

the principal investigators merely collected information; they were not required to provide analysis or to make investigative recommendations. As a result, information developed through background reinvestigations received little analysis.

In committing espionage, Hanssen exploited serious weaknesses in the FBI's document and information security. His access to classified national security information – for both hard copies and computer files – was subject to little control or monitoring throughout his FBI career. As a result, he walked out of the FBI with copies and originals of some of the U.S. government's most sensitive classified material – including numbered Top Secret documents – with little fear of being stopped or detected. The FBI's inability to account for its most sensitive documents and failure to limit this information to those with a "need to know" has been noted both by the OIG and by the FBI's internal reviews in the past, but remains uncorrected. This deficiency is significant with respect to both deterrence and detection, because the FBI's inability to account for its most sensitive documents makes an access-based investigation for an FBI mole extremely difficult to pursue. The starting point for any such investigation is a list of those employees who had access to a compromised operation; at the FBI, that determination is often impossible to make.

During his last period of espionage, Hanssen used the FBI's ACS computer system to track the FBI's most sensitive espionage investigations – including the investigation that was looking for him. Hanssen also routinely searched the system for references to his own name and home address, and to the signal and drop sites that he used, to assure himself that he was not under investigation. Hanssen conducted thousands of searches for highly sensitive information that he had no conceivable "need to know," without fear that a computer audit would reveal his misconduct. As with his record of cash deposits, it would have been difficult for Hanssen to invent an innocent explanation for his repeated searches regarding his name, address, and signal and drop sites. Even more significantly, an audit of Hanssen's ACS activity would have identified him as someone worthy of investigation.

The serious security flaws in the FBI's ACS system – which have been discussed in prior OIG reviews and internal FBI inspection reports – have been apparent since the system's inception in 1995, but have not been remedied. Access restrictions are subject to ready override by Headquarters personnel who, like Hanssen, have no "need to know" about the sensitive operations the access restrictions are designed to protect. The system is likewise prone to human error, with documents concerning highly sensitive operations – such as

the Hanssen investigation – being made available to any curious user because of improper uploading or inadequate restriction codes. The ACS system's audit function, mandated by Justice Department regulations and a principal tool against unauthorized usage as well as espionage, was rarely utilized before Hanssen's arrest.

Today, more than two years after Hanssen's arrest, the ACS system remains insecure and vulnerable to misuse. The current audit program relies on case agent review rather than third-party auditing. Moreover, the program has only retroactive effect; case agents do not receive real-time notice when someone seeks unauthorized access to their cases. The "need to know" principle is not adequately applied in the computer context within the Counterintelligence Division; all Headquarters Counterintelligence Division agents have access to all cases in the Division whether or not their section or unit is connected to the case. Finally, the system's susceptibility to human error has not been remedied. In response to the OIG's findings regarding the ACS system, the FBI reported in July 2003 that "attempting technical changes to improve ACS security would not be a smart business decision" in light of plans to implement a new automated case system known as the Virtual Case File (VCF). The FBI stated that the first delivery of VCF is scheduled for December 2003. In developing and implementing VCF, it is vital for the FBI to rectify the types of security flaws that have been evident in the ACS system for many years.

The FBI's lax approach to personnel and information security also was apparent in its handling of security violations. Hanssen's career was replete with security breaches, none of which were documented in his personnel or security file or (with one exception) reported to the FBI's Office of Professional Responsibility, the Security Programs Manager, the NSD's Security Countermeasures Section, the Justice Department Security Officer, or any other central location for review and consideration of appropriate disciplinary action. While these security breaches did not necessarily show that Hanssen was engaged in, or was predisposed to engage in, espionage, they demonstrated that he was unfit to have access to sensitive information. Our review revealed unwillingness within the FBI to report security violations and take them seriously, even when highly sensitive information was involved. The Hanssen case also highlighted the absence of a centralized reporting program for security violations at the FBI, as well as the absence of a unit at FBI Headquarters responsible for collecting derogatory information concerning FBI employees, particularly in the counterintelligence context. In July 2003, the FBI reported that a security incident program had been instituted that will

be managed by a new Security Compliance Unit. According to the FBI, the Security Division and the Counterintelligence Division will meet on a monthly basis to discuss counterintelligence-related issues.

Many of the security issues that emerged from our review of the Hanssen case stem from deficiencies in training. For example, FBI personnel specialists responsible for employee background reinvestigations did not have the necessary analytical training to assess issues that commonly arise during background investigations. FBI employees using the ACS system did not have sufficient knowledge and training to use the security controls that were built into the system to regulate access to sensitive cases. FBI employees were not knowledgeable regarding the requirements for handling classified materials, particularly at the Sensitive Compartmented Information (SCI) level. And employees and supervisors were not properly trained in how to report and document security violations. We believe that the FBI will not see significant improvement in its internal security until its employees are better trained on security issues.

In sum, the absence of adequate security controls at the FBI made espionage too easy for Hanssen to commit. Because of inadequate document security, he felt comfortable removing thousands of pages of classified documents from FBI offices. Because of lax controls over even the most sensitive information and violations of the "need to know" principle, he knew that he could compromise the FBI's most important Soviet/Russian assets and operations with little risk that the loss of these cases would be traced to him. Because of inadequate computer security, he felt free to conduct thousands of searches on the ACS system for references to himself and for information concerning the FBI's most sensitive counterintelligence cases. Because of the absence of financial disclosure, he felt comfortable depositing thousands of dollars in espionage proceeds into his bank accounts. Because of the absence of polygraph examinations for onboard employees, he never had to confront the issue of what would happen when he failed polygraph questions aimed at determining whether he was or had ever been an agent of a foreign power. And because of a flawed and inadequate background reinvestigation program, he never had to fear that the FBI would uncover spending and other behavior inconsistent with his position at the FBI.

The defects in the FBI's security program were the product of decades of neglect. Historically, FBI management did not allot sufficient resources to security and rejected internal recommendations – for example, in the polygraph area – to make necessary improvements to the program. As a consequence,

following Hanssen's arrest, the FBI faced enormous challenges in the areas of personnel, computer, and document security. While the FBI has made progress in many of these areas, in others – particularly computer security – problems have not been fully remedied and significant work still needs to be done. The FBI's Security Division must receive appropriate resources and support to ensure that the security program is significantly improved.

V. The Failure to Deter and Detect Hanssen's Espionage

The FBI's failure to deter and detect Hanssen's espionage over a more than 20-year period cannot be attributed to any individual FBI employee or small group of FBI supervisors. In addition, it is important to note that the agents and analysts who conducted the FBI's penetration investigations were extremely dedicated and hard-working, and demonstrated an impressive commitment to the counterintelligence mission. Their work produced many successes.

At the same time, we found overarching problems in the FBI's internal security efforts. Most of the deficiencies discussed in our report are of longstanding vintage and reflect the cumulative decisions of many FBI employees, including the Directors and senior managers who failed to remedy serious flaws in the FBI's personnel, document, and information security programs; the Directors and senior managers who failed to devote sufficient resources and attention to the penetration issue in the 1980s and early 1990s, and failed to resolve how important FBI human sources and operations had been compromised; the unwillingness of line personnel working on the espionage investigation of the CIA suspect to reconsider initial conclusions and judgments in the face of investigative failures, and senior managers' failure to insist that they be revisited; the failure of senior managers to ensure that accurate information was supplied to the Justice Department concerning the investigation of the CIA suspect; the supervisors and colleagues who ignored Hanssen's pattern of security violations and his obvious lack of suitability for handling sensitive information; and the managers who provided such lax supervision of Hanssen that he was able to spend much of his time on non-work related matters, or worse, committing espionage. These were widespread failings.

We believe that what is needed at the FBI is a wholesale change in mindset and approach to internal security. The FBI must recognize and take steps to account for the fact that FBI employees have committed espionage in the past and will likely do so in the future. A unit at the FBI must be responsible for asking every day whether there is evidence that the FBI has

been penetrated, and the FBI's internal security program must shift from a program relying on trust to a program based on deterrence and detection. The following 21 recommendations are concrete steps the FBI should take to improve its internal security and ability to deter and detect espionage in its midst.

VI. Recommendations

A. Improving the FBI's Performance in Detecting an FBI Penetration

Recommendation No. 1: New Penetration Unit at FBI Headquarters

A specialized permanent unit should be created within the Counterespionage Section at FBI Headquarters dedicated to determining whether the FBI has been penetrated. This Unit would be responsible for, among other things, analyzing relevant source information, resolving how compromised assets and operations were lost, and reviewing operations that lost their productivity or effectiveness for no apparent reason, all with a view towards determining whether the Bureau has been penetrated.

Recommendation No. 2: Senior Operational Post for Intelligence Community Representative in FBI Counterespionage Section

The FBI should create a senior operational position in the Counterespionage Section at FBI Headquarters that will be filled – on a rotating basis – by senior executives from the CIA and other components of the Intelligence Community.

B. Improving Coordination with the Justice Department

Recommendation No. 3: Criminal Division Involvement in Counterintelligence Investigations

Department of Justice Criminal Division personnel should be full participants in counterintelligence investigations once suspicion has focused on a specific individual.

Recommendation No. 4: More Substantive Role for OIPR Attorneys

OIPR attorneys should have a larger oversight role in ensuring the accuracy and fairness of factual assertions in FISA applications and have direct access to the case agent and the source information relied on in the application.

C. Improving Source Recruitment, Security, and Handling

Recommendation No. 5: Greater Emphasis on and Resources for New Source Recruitment

The FBI should place greater emphasis on and provide more resources for targeting and recruiting intelligence officers in hostile intelligence services who are likely to have knowledge of penetrations of the Intelligence Community.

Recommendation No. 6: Stricter Standards for Handling and Tracking Sensitive Information from Significant Human Sources

The FBI should adopt stricter standards for handling and tracking sensitive information from significant human sources and should enforce the "need to know" policy in disseminating information from such sources. The FBI should also adopt special handling techniques to better account for dissemination of such information.

Recommendation No. 7: Guidelines for Handling Recruitments-in-Place/Defectors

The FBI should adopt guidelines for handling active recruitments-in-place and recent defectors that, among other things, limit the disclosure of sensitive information, such as details of ongoing espionage investigations, to such individuals.

D. Security Improvements

Recommendation No. 8: Central Repository for Derogatory Information

The FBI should create a central repository for the receipt, collection, storage, and analysis of derogatory information concerning FBI employees with access to sensitive information. This repository should be directly accessible to Counterespionage Section personnel responsible for determining whether the FBI has been penetrated. The FBI should mandate that information or allegations that reflect on the integrity, suitability, or trustworthiness of an employee be documented and transmitted to this central repository for analysis. The FBI should also train employees in recognizing the types of behavior that should be reported.

Recommendation No. 9: Documentation of Security Violations

The FBI should create policies and procedures designed to ensure that security violations are reported, documented in an employee's security file, and properly investigated and resolved. A database should be created to track security violations by employees and identify patterns and trends. The FBI should conduct regular security awareness training of its personnel, and this training should include clear instructions regarding the reporting of security violations.

Recommendation No. 10: Meaningful Background Reinvestigations

The FBI should adopt new procedures to ensure that background reinvestigations are thorough, meaningful, and timely. Responsibility for this program should be consolidated within the Security Division, and an automated case management system should be installed that captures, stores, and facilitates the analysis of personnel security information.

Recommendation No. 11: Financial Disclosure

The FBI should implement an annual, computer-based financial disclosure program for employees with access to sensitive information. The program – which should include disclosure of all accounts held by the employee and immediate family members in financial institutions – should be designed to detect unusual fluctuations in assets and cash flow as well as extraordinary levels of debt, and should involve both collection of information and analysis.

Recommendation No. 12: Random Counterintelligence Polygraph Program

The FBI should fully implement a counterintelligence polygraph program for employees with access to sensitive information and develop a counterintelligence polygraph program for non-FBI personnel who are given access to sensitive information.

Recommendation No. 13: Enhanced Security Measures for FBI Employees with Unusually Broad Access to Sensitive Information

The FBI should consider enhanced security measures – for example, more frequent polygraph examinations, more frequent and thorough background reinvestigations, and more detailed financial disclosures – for employees who enjoy unusually broad access to sensitive information.

Recommendation No. 14: Detecting Improper Computer Usage and Enforcing "Need to Know"

The FBI should implement measures to improve computer security, including (a) an audit program to detect and give notice of unauthorized access to sensitive cases on a real-time basis; (b) an audit program designed to detect whether employees or contractors are using the FBI's computer systems to determine whether they are under investigation; (c) procedures designed to enforce the "need to know" principle in the context of computer usage; and (d) a program designed to ensure that restricted information cannot be improperly accessed through the use of security overrides or other means.

Recommendation No. 15: Tracking Classified Information

The FBI should create and implement a program enabling it to account for and track hard copy documents and electronic media containing sensitive information. This program should also be designed to prevent the unauthorized removal of sensitive information from FBI facilities, either through the use of technology that "tags" classified documents and computer media or through other means. The FBI should likewise develop a program to prevent the improper copying of classified information.

Recommendation No. 16: Security Compliance Program

The FBI should implement a security inspection program that ensures that deficiencies in security are detected and remedied within a reasonable time. Compliance with recommendations from internal audits and inspection reviews, as well as from external oversight reviews, should be tracked and monitored until resolution.

Recommendation No. 17: Improving Security Education and Awareness

The FBI should make implementation of an FBI-wide security education and awareness program a top management priority. In addition, the FBI should track and regularly monitor the status of employee security training.

E. Management and Administrative Improvements

Recommendation No. 18: Exercise of Managerial Authority over Espionage Investigations

FBI supervisors must guard against excessively deferring to line personnel when supervising significant espionage investigations and must ensure that the

Department of Justice is properly briefed on the strengths and weaknesses of potential espionage prosecutions.

Recommendation No. 19: Damage Assessments for FBI Spies

Damage assessments concerning FBI employees who have committed significant acts of espionage should be led by experienced counterintelligence personnel and be conducted by an Intelligence Community entity, such as the National Counterintelligence Executive (NCIX).

Recommendation No. 20: Recusal Procedures for FBI Employees

The FBI should adopt written policies and procedures for recusal of FBI employees and supervisors who may be suspects in an espionage investigation.

Recommendation No. 21: Supervision of FBI Detailees

The FBI should ensure that FBI detailees serving in other Intelligence Community components and elsewhere are properly supervised and receive regular performance evaluations.

Glenn A. Fine
Inspector General

August 2003

OlG Investigative Team
Scott M. Barden
Kevin F. Becks
Paul G. Gardephe
Stephen D. Kelly
Mei Lin Kwan-Gett
Jeffrey D. Long
Jeffrey K. Vasey
Dominic N. Russoli
L. Susan Woodside