A Review of the FBI's Progress in Responding to the Recommendations in the Office of the Inspector General Report on Robert Hanssen

EXECUTIVE SUMMARY

Office of the Inspector General
Oversight and Review Division
September 2007

I. Introduction

On February 18, 2001, Robert Philip Hanssen, a former Federal Bureau of Investigation (FBI) Supervisory Special Agent, 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. Hanssen was the most damaging spy in FBI history. His espionage began in November 1979 – three years after he joined the FBI – and continued until his arrest, just two months before his mandatory retirement date. Over more than 20 years, Hanssen compromised some of this nation's most important intelligence 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. On July 6, 2001, Hanssen pled guilty to espionage charges, and on May 10, 2002, he was sentenced to life imprisonment.

Shortly after Hanssen's arrest, the Senate Select Committee on Intelligence and the Attorney General asked the Department of Justice Office of the Inspector General (OIG) to review the FBI's performance in connection with the Hanssen case. The OIG's report, "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen" (Hanssen Report), was issued on August 14, 2003. We produced two classified versions of the report: a full 674-page report classified at the Top Secret/Codeword level because it contained extremely sensitive classified information regarding sources involved in the Hanssen case and FBI counterintelligence activities, and a 383-page report classified at the Secret level, which did not include the detailed source information contained in the full report. In addition, we produced and publicly released a 35-page unclassified executive summary that highlighted the investigation's primary findings.[1]

The OIG's review examined in detail Hanssen's career at the FBI, his espionage, and the FBI's efforts to uncover the cause of the compromises of the U.S. Intelligence Community's Soviet/Russian assets and operations from 1978 to 2001. We concluded that Hanssen did not escape detection because he was a "master spy" who was extraordinarily clever and crafty, but because of longstanding systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program.

---

[1] The executive summary is available on the OIG's website at http://www.usdoj.gov/oig/special/0308/index.htm.

Based on our findings, our report made 21 recommendations to improve the FBI's internal security and its ability to deter and detect espionage by its own employees. The recommendations fell into five general categories: improving the FBI's performance in detecting an FBI penetration; improving coordination with the Justice Department; improving source recruitment, security, and handling; improving internal security; and improving management and administrative oversight concerning several espionage-related issues. A complete list of our recommendations is attached to this report.

II. Summary of the OIG Follow-Up Review and Structure of the Report

Since issuance of our original Hanssen Report, the OIG has followed the FBI's progress toward implementing our recommendations through reports provided to us by the FBI in September 2003 and January 2004. The FBI reports identified each recommendation, stated how the FBI intended to implement it, and provided the status of the implementation efforts.

In this follow-up review, we assessed the FBI's progress in implementing the 21 recommendations we made to help improve FBI counterintelligence and internal security operations. We met with representatives from the FBI and requested information to supplement and update the FBI's earlier reporting concerning programs and initiatives that were in various stages of development. As part of the follow-up review, we also conducted interviews of FBI executives and managers from the Counterintelligence and Security Divisions.

The completion of this follow-up review was delayed by the arrest of former FBI intelligence analyst Leandro Aragoncillo in September 2005 on charges of conspiracy, acting as an unregistered agent of a foreign country, and unauthorized use of a government computer. According to the September 9, 2005, criminal complaint filed against Aragoncillo, he used his computer at the FBI's Fort Monmouth Information Technology Center (FMITC) during a 3½ month period to download and print 101 sensitive documents pertaining to the Philippines, 37 of which were classified Secret. Aragoncillo then transmitted the documents to current and former high-level Philippine government officials. On May 4, 2006, Aragoncillo pleaded guilty to four federal charges: conspiracy to transmit national defense information; transmission of national defense information; unlawful retention of national defense information; and unauthorized use of a computer. On July 18, 2007, Aragoncillo was sentenced to 10 years in prison and fined $40,000.

In light of similarities between Aragoncillo's conduct and Hanssen's espionage activities, and their relevance to our assessment of the FBI's progress in improving its counterintelligence and internal security programs, we requested and received from the FBI information relating to the

investigation and arrest of Aragoncillo, which we considered in this follow-up review.[2]

Our final 97-page report, which is classified at the Secret level, describes the results of our follow-up review assessing the FBI's progress in implementing the recommendations from our Hanssen Report. We have provided the report to the Department of Justice and to appropriate Congressional committees.

The report is organized into sections that correspond to the five general categories of recommendations made in the Hanssen Report. In each section, we examine the FBI's progress in implementing the recommendations and identify what steps, if any, we believe still need to be taken to respond to the concerns the recommendations addressed. In the final section of the report, we examine the Aragoncillo matter. This 41-page unclassified executive summary of the full classified report is similarly organized.

In general, as described in detail below, we found that the FBI has made significant progress in implementing most of the recommendations we made in our original Hanssen Report. However, the FBI has still not fully implemented some of the most important recommendations. In addition, the FBI's progress in several areas has been uneven and in others requires further attention. We also found that despite the FBI's stated policies in response to our recommendations, the Aragoncillo matter reveals mixed progress in the FBI's actual implementation of its responses to some of these recommendations, as well as in its efforts to establish a reliable and effective internal security program across the agency. The circumstances surrounding Aragoncillo's activities and the FBI's response to them are stark reminders of the vulnerabilities that persist within the FBI's security program and the further need to address these vulnerabilities.

We now discuss each of our recommendations and the FBI's response.

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

A. Recommendation No. 1: New Penetration Unit at FBI Headquarters

We recommended that the FBI create a specialized unit within the Counterespionage Section at FBI Headquarters dedicated to determining whether the FBI had been penetrated. This unit would be responsible for

[2] We did not receive all the information we needed during the pendency of the Aragoncillo case. After Aragoncillo pled guilty to the charges, the FBI provided the requested information to us.

analyzing relevant source information, resolving how compromised assets and operations were lost, and reviewing operations that lost their productivity or effectiveness with no apparent reason, all with the view towards determining whether the FBI had been penetrated. We stated that, given the espionage of Hanssen and other FBI employees, the FBI must recognize the very real possibility that a spy could be working within the FBI's ranks and therefore the FBI should institutionalize efforts to detect and deter espionage by FBI employees.

We believed that creating a permanent penetration unit at FBI Headquarters would serve several important purposes:

1. it would ensure that the possibility of an FBI penetration is considered at all times;

2. it would increase the likelihood that patterns in compromised operations that point to an FBI mole are detected;

3. it would ensure that investigations of significant compromises are opened; and

4. the unit would develop expertise and provide continuity that the previous ad hoc method failed to establish.

The FBI stated in its original response to our recommendation that in May 2002 the Counterintelligence Division created a new Counterespionage Section, and within that section established a unit responsible for overseeing espionage investigations and other counterintelligence issues involving FBI employees and applicants, and possible penetrations of the FBI. However, the FBI reported that this unit was also responsible for overseeing two additional programs. Further, we learned that this additional responsibility required a significant amount of work and attention. Nonetheless, the FBI disagreed with our recommendation that the new unit should be dedicated exclusively to potential FBI penetration matters.

During our follow-up review, we raised concerns to the FBI about the new unit's scope of responsibilities. We noted that our recommendation did not merely seek to ensure adequate coverage of reports of alleged penetration made to the FBI, but envisioned a unit whose sole responsibility is to consider the possibility of a penetration. The recommendation also sought to create a unit that focuses proactively – and exclusively – on these issues so patterns in compromised operations or trends in internal irregularities that point to an FBI mole would more likely be detected. We also expressed our belief that this capability is weakened when the unit responsible for such proactive detection is also responsible for investigating other matters.

In response to our comments, the FBI recently agreed to dedicate the new unit exclusively to internal penetration matters. It transferred from that unit the two additional programs for which the unit had oversight responsibility.

We believe that the FBI's decision to fully implement this recommendation, after disagreeing with it for several years, is a positive step. We believe that the changes made to the penetration unit, if the changes are fully implemented and the unit is provided adequate resources, can improve the FBI's ability to proactively review compromised operations and anomalous personnel security information that suggest an FBI penetration.

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

We recommended that the FBI create a senior operational position in the Counterespionage Section at FBI Headquarters to be filled on a rotating basis by a Central Intelligence Agency (CIA) or other Intelligence Community senior executive. We made this recommendation to address our finding that the FBI's penetration efforts between 1979 and 2001 demonstrated a marked reluctance to consider the possibility that an FBI employee might have compromised FBI operations. In the investigation of the mole that turned out to be Hanssen, the FBI failed to seriously pursue the possibility that the mole was an FBI employee, despite significant leads suggesting just that.

In our judgment, placing a CIA or other Intelligence Community counterintelligence expert in a high-level position within the FBI's Counterespionage Section (such as Assistant Section Chief) would benefit FBI penetration efforts by helping to ensure impartiality and an objective evaluation of source information and other evidence.

In its initial response to our recommendation, the FBI stated that a senior executive-level CIA employee had been detailed to the FBI's Counterintelligence Division and was "in a position to have a birds-eye view of information flowing through that Division." According to the administrative agreement between the FBI and the CIA, the senior executive served as the Special Assistant to the Assistant Director for the Counterintelligence Division. His responsibilities "relate[d] to all counterintelligence and espionage investigations being conducted by the FBI that involve CIA interests and equities," and he had "access to all such investigations and advise[d] the [Deputy Assistant Director] on those investigations."

However, we learned during our follow-up review that the arrangement with the CIA had changed, and that instead of placing a high-level Special Assistant detailee in what had essentially become a monitoring role, CIA

detailees were assigned to the operational sections within the FBI's Counterintelligence Division. According to the Division's Assistant Director, the advantage of this arrangement is that CIA personnel are "plugged in" at the section level – as compared to the division level where the Special Detailee was assigned – where operational anomalies in cases will first be detected, thereby better positioning the CIA personnel to provide meaningful assistance in areas of concern.

While we recognize the important benefits of the modified arrangement with the CIA, we expressed concern during our follow-up review that the arrangement failed to provide continuing CIA involvement once an anomaly or other concern causes the FBI's Counterespionage Section to initiate an investigation. We believed that some level of representation in this section was still needed to help ensure the impartial and objective evaluation of cases.

The FBI has since reported that it made a formal request to the CIA for a detailee to serve as an Assistant Section Chief in the Counterespionage Section at FBI Headquarters. The FBI also reported that the CIA verbally agreed to provide a candidate for the position. We believe that once a candidate is identified and begins the detail, the FBI will have fully implemented our recommendation, which could lead to improved evaluation and investigation of penetration matters.

IV. Improving Coordination with the Justice Department

A. Recommendation No. 3: Criminal Division Involvement in Counterintelligence Investigations

Our recommendation that the FBI improve its coordination with the Criminal Division on counterintelligence investigations was made shortly after the law governing intelligence information sharing underwent significant change. Until November 2002, the Department of Justice Criminal Division's Counterespionage Section was unable to properly supervise espionage investigations because of the FBI's concern that sharing information with or obtaining advice from the Counterespionage Section might be prohibited by law. Both the FBI and Department of Justice Office of Intelligence Policy and Review (OIPR) believed that the Foreign Intelligence Surveillance Act (FISA) prohibited the Criminal Division from providing guidance or advice to the FBI on espionage cases until the FBI was virtually certain that the investigation would lead to a criminal prosecution, because of the belief that that the "primary purpose" of FISA surveillance had to be obtaining foreign intelligence information as opposed to evidence of a crime.

Following the September 11, 2001, terrorist attacks, the Department took several steps to remove the separation – or "wall" – between intelligence

and criminal information. These included significant amendments to the USA Patriot Act in October 2001; new guidelines issued by the Attorney General in March 2002 regarding intelligence-sharing procedures that implemented the FISA amendments and effectively removed the wall between intelligence and criminal investigations; and an opinion issued by the FISA Court of Review in May 2002 that held FISA permitted the use of intelligence in criminal investigations and that coordination between criminal prosecutors and intelligence investigators was necessary for the protection of national security.[3]

Taken together, these changes clearly established that the Criminal Division could play a much more active role in the FBI's intelligence investigations than in the past. The changes were also reflected in the Department's October 2003 Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. The Guidelines require the broad information-sharing practices between the FBI and the Department's Criminal Division and OIPR that we recommended in our Hanssen Report. The FBI is now required to provide the Criminal Division and OIPR notices of the initiation of foreign intelligence and counterintelligence investigations, annual notices and summaries concerning active investigations, and to "make available to the Criminal Division and [OIPR] relevant information from investigative files." The Guidelines further provide that the FBI, Criminal Division, and OIPR "shall consult with each other concerning national security investigations and other activities under these Guidelines, and shall meet regularly to conduct such consultations."

As part of this follow-up review, we interviewed the Chief of the Department's Counterespionage Section. He told us that as a result of the changes in the law and FBI practices, there is now a partnership between his section and the FBI. The Chief said that the FISA Court of Review decision was accompanied by a change in senior management at the FBI that brought officials who were willing to coordinate with the Counterespionage Section and who were more receptive to the Section's guidance. He also said that attorneys in the Counterespionage Section now regularly provide agents with advice on investigations. The Chief told us that he does not have any concerns regarding the current relationship between his section and the FBI and believes it is working as it should. The FBI's Assistant Director for the Counterintelligence Division shared this assessment of the current relationship between the FBI and Counterespionage Section.

---

[3] In June 2006, the OIG publicly released a report that includes a detailed examination of the creation of the wall separating criminal and intelligence investigations. The report, entitled *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks* (November 2004), is available on the OIG's website at http://www.usdoj.gov/oig/special/s0606/index.htm.

The assessments we received of the relationship between the Counterespionage Section and the FBI indicate that our recommendation that Criminal Division personnel be full participants in counterintelligence investigations has been addressed. We believe that this collaboration should help build better cases by ensuring that evidence collected will be admissible in court.

B. Recommendation No. 4: More Substantive Role for OIPR Attorneys

Our Hanssen Report recommended that OIPR have a larger oversight role in reviewing the factual assertions in the FBI's FISA applications and have direct access to the case agent and the source information relied on in the application. OIPR represents the United States before the FISA Court and prepares FISA applications on behalf of the FBI.[4] Particularly during the 1990s, OIPR attorneys had to draft so many FISA applications that they could not devote much time to any particular case. Instead, they relied on the information provided by the FBI and rarely questioned the accuracy or strength of the FBI's representations. The FBI, in turn, selectively provided information to OIPR, tended not to volunteer facts that reflected negatively on the investigation, and generally did not consult with OIPR on substantive investigative decisions. Furthermore, OIPR's contact person at the FBI was the FBI Headquarters Supervisory Special Agent assigned to the case, not the case agent. As a result, many of the FISA applications submitted in cases we reviewed during our original Hanssen review omitted critical facts.

In 2001, the Attorney General and the FBI established new procedures that encouraged direct contact between OIPR attorneys and FBI field office personnel on FISA applications and that required case agents to review draft affidavits in FISA applications for accuracy. Consistent with these changes, in our Hanssen Report we recommended that OIPR play a more substantive role in reviewing the FBI's FISA-related investigations by being provided full access to all aspects of the FBI's investigation, including the entire case file and results from prior FISA applications. As we noted above, the October 2003 Attorney General's Guidelines provide for the broad information sharing and consultation our recommendation urged.

In this follow-up review, we interviewed the Counsel for OIPR and the FBI's Deputy General Counsel for the National Security Law Branch (NSLB) to assess the implementation of our recommendation and the impact of the

---

[4] OIPR was merged into the Department's National Security Division, which was created by the reauthorization of the Patriot Act in March 2006. The new National Security Division consists of the Counterterrorism and Counterespionage Sections, the Office of Intelligence Policy and Review, and a new Law and Policy Office.

October 2003 revisions to the Attorney General's Guidelines.[5] While both officials told us that OIPR has in fact taken a more substantive and active role in reviewing FISA applications, the OIPR Counsel's assessment of this progress was mixed. He told us that our recommendation matched his expectation of what OIPR should be doing in the FISA process, but that OIPR still has the occasional fight with the FBI to get full access to information, particularly information pertinent to the reliability of sources relied on in FISA applications.

While the OIPR Counsel stated that OIPR attorneys should be involved in FISA-related investigations, he also noted several factors working against his office's ability to play the substantive role we recommended. These included a "staggering" volume of work and insufficient staffing, the occasional difficulty for the mostly Washington, D.C.-based OIPR attorneys to establish cooperative and trusting working relationships with case agents located in FBI field offices throughout the country, and the natural tension between OIPR's oversight and intelligence-gathering functions and the FBI's interest in investigation that can cause the FBI – as well as prosecutors – to resist OIPR's substantive involvement in cases.

From the FBI's perspective, the NSLB Deputy General Counsel said that when she joined the FBI in October 2004 she was told the relationship between OIPR and the FBI was a "work in progress." She said that her priority, and that of her operational counterparts at the FBI, has been to improve the FISA process by introducing objective measures of performance and developing a team approach between the FBI and OIPR to address problems. She also told us that she believes the relationship between NSLB and OIPR attorneys is very good on a personal level, and she pointed to activities that have facilitated this, such as a joint training seminar held by NSLB and OIPR and an approximately year-long period during which OPIR attorneys were co-located with NSLB attorneys and FBI agents at the National Counterterrorism Center located in Northern Virginia.

The NSLB Deputy General Counsel acknowledged that disagreements still arise with OIPR, but she believes the FBI has taken steps to resolve some of the specific disputes. She also told us that she does not believe that the natural tension that exists between NSLB and OIPR causes the FBI to resist OIPR's involvement in investigations.

In our view, the relationship between the FBI and OIPR was redefined by the October 2001 Patriot Act, the November 2002 Court of Review opinion, and the October 2003 Attorney General's Guidelines, and information sharing and meaningful consultation is now the rule rather than the exception. According

[5] The NSLB serves as the FBI's in-house counsel in matters between the FBI and OIPR. The Counterintelligence Division works with OIPR through NSLB.

to both OIPR and the FBI, OIPR attorneys are taking a more substantive, assertive role in investigations and the FBI has implemented new practices that facilitate the OIPR attorneys' oversight responsibility in ensuring accuracy and fairness in FISA applications. We believe that these actions address our recommendation.

V. Improving Source Recruitment, Security, and Handling

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

In the Hanssen Report, we noted that the recruitment of human assets in hostile intelligence services is the most valuable tool for identifying moles in the Intelligence Community. As a result, we believe that source recruitment should always be a major priority for the FBI. However, our Hanssen review found that for over two decades the FBI's financial and resource commitment to source recruitment was inconsistent. At times, little meaningful source recruitment activity had occurred, while during other periods the FBI had dedicated an entire squad of agents to the task and worked closely with other agencies in joint recruitment efforts. We therefore recommended that the FBI expand its recruitment program, coordinate its activities with the CIA and other Intelligence Community components, and focus on intelligence officers in hostile intelligence services who are likely to have knowledge of penetrations of the U.S. Intelligence Community.

The information contained in the FBI's response to this recommendation is classified and therefore we have not included it in this executive summary. Generally, the FBI's response identified several initiatives designed to improve source recruitment and highlighted source recruitment-related training that was developed by the FBI's Counterintelligence Training Center.

As part of our follow-up review, we interviewed the Assistant Director for the FBI's Counterintelligence Division to discuss the status of the FBI's new source recruitment efforts. He told us that the FBI's emphasis on source recruitment has increased with the dramatic changes that have taken place in the Counterintelligence Division. The number of agents assigned to the division has grown significantly since September 11, 2001, and growth is expected to continue. The Assistant Director also told us that he believed that counterintelligence work has been transformed from the FBI's unwanted "stepchild" to a coveted assignment, and that the counterintelligence program has grown from a cluster program in a limited number of offices to a nationwide, proactive program represented by a counterintelligence squad in each of the FBI's 56 domestic field offices.

Based on our review, it appears the FBI is making significant progress in implementing this recommendation. Through a combination of increased and improved source recruitment training, the existence of joint recruitment and detection programs with other intelligence agencies and services, and the enhanced profile of and resources allocated to its Counterintelligence Program, the FBI appears to be taking seriously the critical role source recruitment plays in its ability to detect penetrations of the U.S. Intelligence Community.

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

We also recommended that the FBI adopt stricter standards for handling and tracking sensitive information from significant human sources and vigorously enforce the "need to know" policy in disseminating information from such sources. We found during our Hanssen review that for two decades the FBI's investigation of potential FBI moles and unexplained asset losses had been handicapped by its inability to account for and track this category of information. Apart from considerations regarding espionage investigations, success in source recruitment and retention also depends in part on the proper handling of source information.

We also noted that after the arrest of Aldrich Ames, the CIA developed a new special information handling system to protect its most sensitive human intelligence sources. The system, called the Human Intelligence Control System, or HCS, requires special handling procedures that limit the dissemination of, and control access to, sensitive source information. To avoid the incongruity of the same human sources being given different levels of protection by two agencies within the Intelligence Community, we recommended in our Hanssen Report that the FBI adopt HCS. We believed this measure could be an important step in remedying the FBI's longstanding problem concerning the improper dissemination of sensitive source information.[6]

In response to our recommendation, the FBI stated that it "supports the principle that HCS material within the Intelligence Community should be afforded consistent levels of protection throughout the Community." In furtherance of this principle, the FBI has developed stricter standards for handling and tracking sensitive human source information received from other agencies.

---

[6] The Commission for the Review of FBI Security Programs, commonly referred to as the Webster Commission for its Chairman, William H. Webster, made the same recommendation in its March 2002 Review of FBI Security Programs report.

However, the FBI has told us that it is not considering adopting HCS for its own source information of comparable sensitivity. Instead, the FBI reported that it has implemented "a business model which significantly modifies existing practices to address operational security reviews and assessments and ensure stricter standards for handling and tracking sensitive information from all FBI [Confidential Human Sources]." The FBI told us that it employs more human sources than any other Intelligence Community agency and that this business model is an effective and appropriate approach.

Our follow-up review recognized the FBI's ongoing efforts with the Human Intelligence Reengineering Project, which we were told would "enhance and improve the administration and operation of the FBI's Human Source Program." It is not clear to us whether the business model identified in the FBI's response to our draft report is part of the reengineering project, is a complementary effort to that project, or is a different approach entirely. Thus, while we remain encouraged that the FBI is making efforts to improve its handling of sensitive source information, those efforts clearly are still in the developmental stage and the OIG could not fully assess their adequacy at this time.

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

Because of problems we found in the Hanssen case concerning the FBI's handling of sources, we recommended that the FBI adopt guidelines for handling active recruitments-in-place and recent defectors that would, among other things, limit the disclosure of sensitive information – such as details of ongoing espionage investigations – to these sources. To the extent practicable, there should be a one-way flow of information from the source to the debriefer. By sharing information with a source, debriefers risk contaminating future reporting from the source and jeopardizing the security of the operation discussed. The loyalties of sources that are not under the FBI's complete control also may change over time, or their activities on the FBI's behalf may be detected, leading to interrogation that could result in the disclosure of information the FBI provided. Moreover, in the event a source becomes a witness in a criminal trial, such disclosures could undermine the credibility of the source.

The FBI's response stated that the FBI concurs with our recommendation and has incorporated explicit guidance on this subject in the FBI's classified revised guidelines for human sources, which we were provided access to as part of our follow-up review. In addition, the FBI reported that the guidance is included in training given to Special Agents at various stages of their careers.

It appears the FBI is taking seriously the importance of establishing clear guidance on the subject of sharing investigative information with sources. We

believe that the combination of the explicit language contained in the revised guidelines for human sources, together with the enhanced training identified by the FBI, addresses our recommendation.

VI. Security Improvements

A. Recommendation No. 8: Central Repository for Derogatory Information

We recommended that the FBI create a central repository for the receipt, collection, storage, and analysis of derogatory information concerning FBI employees with access to sensitive information. We recommended that information or allegations that reflect on the integrity, suitability, or trustworthiness of an FBI employee should be documented and transmitted to this repository for analysis, and that the repository should be directly accessible to counterespionage personnel responsible for determining whether the FBI has been penetrated. A central repository would help ensure that derogatory information is collected in one location for analysis and, if warranted, investigation.

The FBI's written responses to our recommendation, as well as interviews we conducted during this follow-up review, addressed FBI efforts in the areas of information technology and organizational structure that were relevant to establishing such a central repository. We found that both efforts are works in progress.

The FBI's Security Division is in the early stages of developing an information technology architecture, called the Security Management Information System (SMIS) that it states will serve as the "backbone" for the division's automation efforts and facilitate information sharing among the division's components and potentially across FBI divisions. One official described SMIS as essentially a tool to manage workflow, facilitate information sharing, and provide enhanced security. The official told us that the FBI's goal under SMIS is to automate and integrate by 2012 the FBI's business processes identified within the Security Division. Some of these processes have already been automated, while others are in various stages of development. In September 2006, the FBI awarded the SMIS integration contract to a consulting firm and is presently completing an "integrated master project schedule" that will identify, prioritize, and track each automation project through 2012. The consulting firm is responsible for building the enterprise architecture for the Security Division and integrating the automated business processes into that architecture.

If SMIS is deployed successfully, the FBI will have an automated network that contains the categories of personnel information that we would expect to

be relevant to the central repository for derogatory information that our Hanssen Report recommended. Financial information, polygraph results, security incident histories, background reinvestigation documents, facility access records, and foreign travel and contact forms are among the types of personnel information that are essential for any meaningful review of an employee's activities. We were told that these categories of information will be automated (some already are) and that the technical capability to search the information through SMIS will exist.

The organizational arrangement the FBI identified in response to our recommendation is also a work in progress. The FBI told us that derogatory information regarding FBI and non-FBI personnel is collected and analyzed through an arrangement among several components across three FBI divisions. These components are responsible for distinct but related personnel security matters, such as security incidents, failed polygraphs, anomalous finances, and allegations of misconduct. We were told that there is regular, formalized interaction among these components (including the penetration unit we described in Recommendation No. 1) with the goal of sharing derogatory information on matters raising potential security and espionage concerns.

However, we concluded based on our follow-up review that the FBI needs to establish written procedures to govern this information-sharing arrangement. We found that the current arrangement lacks sufficient clarity and standards concerning the sharing of information and relies too heavily on the personal relationships of the components' current managers. In particular, we found there was insufficient assurance that the FBI's penetration unit will ever be alerted about certain matters that are handled by Security Division components and that much of the reporting of information to the penetration unit is discretionary.

In sum, the FBI has not yet established a fully functioning central repository to receive, collect, store, and analyze derogatory information concerning FBI employees with access to sensitive information. While SMIS can provide a powerful tool for FBI components responsible for analyzing and investigating derogatory personnel information, this technology is in the early stages of development. Similarly, while we found that the several components currently responsible for analyzing derogatory employee information are making good faith efforts to coordinate their activities, we believe the FBI must still develop and implement information-sharing standards and requirements to ensure that derogatory information will be properly collected, analyzed, and investigated.

B. Recommendation No. 9: Documentation of Security Violations

We recommended that the FBI create policies and procedures designed to ensure that security violations are reported, documented in an employee's

security file, and properly investigated and resolved. We stated that a database should be created to track security violations by employees and identify patterns and trends. We also recommended that the FBI conduct regular security awareness training of its personnel that includes clear instructions regarding the reporting of security violations. These recommendations were based on our findings in the Hanssen Report that numerous security incidents and breaches by Hanssen were never documented, in either Hanssen's personnel or security file, and (with one exception) were not reported to the FBI's Office of Professional Responsibility, the FBI Security Programs Manager, or any other central location for review and consideration of disciplinary action. We found that the FBI historically lacked a centralized reporting program for violations, and failed to issue policies defining what constitutes a security violation, what procedures should be followed when security violations are discovered, and what remedial actions or discipline should be imposed regarding security violations.

In response to our recommendation, the FBI stated that in August 2002 the Security Division created the Security Compliance Unit to "address security incidents within the Bureau." In March 2003, the Security Compliance Unit created the Security Incident Program, which it now administers. According to the FBI-wide communication announcing the establishment of the program, under past practices security incidents were reported only if they caused actual damage. In addition, damage assessments conducted in response to a reported security incident focused only on the harm caused, and typically did not address any policy or training gaps that might have contributed to the incident. The communication stated that the Security Incident Program was created to rectify the FBI's inability to track all security incidents committed by employees and contractors, identify patterns in improper security practices, and determine what corrective action might be appropriate, such as additional training or a change in policy. In August 2003, the Security Compliance Unit issued preliminary reporting protocols for the Security Incident Program, which were later expanded and incorporated into the FBI's September 2005 Security Policy Manual.

The Security Compliance Unit is also responsible for ensuring that reported security incidents are investigated properly. This involves the unit conducting its own inquiry, directing the responsible Chief Security Officer to conduct an inquiry, or referring the incident to another FBI component for investigation. The Security Compliance Unit is additionally responsible for conducting or requesting damage assessments and recommending, as necessary, remedial action for security incidents, such as security awareness training.

FBI efforts to automate the Security Incident Program are ongoing. Currently, the only automation is an incident database created using Microsoft Access software to help prepare the monthly and quarterly security reports the

Security Compliance Unit is required to provide to FBI executives. However, we were told that as of October 2006, the FBI had funded the automation project for the Security Incident Program and selected a contractor to develop the software. Unit management hopes the automated process – to be called the Security Incident Reporting System – will be operational by the end of fiscal year 2007.

In our judgment, the creation of the Security Compliance Unit, and the Security Incident Program it administers, represents a significant improvement in the FBI's ability to effectively collect and respond to security incidents. The unit has established well-defined reporting and investigative protocols. In addition, the Unit Chief has developed cooperative working relationships with counterparts in other relevant units which, in the absence of an electronic network for information sharing, are a critical component of an effective reporting program. It also appears that the Security Compliance Unit has expended significant effort with the resources it has available to educate FBI employees, and in particular Chief Security Officers, about the unit and the Security Incident Program.

C. Recommendation No. 10: Meaningful Background Reinvestigations

In our review of Hanssen's espionage activities, we found that he was subject to only one background investigation during his 25-year career at the FBI, and that issues raised during this investigation regarding his finances and contacts with a Russian defector were never pursued or resolved. The reinvestigation did little more than complete a "checklist" of items before making a favorable security determination; it did not substantively analyze Hanssen's risk.

The FBI made several changes to its reinvestigation program in response to the Hanssen case, including transferring the adjudication function for reinvestigations from the National Security Division to the newly created Security Division and establishing a unit responsible for ensuring that anomalies that arise during background reinvestigations are analyzed, investigated, and resolved.

We recommended additional changes to further improve management of the background reinvestigation program. First, we recommended that the FBI transfer the investigative function for reinvestigations to the Security Division in order to fully consolidate the program under one division. The FBI has done this.

Second, we recommended that the FBI install an automated case management system to capture, store, and facilitate the analysis of personnel security information. The FBI's progress in this area has been limited. A

software application that had been under consideration since 2003 was recently determined to not be a viable technology for the FBI. In addition, while we were told the Security Division has made the personnel security process its top automation priority and that some aspects of the process have already been successfully automated, substantial work remains to complete an automated case management system for personnel security information.

Our Hanssen Report also made several specific recommendations regarding the conduct of background reinvestigations, such as providing the principal background investigator with access to all relevant source materials, including the subject employee's personnel file, security file, and financial information; interviewing any FBI relatives and the spouse or roommate of the subject employee; verifying the employment of the subject employee's spouse; and requiring the subject employee to identify non-FBI references for interview.

We learned during our follow-up review that a recent change in applicable federal guidelines significantly affected the conduct of background reinvestigations and, consequently, the FBI's implementation of our recommendations. These guidelines, issued by the Director of Central Intelligence, are called the *Investigative Standards for Background Investigations for Access to Classified Information.* The guidelines establish investigative standards for individuals who require access to classified information and "are to be used by government departments and agencies as the investigative basis for final clearance determinations." In December 2004, the guidelines were amended to eliminate the requirement for interviews of references and neighbors as part of an employee background reinvestigation, unless security concerns are raised by other sources of information, such as credit reports.

The FBI adopted the amended investigative standards in March 2005 and consequently no longer conducts reference or neighborhood interviews, and also does not go beyond the investigative sources required under the guidelines (including the employee subject interview, criminal history, and credit reports) unless security concerns are raised during the reinvestigation. The FBI told us that it adopted the new requirements in order to address the growing backlog of reinvestigation cases. The FBI reported that it "has made significant strides in reducing the overall backlog, thus allowing a more intensified review of the anomalous cases."

We recognized that the amended reinvestigation standards reflect the collective judgment of the personnel security community, and we have no basis to believe that the standards are unreasonable. However, we believe the amendments do not obviate the need for further action in response to our recommendations. We suggested, for example, that reinvestigations include interviews of any FBI relatives and the spouse or roommate of the subject, verification of the spouse's employment, and the requirement that the subject

list non-FBI references for interview. These are important sources of information and should still be considered in any enhanced reinvestigation the FBI conducts.

We also recommended that each reinvestigation subject be assigned a principal background investigator with full access to all relevant source materials. While reference and neighborhood interviews have been eliminated in most cases, the reinvestigation guidelines still require interviews of the subject employee and work colleagues. We were told these interviews are typically conducted by the Chief Security Officers assigned to the employees' field office or division; however, the Chief Security Officers currently are provided only the subjects' reinvestigation security questionnaire – completed by the subjects – to prepare for the interviews. We still believe the FBI should implement our recommendation that Chief Security Officers be given access to all relevant source materials to ensure meaningful and thorough interviews of subject employees and work colleagues.

Finally, we observed during our follow-up review that with the amendments to the reinvestigation standards it is now even more critical that the FBI have a staff of professional, well-trained Personnel Security Specialists to detect security concerns and identify appropriate follow-up investigation. We did not find that the FBI has achieved this level of expertise. We were told that expertise levels for Personnel Security Specialists are not high at this time and that, in one senior manager's judgment, there are not enough Personnel Security Specialists to handle the volume of work. The Security Division has taken steps to address the training deficiency and is working to "professionalize" the Personnel Security Specialist position to attract strong candidates and retain skilled employees. We are encouraged that senior management recognizes the critical need for more Personnel Security Specialist training, and we recommend that the FBI devote the resources necessary to continue developing a more professional and knowledgeable Personnel Security Specialist staff.

D. Recommendation No. 11: Financial Disclosure Program

We recommended that the FBI implement an annual, computer-based financial disclosure program for employees with access to sensitive information. We found during our review of Hanssen's espionage that he was never required to complete a detailed financial disclosure form. As a result, Hanssen, like Aldrich Ames, was able to safely invent stories about family wealth and successful investments to explain his spending. Analysis of his bank accounts would have revealed a flood of cash for which Hanssen had no explanation. During interviews after his arrest, Hanssen himself identified meaningful financial disclosure and analysis as the security technique that would have provided the greatest deterrent to his espionage.

In response to Hanssen's arrest, the FBI implemented a Financial Disclosure Program in August 2003. The program, which was approved by the Attorney General and is administered by the Security Division's Analysis and Investigations Unit, applies to all employees and contractors with Sensitive Compartmented Information (SCI) access and is intended to "identify personnel with unexplained affluence or who are financially overextended and potentially at risk for becoming a target of espionage." The program is supported by software that performs the collection and preliminary analysis of financial information.

While the Financial Disclosure Program technically applies to all employees and contractors with SCI access, it has been implemented gradually. In October 2003, the FBI's Senior Executive Service (SES) was the first group of employees required to file the new Financial Disclosure Forms. According to the FBI, this group served as a pilot test for the program. The program has since expanded significantly. In 2006, all employees with SCI access from FBI Headquarters, Legal Attaché offices, and several field offices were required to file Financial Disclosure Forms – currently approximately 10,000 employees in total, according to the Assistant Section Chief for the Personnel Security Adjudication Section. In 2007, the FBI plans to continue expanding the program to additional field offices, and by 2008 hopes to have all 19,000 employees with SCI access filing Financial Disclosure Forms.

In our view, the FBI has made considerable progress implementing our recommendation. The program is fully automated and the pace of expansion over the past several years has been significant. Provided the program is adequately funded and there are not delays, we believe the FBI will likely meet its 2008 goal of having the Financial Disclosure Program cover all FBI employees holding SCI access.

E. Recommendation No. 12: Random Counterintelligence Polygraph Program

We recommended that the FBI fully implement a counterintelligence polygraph program for employees with access to sensitive information, and develop a similar program for non-FBI personnel who are given access to sensitive information. Prior to Hanssen's arrest, the FBI had no mandatory polygraph program for onboard employees, and Hanssen was never required to undergo a polygraph examination despite his extraordinary access to sensitive operations from across the U.S. Intelligence Community.

Hanssen's 2001 arrest prodded the FBI to significantly expand its polygraph program for security matters beyond pre-employment examinations. In April 2002, the FBI Director approved expansion of the polygraph program to include a counterintelligence-focused polygraph examination as part of the 5-year background reinvestigation for onboard employees assigned to the

Counterintelligence, Counterterrorism, and Security Divisions. In August 2003, the FBI added to the program a random polygraph examination for these employees. According to the September 2005 Security Policy Manual, the program now applies to all FBI employees.

The FBI has also added non-FBI personnel – such as task force members and contractors – to its polygraph program for initial clearance and access to FBI information and space. According to the OIG's September 2006 report, *Use of Polygraph Examinations in the Department of Justice*, between 2001 and 2005 the number of FBI and non-FBI personnel subject to mandatory random and periodic testing under the FBI's Personnel Security Polygraph program increased from 550 to 18,384.[7] The FBI conducted a total of 4,721 personnel security polygraph examinations from fiscal year 2002 through 2005. As part of our Hanssen follow-up review, the FBI reported that it has increased the number of random polygraph examinations it administers annually.

In sum, the FBI has made significant progress in expanding its security polygraph program. We believe that, in particular, the random component of the program is a critical tool for deterring future espionage and other misconduct involving national security information. In our judgment, by steadily increasing the number of random examinations conducted and educating FBI and non-FBI personnel regarding the polygraph requirement, the FBI will strengthen the examination's deterrent effect.

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

We recommended that the FBI consider enhanced security measures for employees who enjoy unusually broad access to sensitive information. During his FBI career, Hanssen served in a series of positions that offered him this kind of access. Hanssen's position in the Soviet Analytical Unit, in particular, provided him with access not only to sensitive FBI information, but to large quantities of classified information from a variety of Intelligence Community components. However, while serving in this and other positions, Hanssen was subject to no greater scrutiny than FBI employees who had much less access to sensitive information.

Our recommendation was based on the principle that personnel security requirements should not be uniform, but should reflect differences in the levels of access that individuals enjoy. Individuals who have unusually broad access to sensitive information should receive greater scrutiny than employees who do

---

[7] See *Use of Polygraph Examinations in the Department of Justice*, Evaluation and Inspections Report I-2006-008, September 2006. A public version of this report is available on the OIG website at www.usdoj.gov/oig/reports.

not have this degree of access. We recommended that this principle be extended more broadly and suggested more frequent polygraph examinations, more frequent and thorough background reinvestigations, and more detailed financial disclosures as examples of possible enhanced security measures.

In this follow-up review, we found that the FBI has made credible progress implementing our recommendation. The FBI highlighted the random counterintelligence polygraph program and the Financial Disclosure Program, both implemented in August 2003, as measures the agency has taken to enhance security for persons with unusually broad access to sensitive information. (These programs are described in the preceding two sections of this executive summary.) As we discuss in the next section of this summary, the FBI also has developed and deployed significant monitoring capabilities for its primary information systems. In addition, the FBI implemented in October 2002 a program called the Post Adjudicative Risk Management (PARM) program. The program is designed to manage and, where possible, mitigate the elevated risk associated with an employee's inconclusive or deceptive polygraph results or anomalous financial activity.

We believe that these security enhancements are important components of a successful internal security program and that they represent improvements in the FBI's security program.

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

We recommended that the FBI implement measures to improve computer security, including (1) a third-party audit program to detect and give notice of unauthorized access to sensitive cases on a real-time basis; (2) an audit program designed to detect whether employees or contractors are using the FBI's computer systems to determine whether they are under investigation; (3) procedures designed to enforce the "need to know" principle in the context of computer usage; and (4) a program designed to ensure that restricted information cannot be improperly accessed through the use of security overrides or other means.

This recommendation reflected the significant security deficiencies we identified, both in our Hanssen Report and in other OIG reports, with the Automated Case Support (ACS) system, the FBI's principal computer-based case management tool. These deficiencies included employees' failure to use the ACS system's cumbersome auditing capability, vulnerabilities created by an access override feature in the ACS system, and FBI users' lack of knowledge and training in how to use the ACS system. In addition, we found that sensitive information was often uploaded into the ACS system without appropriate restrictions, and that FBI agents viewed the ACS system as so

insecure that they were unwilling to upload sensitive information onto the system.

Our 2003 Hanssen Report found that the FBI had made only limited progress in resolving the flaws in ACS in the two years following Hanssen's arrest. In its July 2003 response to the review, the FBI stated that "attempting technical changes to improve ACS security would not be a smart business decision" in light of plans to implement the automated case management system known as the Virtual Case File, or VCF. We observed in our Hanssen Report that until the FBI rectified the security flaws evident in the ACS system, its most sensitive computer-based information would remain vulnerable to unauthorized access and compromise.

In January 2005, the FBI abandoned the VCF effort. An OIG audit of the project found that VCF failed for a variety of reasons, including poorly defined design requirements, lack of mature technology investment practices, and poor management continuity and oversight.[8] The FBI's current information technology project to replace VCF and add additional capabilities is called Sentinel and is presently under development, with a four-phase implementation schedule that anticipates full operational capability by December 2009. At the request of the FBI Director and congressional appropriations and oversight committees, the OIG is conducting a series of audits to monitor the progress and implementation of Sentinel. Our third and most recent audit was completed in August 2007.[9]

In light of VCF's failure, our Hanssen follow-up review examined the progress, if any, the FBI had made in addressing the security deficiencies in ACS that we identified in our original Hanssen Report. The FBI considers much of its effort in this area highly sensitive. In particular, the FBI has classified the specific monitoring capabilities it has deployed for FBI information systems, as well as additional measures the FBI has taken to address other information security deficiencies. In general, we found that the FBI has made considerable progress in improving the security posture of ACS and other FBI information systems. We also found that the FBI has taken sensible steps to address some of the specific security deficiencies exploited by Hanssen. However, we also found that ACS continues to suffer from inadequate user training and certain inherent technical vulnerabilities that are the focus of ongoing FBI efforts.

---

[8] See *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Audit Report Number 05-7, February 2005. A public version of this report is available on the OIG website at www.usdoj.gov/oig/reports/FBI/a0507/index.htm.

[9] See *Sentinel Audit III: Status of the Federal Bureau of Investigation's Case Management System*, Audit Report 07-40, August 2007. A public version of this report is available on the OIG website at www.usdoj.gov/oig/reports/FBI/index.htm.

H. Recommendation No. 15: Tracking Classified Information

We recommended that the FBI create and implement a program enabling it to account for and track hard copy documents and electronic media containing classified or sensitive information. We suggested that the 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. We also recommended that the FBI develop a program to prevent the improper copying of classified information.[10]

The FBI's initial responses to this recommendation stated that the FBI was "in the process of identifying funding for a contract that will devise, implement and refine improved levels of security provided to the FBI's sensitive and classified information, including paper documents," and that "unauthorized efforts to access digital information will be detected by [the Enterprise Security Operations Center], and appropriate responsive investigative and mitigation efforts implemented."

However, during the course of our follow-up review the FBI told us that it had re-evaluated its approach to accounting for and tracking hard copy documents and stated that the new approach, which it said reflects the Intelligence Community's move toward a digital environment, "will focus on controlling access and tracking of documents from the point of creation rather than investing limited resources into a paper based solution." The Assistant Director for the FBI's Security Division told us that a fixation on paper ignores the reality that the most sensitive information can be carried in an employee's head and feels the FBI's resources are better spent on digital, rather than paper, technologies to control and track the flow of sensitive information. The Unit Chief for the FBI's Information Assurance Technology Unit, who joined the FBI after working for over 30 years in the information technology systems and communications security fields, shares the Assistant Director's view and told us that to the best of his knowledge there is no viable technological solution to controlling every sensitive piece of paper at the FBI.

While the FBI is not pursuing a tagging solution to control FBI information, the Assistant Director and other managers within the Security Division told us that the FBI is significantly changing how it protects classified and unclassified FBI information. In July 2003, the FBI completed its first-

[10] Our Hanssen Report highlighted several steps the FBI took to improve document security following Hanssen's arrest, such as establishing security and sanitization requirements for the use of commercial copiers to duplicate classified information and improving SCI security by creating an SCI Program Manager position. The FBI has included these and other security requirements and procedures in its Security Policy Manual, which is available to all employees on the Security Division's intranet site.

ever Information Assurance Program Plan.[11] The goal of this plan is to integrate all aspects of information security so that it will grow and adjust as information systems gain new capabilities, products, and users. The strategy is effectuated by applying "layers" of security, such as information assurance plans, policies, and procedures; continual enterprise risk assessment; increased and enhanced security training, education, and awareness for information system users; information assurance implementation, management, and oversight by a staff of information security professionals; engineering and new technologies designed to counter threats to FBI information and information systems; and enterprise security operations that will monitor FBI information systems for internal and external threats.

A full examination of the FBI's Information Assurance Program would have exceeded the scope of our follow-up review. However, we concluded that the FBI has made important progress under the program that demonstrates positive change in the FBI's approach to handling sensitive information. Examples include demonstrable improvements in security training, education, and awareness; movement toward professionalizing the staff of information security specialists deployed throughout the FBI; and the deployment of new technologies to counter threats to FBI information and information systems.

Overall, we believe the FBI has made progress in its approach to protecting information and information systems. The Information Assurance Program is an ongoing, complex, and ambitious effort. We also believe that the FBI's approach has benefited from hiring and contracting with security and information technology professionals from private industry and other government agencies. We are mindful, however, that the Information Assurance Program must overcome a well-documented history of FBI security deficiencies. We believe that if the FBI is to succeed in creating the secure digital environment described to us by Security Division managers, sufficient resources must be committed to the effort. We also observe that a major focus of our recommendation in the Hanssen Report – Hanssen's ability to walk out of FBI Headquarters with classified documents undetected – is not addressed by the Information Assurance Plan. We recognize this is a difficult security issue faced by every federal agency that handles sensitive national security information, but we also believe it is a vulnerability that warrants attention even as the FBI moves toward a digital environment.

I. Recommendation No. 16: Security Compliance Program

We recommended that the FBI implement a security inspection program which ensures that deficiencies in security are detected and remedied within a

[11] Information Assurance refers to the technical and managerial measures designed to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

reasonable period of time. The security compliance program in effect during Hanssen's career did not ensure that classified national security information held by the FBI was properly safeguarded. Despite repeated findings by the Justice Department's Security and Emergency Planning Staff, the FBI Inspection Division, and the OIG, the FBI did not remedy serious security deficiencies. Moreover, recommendations for security changes and improvements were not tracked and periodically reviewed to determine whether the FBI was responsive to recommendations for remedial action.

The FBI has addressed its failure to develop a centralized security structure by consolidating its security programs into a single division, appropriately named the Security Division. Within this division, the Security Compliance Unit is responsible for ensuring that security deficiencies are detected and remedied. The Security Incident Program is the primary tool for meeting this responsibility by establishing how security incidents at the FBI are defined, reported, documented, investigated, and remedied.

The Security Compliance Unit also is responsible for monitoring compliance with corrective actions for security deficiencies identified in internal audits of FBI field offices and Headquarters divisions. These audits, known as Security Programs Management (SPM) Audits, are conducted by a Chief Security Officer and are a component of the FBI Inspection Division's reviews – which are conducted on 3-year cycles – of operational and administrative functions of field offices and Headquarters divisions. The SPM Audits assess compliance with FBI security requirements, and where deficient, prescribe corrective actions. Audit results are forwarded to the Security Compliance Unit and are assigned to a Security Specialist responsible for monitoring compliance with the prescribed corrective actions. We were told that the Inspection Division cannot close a security matter as resolved until the Security Compliance Unit indicates it is satisfied with the corrective action taken.

For external reviews of FBI operations – such as the Webster Commission Report or the OIG's Hanssen Report – the Strategic Planning and Coordination Unit of the Mission Support Section is responsible for tracking compliance with recommendations. According to the Section Chief for the Mission Support Section, recommendations are integrated into the Section's Strategic Plan as either short-term or long-term goals depending on the scope of the recommendation and the anticipated work required for implementation. Progress is regularly monitored and that part of the Section's quarterly performance review includes evaluating the status of the recommendations' implementation.

We believe the FBI has made significant progress toward a viable security compliance program by implementing the Security Incident Program, improving how security audits are conducted, designating the units responsible for

compliance issues, and establishing procedures for tracking and ensuring compliance.

J. Recommendation No. 17: Improving Security Education and Awareness

We recommended that the FBI make the implementation of an FBI-wide security education and awareness program a top management priority, and that the status of employee security training be tracked and monitored. In our Hanssen Report, we found that many security weaknesses stemmed from training deficiencies in such areas as ACS security controls, the requirements for handling classified materials, and properly recognizing, reporting, and documenting security violations.

In its response to our Hanssen Report, the FBI identified several measures taken to improve security education and awareness and gave the OIG a list and description of security training provided in fiscal years 2004-2006 to FBI employees, contractors, and task force members. The FBI told us that the Security Division created the Security Policy, Education, and Training Unit to develop security training programs based on an "integrated approach . . . designed to address issues across security disciplines, especially with regard to information assurance, document control, and classification markings." In addition to the examples of formal security training, the FBI reported that the Security Division implemented other initiatives designed to improve security awareness and knowledge, such as the weekly distribution of security awareness tips to all employees, the expanded production and distribution of security awareness brochures and pamphlets, and the creation of an informational website.

The FBI also reported that the Security Division devoted significant resources to implementing a Chief Security Officer Program. Designed to "develop a professional security staff and achieve credibility within the U.S. Government and Intelligence Community," the program established a Chief Security Officer position in each FBI field office and Headquarters division to serve as the senior security representative. The Security Division introduced a Basic Security Officers Course in 2003 and has since implemented an Intermediate Security Officers Course. In addition, the FBI is developing an Advanced Security Officer Training Course and Chief Security Officer certification program.

We believe the FBI has taken seriously the need for a more comprehensive security education, awareness, and training program. In our view, the combination of increased formal training, regular security reminders and updates, the availability of an informational website, and the presence of a trained and visible security officer in each office will contribute to a security-conscious environment where employees are less likely to commit security

violations and more likely to report observations of improper or suspicious activity. We recommend that the FBI continue these efforts and, in particular, devote the resources necessary to sustain a professional, well-trained, and highly visible Chief Security Officer program.

However, we are not as encouraged by the FBI's security efforts related to the FBI's most glaring, and oft-cited, training deficiency: users' lack of knowledge regarding ACS. In our 2003 Hanssen Report, we cited examples of employees who did not know how to use ACS and were unaware of its security controls, and others who never received training on the system's audit function or on how to create access restrictions to cases. We also noted that previous OIG reports had alerted the FBI to the fact that agents were not adequately trained to utilize the ACS system.

The FBI currently has one official ACS Training Instructor and no centralized ACS training program. We were told that until approximately 2003, there was a 20-person unit responsible for providing training to FBI personnel on ACS and other information systems. At some point in 2003, ACS training for field offices was discontinued because a new case management system called the Virtual Case File (VCF) was expected to replace ACS (new agent classes at the FBI Academy in Quantico, Virginia, continued to receive training in ACS). The training unit was then dissolved as a result of a reorganization of FBI training programs and personnel. Today, there is no unit responsible for conducting ACS training and there is only one ACS training instructor for all new agent and new analyst classes at the FBI Academy. This same training instructor is also responsible for providing ACS training to FBI field offices, but has not been able to do so in the past 2 years despite receiving regular requests. While some field offices and FBI Headquarters divisions have ad hoc ACS training programs for new hires, there is no coordination of this effort by the FBI's Training Division.

Our Hanssen Report stated that "[w]e cannot overemphasize how vital it is for the FBI to rectify the security flaws that have been evident in the ACS system for many years. Until these weaknesses are corrected, the system remains insecure and vulnerable to attack." The lack of ACS training is one of the flaws we identified, and the FBI's continued failure to adequately train its employees on its most widely utilized information system is troubling. Without a uniform, comprehensive training program, ACS's significant security features will continue to be ignored or underutilized, and an environment susceptible to employee error or abuse will persist. Given the recent experience with VCF, we believe the FBI must reinvigorate and enhance ACS training for its employees while ACS remains in operation as Sentinel's development and implementation continues.

VII. Management and Administrative Improvements

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

We recommended that FBI supervisors guard against excessively deferring to line personnel when supervising significant espionage investigations and ensure that the Department of Justice is properly briefed on the strengths and weaknesses of potential espionage prosecutions. In our Hanssen review and our earlier review of the FBI's performance in the Aldrich Ames case, we saw a tendency on the part of FBI supervisors to excessively defer to line personnel concerning how espionage investigations should be conducted.

In response to our recommendation, the FBI identified two fundamental changes to improve the exercise of managerial authority over espionage cases. First, the FBI centralized the management of counterintelligence cases at FBI Headquarters. The August 2002 National Strategy for Counterintelligence called for the FBI to move toward "a centrally controlled and managed FCI [Foreign Counterintelligence] Program that guides, directs and provides adequate resources to support an effective national FCI Program." The FBI also reported that supervision over espionage matters is emphasized at various training venues, such as Special Agent in Charge counterespionage executive conferences and counterintelligence supervisor seminars, and in counterintelligence briefs given to agent and support personnel attending courses at the FBI's Counterintelligence Training Center.

The second change that the FBI believes has improved the exercise of managerial authority over espionage cases is the reform the FBI implemented in response to the focus on information sharing after the September 11 attacks. As briefly summarized in Sections IV.A. and B. of this executive summary, the relationship between the FBI and the Department of Justice was redefined by the October 2001 Patriot Act, the November 2002 FISA Court of Review opinion, and the October 2003 revisions to the Attorney General's Guidelines. The FBI reports that increased information sharing and increased oversight by the Justice Department's Counterespionage Section have improved the FBI's management of espionage cases.

We believe that the centralization of management of espionage cases, combined with a more cooperative relationship with the Department, will result in FBI supervisors not excessively deferring to case agents, in accord with our recommendation. We also believe that the improved relationship with the Department makes it more likely case agents' analytical and investigative judgments in counterespionage cases will be adequately scrutinized.

B. Recommendation No. 19: Damage Assessments for FBI Spies

We also recommended in the Hanssen Report that damage assessments for FBI employees who have committed significant espionage should be led by experienced counterintelligence personnel and be conducted by an Intelligence Community entity, such as the National Counterintelligence Executive (NCIX). This recommendation addressed our criticism of the FBI's decision to conduct a unilateral damage assessment of the espionage of former FBI Special Agent Earl Pitts, ignoring a request from the National Counterintelligence Center (the precursor to NCIX) to conduct the assessment.

By statute, the NCIX is now responsible for oversight and coordination "of strategic analyses of counterintelligence matters, including the production of counterintelligence damage assessments and assessments of lessons learned from counterintelligence activities." The FBI's response to our recommendation recognized NCIX's statutory responsibility for overseeing counterintelligence damage assessments and referenced the Hanssen damage assessment conducted by NCIX as an example of the FBI's compliance with the statute. We were also told that NCIX is conducting the damage assessment relating to Aragoncillo's activities. Therefore, we believe that the FBI has addressed this recommendation.

C. Recommendation No. 20: Recusal Procedures for FBI Employees

We recommended that the FBI adopt recusal policies and procedures for FBI employees and supervisors who may be suspects in an espionage investigation. In conducting the Hanssen and Ames reviews, we encountered supervisors who stated that they had been unwilling to influence the course of certain espionage investigations because of a concern that they might be suspects.

The FBI told us that they believed such policies were already in place but not formally documented. The FBI addressed this on October 1, 2003, by implementing a formal disqualification policy for national security investigations involving FBI employees. The policy sets forth the procedures "by which FBI personnel are to be disqualified from participation in, or from gaining knowledge of, an investigation, and by which authority may be obtained to read potential suspect pool candidates into an investigation or to allow them to be involved in an investigation." This policy requires that "no FBI employee may participate in an investigation in which he or she is a suspect or otherwise has an interest in the outcome," and establishes recusal procedures for any such employee.

During our follow-up review, we found that the policy could be improved by providing guidance about what constitutes an employee who "otherwise has

an interest in the outcome." We were concerned that this broad, undefined phrase would be susceptible to inconsistent interpretation and application. In response to the draft report of our follow-up review, the FBI revised the language to read "or is judged by field office or Headquarters supervisory personnel to have a close, personal relationship with a suspect employee."

We believe this revision clarifies the guidance to FBI personnel overseeing espionage investigations.

D. Recommendation No. 21: Supervision of FBI Detailees

We recommended that the FBI ensure that FBI detailees serving in other Intelligence Community components are properly supervised and receive regular performance evaluations. We found that Hanssen did not receive any meaningful supervision or performance reviews during the 6-year period (1996-2001) that he was detailed to the State Department's Office of Foreign Missions. This lack of supervision allowed Hanssen to spend hours on his computer conducting defensive searches of the FBI's electronic files to ensure he was not the subject of an espionage investigation, and to obtain and download vast amounts of sensitive information from the computer system that he later passed to the Russians.

The FBI's response to the recommendation stated that in January 2001 it established reporting requirements for FBI detailees serving in other Intelligence Community agencies, including semiannual progress reviews and "After Action" reports addressing the purpose of the assignment and related accomplishments, impediments, and areas for improvement. The FBI also said that detailees have routine contact with their FBI rating officials and that the Assistant Director for the Counterintelligence Division meets bi-monthly with all detailees to discuss Intelligence Community issues. In addition, the FBI established a central point-of-contact at FBI Headquarters to maintain regular contact with the detailees and ensure compliance with the reporting requirements. The information compiled by the point-of-contact is reviewed by senior FBI management on a regular basis.

We believe that the procedures identified by the FBI, if followed, adequately address our recommendation and will help ensure that FBI detailees are properly supervised and receive regular performance evaluations.

VIII. The Aragoncillo Matter

In this section of the report, we discuss the case of Leandro Aragoncillo. We include this case in our report because of similarities between Aragoncillo's conduct and Hanssen's espionage activities, and their relevance to our

assessment of the FBI's progress in improving its counterintelligence and internal security programs.

Aragoncillo worked as an FBI Intelligence Analyst from July 11, 2004, to September 10, 2005. Prior to this, from July 1999 to April 2002 he served in the Office of the Vice President as a staff assistant to the military advisors for the Vice President. From these two positions, Aragoncillo unlawfully obtained and passed classified documents and information to current and former Philippine government officials.

On September 10, 2005, the FBI arrested Aragoncillo. Early reports about the matter indicated that Aragoncillo's conduct bore some resemblance to Hanssen's, including the improper use of the FBI's ACS system, and that the case demonstrated missed opportunities by the FBI to uncover the conduct earlier. We learned more information during our follow-up review about the Aragoncillo case, and it became clear that several aspects of the matter were relevant to our assessment of the FBI's implementation of the Hanssen Report recommendations. We therefore reviewed aspects of Aragoncillo's hiring and employment with the FBI to assess their relevance to the FBI's progress in implementing the recommendations from our Hanssen Report. To conduct this review, we obtained Aragoncillo's FBI personnel and security files and documents from the FBI's criminal investigative file on Aragoncillo. We also interviewed Aragoncillo's FBI colleagues and supervisors, as well as personnel in the FBI's Security Division knowledgeable of Aragoncillo's hiring and related personnel security issues.

We set forth in detail our factual findings and analysis of the Aragoncillo matter in the classified version of this follow-up review. In sum, we found that despite the FBI's stated policies in response to our recommendations, the Aragoncillo matter reveals mixed progress in the FBI's actual implementation of its responses to some of these recommendations, as well as in its efforts to establish a reliable and effective internal security program across the agency. We found that Aragoncillo's conduct should have been detected and investigated significantly earlier than it was and that his conduct was finally uncovered only as a result of inquiries made by another federal agency.

We provide below a summary of the factual background of the Aragoncillo matter. We then summarize what we believe the Aragoncillo matter illustrates about the FBI's progress in implementing specific recommendations in our Hanssen Report.

A. Summary of Factual Background

1. Aragoncillo's FBI background investigation

On April 20, 2003, Aragoncillo applied to the FBI for one of three Intelligence Analyst positions located at the FBI's Fort Monmouth Information Technology Center (FMITC) in New Jersey.[12] In January 2004, Aragoncillo was interviewed telephonically by an interview board of three FMITC employees. Based on his background and relevant work experience, the interview board unanimously selected Aragoncillo and two others for the openings. The selections were approved by the Chief of the FMIITC, and on February 23, 2004, the FBI made Aragoncillo a conditional offer of employment pending successful completion of a background investigation, polygraph examination, and drug test.

The background investigation included a pre-employment personnel security interview, a review of and interviews concerning Aragoncillo's military background and work history, criminal records checks, and interviews of references. The FBI did not receive or identify any derogatory information concerning Aragoncillo from these sources of information. However, the credit report for Aragoncillo obtained by the FBI on March 23, 2004, indicated a significant level of indebtedness. In addition, the credit report indicated that a substantial payment was made to a creditor in February 2004, just six months before Aragoncillo joined the FBI. The credit report did not list any incidents of late payments or other negative information.

The FBI did not conduct any additional investigation concerning Aragoncillo's finances based on the credit report. Instead, according to the analysis contained in Aragoncillo's security file, "[a] review of [Aragoncillo's] credit report disclosed no pertinent information."

Aragoncillo was given a polygraph examination on April 26, 2004. Aragoncillo was asked, among other questions, whether he had ever disclosed classified information to an unauthorized person. Aragoncillo answered "no" to this and the other questions. According to FBI records, the examination found no indications of deception.

On June 9, 2004, the FBI approved Aragoncillo for a Top Secret security clearance. According to the communication reporting this determination, Aragoncillo was not eligible for access to Sensitive Compartmented Information, or SCI, because he had relatives (two siblings) who were not U.S. citizens. The

---

[12] The FMITC provides investigative, analytical, and technical support to FBI investigations and operations. Intelligence Analyst responsibilities include reviewing financial, telephone, travel, and other types of records to assist FBI agents in field offices and at FBI Headquarters.

standards governing the SCI program require that immediate family members of the individual being considered for SCI access must be U.S. citizens.[13]

2. Aragoncillo's employment with the FBI

Aragoncillo began work with the FBI on July 11, 2004, as a GS-9 Intelligence Analyst. Aragoncillo's training curriculum included FBI security matters and covered topics such as handling classified information, the "need to know" principle, and information that should be reported to the FMITC Security Officer. Fellow analysts told the OIG that Aragoncillo generally was considered friendly but somewhat arrogant and ingratiating. FMITC records state that he was an excellent trainee who appeared eager and capable. According to his training records, Aragoncillo quickly learned how to use ACS and other information systems and began working independently during the training period.

When Aragoncillo entered on duty with the FBI, he was granted access to various FBI and other government agencies' classified and unclassified databases needed to perform his job as an intelligence analyst. On August 23, 2004, Aragoncillo completed an SCI Security Questionnaire used to determine whether he was eligible for SCI access. In response to the question, "Do you have any immediate relatives (spouse, parents, siblings, children, or cohabitants) who are not U.S. citizens?", Aragoncillo falsely responded that he did not. The questionnaire was sent to FBI Headquarters for an eligibility determination. Eligibility was approved on August 30, 2004, and Aragoncillo was briefed into the SCI program on October 14, 2004, despite the FBI's explicit written determination during his background investigation that Aragoncillo was ineligible for SCI access because he had non-U.S. citizen relatives.[14]

Aragoncillo's training program ended in mid-October 2004. Shortly thereafter, Aragoncillo began engaging in conduct that his training instructor considered improper or inappropriate. For example, Aragoncillo began to regularly ask his training instructor and another senior analyst about projects they were working on and what various cases were about. Aragoncillo's questions violated the need to know principle. The analysts reminded Aragoncillo of this, advised their supervisor of the issue, and asked the Security Officer to review the need to know principle with Aragoncillo and the other new analysts.

---

[13] The term "Immediate family" is defined as the spouse, parents, siblings, children, and cohabitant of the individual requiring SCI access.

[14] The regulations governing the SCI program provide that an exception to this requirement can be made upon "certification of a compelling need." There was no evidence that anyone requested that Aragoncillo be granted SCI access on this basis.

Aragoncillo's training analyst also considered Aragoncillo's use of his personal cell phone excessive and highly unusual. He rarely placed or received calls on his office phone and always left the workspace to use his cell phone. She observed that Aragoncillo's cell phone rang every day at 6:50 a.m. and that he promptly left the workspace to receive the call. Most of the conversations the analyst heard were in Tagalog, Aragoncillo's native language. Other analysts made similar observations. Aragoncillo's cell phone usage was brought to the attention of his supervisor on multiple occasions, but the concerns were dismissed because the supervisor did not consider the usage unusual.

Then, on November 5, 2004, an analyst walking past Aragoncillo's cubicle observed on his computer monitor the results of an ACS search with the terms "Philippines" and "corruption" highlighted, indicating that Aragoncillo entered the words into ACS as search terms. The analyst told us that she was "shocked" when she saw the screen because she knew that the analysts in Aragoncillo's group worked on terrorism cases and also because she was aware Aragoncillo was Filipino. She shared what she saw with two co-workers, and they agreed that she should report her observation to the Security Officer, which she did that same day.

The analyst told the Security Officer that Aragoncillo was viewing ACS information regarding public corruption in the Philippines. She told the Security Officer she was concerned because Aragoncillo had just returned from visiting family members that reside in that country. The Security Officer wrote in a memorandum documenting the meeting, "[the analyst] just wanted to tell someone since everyone is more cautious about viewing information after the 'Hansen' [sic] case."

According to the Security Officer's memorandum, he provided the analyst the following response to her concerns:

> I told her that I doubted that there was any concern here; [sic] because; [Aragoncillo's] terminal faces out into the room and anyone who walks by his desk can see what he is viewing. If you were going to view documents that do not pertain to your case load, I don't believe he would do it in such a public atmosphere. I also told her that he would probably have had access to more information than what we have on file here at his former position in the White House. I told her I would monitor the situation for further complications.

While the analyst recalled that the Security Officer told her there was an audit log for ACS activity that could be reviewed to find out what Aragoncillo was looking at, the Security Officer told us that he never considered conducting an ACS audit of Aragoncillo's usage. He said that he did not believe the

analyst's concerns warranted that action, despite Aragoncillo's connection to the Philippines. He told us, however, that his assessment might have been influenced by Aragoncillo's background as a U.S. Marine and his work at the White House. The Security Officer said he "monitored the situation" by walking through the work space a couple of times to see if he could observe anything out of the ordinary, but he did not see anything unusual. The only other action taken by the Security Officer in response to the analyst's concerns was to memorialize the meeting for "historical information" in case anything else concerning Aragoncillo ever came to his attention.

Aragoncillo began improperly using ACS to obtain information regarding the Philippines in September 2004, just over a month before the analyst reported her observations to the Security Officer. Aragoncillo's activity on ACS continued for another eight months until it was uncovered by the FBI in July 2005.

3. FBI investigation of Aragoncillo

On March 18, 2005, U.S. Immigration and Customs Enforcement (ICE) contacted the FBI's New York office to inquire about Aragoncillo's involvement in an immigration matter concerning Michael Ray Aquino, a former high-ranking Philippine police official who was later prosecuted with Aragoncillo as a co-conspirator for theft of FBI information. The ICE inquiry was referred to the FMITC, which immediately contacted ICE for additional information. The FMITC learned that Aquino was arrested by ICE agents on March 7, 2005, for overstaying his visa and that Aragoncillo became involved in the matter at the request of Aquino's wife following the arrest. Aragoncillo attended a meeting between ICE agents and Aquino's attorney on March 8, 2005, during which time he identified himself as an FBI employee, displayed his official identification, and also advised of his former employment at the White House. ICE stated that Aragoncillo gave the impression that the FBI was involved in the matter, and that Aragoncillo had contacted ICE numerous times over the course of the next week to inquire about the status of Aquino's case.

After being advised of these and other details, the FMITC immediately informed the FBI's Security Division of the ICE inquiry and sought guidance regarding how to proceed. In a communication sent to the Security Division providing details regarding "a possible personnel security issue which may include improper conduct," the FMITC raised several specific concerns, including whether Aragoncillo had conducted searches of FBI or other Intelligence Community databases and passed information to foreign government officials, and whether he had interfered with another agency's investigation. The FMITC did not conduct its own audit at that time because it believed approval from FBI Headquarters' Security Division was required. The FMITC made several inquiries to the Security Division about how to proceed

after the communication was sent, but was told not to take any action until contacted by investigators.

The FMITC Security Officer was present during the call between the FMITC and ICE about Aragoncillo's involvement in Aquino's immigration case, and he helped draft the communication from the FMITC to the Security Division reporting the matter and requesting guidance about how to proceed. Yet, despite this first-hand involvement, the Security Officer never drew any connection between the ICE inquiry and the concerns raised just four months earlier by an analyst who saw evidence of Aragoncillo using ACS to search "Philippines" and "corruption." The Security Officer acknowledged to us that he should have made such a connection, but did not do so until three months later. In the interim, Aragoncillo's improper use of ACS and other databases continued undetected.

On March 21, 2005, the Security Division informed the FMITC that the Aragoncillo matter had been referred to the Security Division's Analysis and Investigations Unit. From there, the matter was referred to the Inspection Division's Internal Investigations Section as a potential non-security related misconduct matter. On April 11, 2005, a formal administrative inquiry was initiated into the allegation that Aragoncillo misused his position with the FBI for the gain or advantage of an associate. Over the next two months, the FBI agent assigned to the case interviewed ICE personnel and Aragoncillo. The investigation was delayed by approximately three weeks because Aragoncillo took previously scheduled leave to the Philippines during most of June 2005. Aragoncillo returned on July 5 and signed his sworn statement explaining his involvement in Aquino's immigration matter on July 8.

During the period between Aragoncillo's interview on June 2 and the signing of his statement on July 8, the Chief of the FMITC learned for the first time that in November 2004 an analyst had reported to the Security Officer that Aragoncillo might have misused ACS. The Chief immediately sent an e-mail to the Security Officer asking for additional information. The Security Officer responded that same day – June 23, 2005 – and described the November 2004 meeting he had had with the analyst. This was the first time the Security Officer made the connection between the reported ACS misuse and Aragoncillo's involvement in the immigration matter.

The next day the Chief of the FMITC forwarded his exchange with the Security Officer to the agent conducting the administrative inquiry, stating, "It seems like we dropped the ball on this in a big way." The Chief recommended that an ACS audit be conducted and that Aragoncillo be asked whether he used ACS for unofficial purposes.

From this point, events unfolded quickly. A preliminary ACS audit was conducted for the period from March 1, 2005, to March 31, 2005. The results

indicated that Aragoncillo was conducting ACS queries outside the scope of his official duties, including regular searches of his name. On July 6, 2005, the Chief of the FMITC forwarded what he characterized as "very disturbing" results to the Analysis and Investigations Unit and to the agent conducting the administrative inquiry. On July 8, 2005, prior to Aragoncillo signing his sworn statement, he was asked whether he had searched FBI databases for information concerning Aquino and a Philippine senator. Aragoncillo falsely stated that he had not.

Also on July 8, 2006, a more expansive ACS audit was conducted for the period from April 21, 2005, to July 7, 2005. The results indicated that Aragoncillo had downloaded or printed 106 classified and unclassified documents from the FBI and other government agencies that were unrelated to any of his official duties. Aragoncillo reportedly viewed on ACS many times this number of documents. These results were forwarded to the Analysis and Investigations Unit, which in turn notified the Counterespionage Section's penetration unit. That section took the lead coordinating the investigation, and on July 13, 2005, a formal counterespionage investigation was opened.

Through a variety of investigative techniques, the investigators quickly determined that on a daily basis Aragoncillo was obtaining and providing his co-conspirators with classified and unclassified information pertaining to the Philippines. Most of the information was obtained from ACS. Occasionally using pseudonyms and code words, the information was transmitted to his co-conspirators by hand, e-mail, facsimile, and orally over the telephone. Aragoncillo provided, for example, documents containing national defense information relating to confidential U.S. intelligence sources and terrorist threats to U.S. military personnel in the Philippines. Some of the documents Aragoncillo provided identified the confidential sources for the information contained in the documents.

On September 10, 2005, the FBI arrested Aragoncillo and on May 4, 2006, he pled guilty to four federal charges: conspiracy to transmit national defense information, transmission of national defense information, unlawful retention of national defense information, and unauthorized use of a computer. Aragoncillo stated during his plea hearing that he committed the crimes out of a sense of loyalty to his place of birth, the Philippines. He said that he provided some of the documents and information because he believed it would be helpful to the efforts of his co-conspirators to destabilize and remove the current government of the Philippines. On July 18, 2007, Aragoncillo was sentenced to 10 years in prison and fined $40,000.

B. Summary of the OIG's Analysis of the Aragoncillo Matter

1. Recommendation Nos. 1 and 8: New Penetration Unit and Central Repository for Derogatory Information

In response to our recommendations that the FBI create a single unit to investigate internal espionage matters and establish a central repository to collect and analyze derogatory personnel information, the FBI described an arrangement among a number of components with related personnel security responsibilities that is intended to leverage specific expertise and establish a system for information sharing. We expressed concern during our follow-up review about how this unwritten arrangement was working in practice. The Aragoncillo matter tested the effectiveness of this arrangement and, in our view, the results were mixed.

We found that after the ACS audit finally was conducted in July 2005, and Aragoncillo's activities became apparent, the components' response was swift and effective. The FMITC reported the audit results immediately to the Security Division and to the agent conducting the administrative inquiry of Aragoncillo. That same day, the Security Division notified the Counterespionage Section's penetration unit about the case, which in turn immediately began coordinating the espionage investigation. From that point, these three units each played distinct but cooperative roles.

Where the arrangement was ineffective, in our judgment, was in the 3-month period between March 2005 when the FMITC first notified the Security Division about Aragoncillo's involvement in an immigration matter, and July 2005 when the FMITC notified the unit about the ACS audit results. We concluded that the information contained in the communication from the FMITC to the Security Division raised significant security concerns that clearly fell under that division's responsibility to investigate security violations. We also believe the Security Division should have reported the information to the Counterespionage Section to assess whether the alleged conduct had indicia of espionage warranting investigation. At a minimum, the Security Division should have caused an ACS audit to be conducted and contacted its Security Compliance Unit to seek records of any other security incidents committed by Aragoncillo. Yet, these steps were not taken and the matter was instead referred to another division as a potential misconduct case.

The consequence of the decision was that Aragoncillo's activities remained undetected for an additional three months. We highlight this aspect of the FBI's response to Aragoncillo because it demonstrates how the current arrangement the FBI describes as its solution to detecting internal penetrations can fall short. It also reinforces our belief that the FBI must institutionalize the arrangement to ensure that the lines of responsibility and coordination are

clear and that information is shared as a matter of course and not as a matter of discretion.

2. Recommendation No. 9: Documentation of Security Violations

The FBI created a Security Compliance Unit to administer the Security Incident Program, which is intended to identify patterns in improper security practices and determine what corrective action might be appropriate. The program defines a "security incident" as a failure to safeguard material in accordance with FBI policies, and a "security violation" as any incident that results in the "actual loss, compromise, or suspected compromise of classified national security information, or unclassified information." The FBI's Security Policy Manual provides that Security Officers should report security violations to the Security Compliance Unit through the Security Incident Program.

The analyst's report of Aragoncillo's possible misuse of ACS constituted a security incident that, at a minimum, should have been reported to the Security Compliance Unit by the FMITC Security Officer because it concerned an allegation of a suspected compromise of sensitive information. The Chief for the Security Compliance Unit told us that one reason for this reporting requirement is to ensure that incidents are investigated properly. If the FMITC Security Officer had reported the alleged incident, an analyst in the Security Compliance Unit likely would have recommended conducting an ACS audit. The FMITC Security Officer had completed all of the required Security Officer training and had attended security conferences where the Unit Chief for the Security Compliance Unit made presentations about the Security Incident Program. Yet, the Security Officer did not act in accordance with his training in this matter.

3. Recommendation No. 10: Meaningful Background Reinvestigations

We believe that the recent changes to federal background reinvestigation standards heighten the important role played by the FBI's Personnel Security Specialists in the analysis of personnel security information. As discussed previously, we have concerns about the current level of expertise within the ranks of the Personnel Security Specialists and urge the FBI to enhance the training provided.

The Aragoncillo matter provides two glaring examples of our concern. First, the specialist assigned to assess Aragoncillo's eligibility for a Top Secret security clearance determined that his credit report "disclosed no pertinent information." The Security Division acknowledged to us that this assessment was inadequate and that Aragoncillo's significant level of indebtedness should have received additional scrutiny.

Second, Aragoncillo was granted SCI access despite the fact that, according to the regulations governing the SCI program, he was ineligible for such access by virtue of having non-U.S. citizen immediate family. Aragoncillo's ineligibility was expressly noted in his security file, but the specialist responsible for approving his SCI access apparently took no steps to verify Aragoncillo's responses on his SCI Questionnaire.

We do not know whether Aragoncillo would still have been hired or his espionage prevented if the Personnel Security Specialists had performed their jobs competently. While we are not aware of any evidence that Aragoncillo received significant sums of money for providing documents and information to his co-conspirators, we do not know what additional investigation concerning his finances might have uncovered. Similarly, we do not know whether an inquiry into the conflict between Aragoncillo's statements in his SCI Questionnaire and those he provided during his background investigation might have uncovered additional derogatory information. However, the failures in the personnel security process should not have occurred. The fact that they did reinforces the importance of establishing a skilled and well-trained staff of Personnel Security Specialists.

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

We found during our follow-up review that the FBI has made progress in improving the security of its information systems. However, as noted above, the FBI's primary case management system – ACS – remains vulnerable to the improper accessing of cases and information by authorized users. Aragoncillo conducted searches daily, without detection, on ACS for documents and information for which he had no need to know. He was also able to print and download information from ACS at will. We believe the Aragoncillo matter reinforces the critical importance of the FBI's ongoing efforts to improve the security of FBI information systems.

5. Recommendation No. 17: Improving Security Education and Awareness

The Aragoncillo matter provides evidence that the FBI's program to improve security education and awareness among employees is making progress. The FMITC employees we interviewed appeared to take their security responsibilities seriously. They also told us that generally they believe their Security Officer has done a sound job of promoting security awareness and ensuring that employees comply with facility and personnel security regulations. The employees' security awareness was evident in the observations by other analysts regarding Aragoncillo's behavior and the reporting of concerns to Aragoncillo's supervisor and to the Security Officer.

Ironically, it was the response to an employee's reported concern that we found deficient. The Security Officer's response to Aragoncillo's ACS usage was clearly deficient and his failure to connect this incident with the ICE report concerning Aragoncillo's involvement in an immigration matter was perplexing. While we do not know whether this example of failure to adhere to the reporting requirements under the Security Incident Program and lack of knowledge concerning authority to conduct ACS audits is representative of FBI Security Officers at large, we recommend that the FBI highlight these subjects at Security Officer training programs and conferences.

IX. Conclusion

In conclusion, we believe the FBI has made significant progress in implementing many of the recommendations from our Hanssen Report. However, in several areas the FBI's record is mixed, and it has not implemented some critical recommendations, such as creating a central repository to receive, collect, store, and analyze derogatory information concerning FBI employees. In addition, the FBI has only recently decided to fully implement others, such as establishing a penetration unit whose sole responsibility is to assess potential FBI penetrations. We believe the FBI must continue to address these issues and remain vigilant in attempting to deter and detect the internal penetrations that are likely to occur in the future. We believe that full implementation of our recommendations can help the FBI in this effort.

APPENDIX A

HANSSEN REPORT 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 FBI 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 Program

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.