

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

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

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.

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

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.

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.

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

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 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

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.

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.

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.

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.

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

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.

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

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.

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

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

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

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.

APPENDIX A

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. 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.