Testimony of

Mr. Kenneth H. Senser

April 9, 2002

Good morning Chairman Leahy, Senator Hatch and other members of the Committee. I spoke to you initially on July 18, 2001, about our analysis of the FBI Security Program and the work we are doing to transform our internal security operation into one fully capable of addressing the diverse and formidable threats facing the Bureau. I am very pleased to be back again to provide the Committee with an up-date regarding the FBI's progress on this matter and to commend the comprehensive and extraordinarily helpful work performed by Judge Webster and his Commission on the Review of FBI Security Programs.

Your continued interest in ensuring that the FBI operates in a secure environment is much appreciated because without the support of Congress, this badly needed transformation would not be possible to complete. We also commend Judge Webster and his Commission for the extremely detailed and independent review of the FBI's internal security program. The product of their efforts will serve the FBI well as a measuring stick on where we need to be on the multiple fronts that affect our internal security. When then Director Freeh and Attorney General Ashcroft asked Judge Webster to undertake this critical task, our hope and expectation was exactly as he and the Commission delivered, i.e., a comprehensive and brutally candid assessment of where we are and where we need to be. It will be our roadmap.

As I mentioned in previous testimony, prior to the arrest of former Special Agent Robert P. Hanssen for espionage, the FBI had taken some limited steps to improve its Security Program, a program that was fragmented, dispersed across several different divisions and substantially inadequate in a number of respects. The Program lacked an integrated vision and security initiatives were often poorly coordinated, inefficient, and not effective. Succinctly put, security, other than physical security, was not inculcated into the culture as a priority that must be practiced, observed and improved upon everyday. Additionally, as I testified previously, the FBI identified in early 2000 seven areas within the Security Program requiring greater focus. Through his recommendations, Judge Webster provides specific and sound guidance on each area.
Since my July testimony, two other United States citizens have been arrested for espionage -- Brian P. Regan, a former member of the Air Force assigned to the National Reconnaissance Office, and Ana Belen Montes, an employee of the Defense Intelligence Agency. Additionally, on September 11th, members of Al Qaeda conducted a heinous act of terrorism against the United States. These actions validate the premise that there are adversaries of the United States that will stop at nothing to harm the interests of this country. The FBI, our many employees and the sensitive information in our files are attractive targets for a wide variety of opponents who continuously strive to impede investigative operations, obtain that sensitive information, and initiate and implement reprisal actions against Bureau personnel or facilities. For all of these reasons, I will confine my public remarks to a more generic description of the progress made by the FBI and I would be pleased to provide the Committee with a more comprehensive briefing in a closed session.

Webster Commission Recommendations

Judge Webster identified the need for extensive improvement throughout the FBI's internal Security Program. His report concludes that there are serious deficiencies in most security elements analyzed in the course of the study. Some of the identified vulnerabilities are more critical than others and represent a more significant level of risk to the security of FBI operations. The Commission grouped its recommendations into the following categories:

? Organizational Structure
? Information Systems Security
? Personnel Security
? Document Security

A review of the vulnerabilities serving as the basis for the Commission's recommendations provides traceability to the original seven critical areas previously identified by the FBI as badly in need of improvement. While of little consolation, the Commission found no others. That does not, however, mitigate the severity of the shortcoming that had developed over the years or the urgency that must attach to fixing these problems. With that we are in total agreement with Judge Webster.

Since Hanssen's arrest in February 2001, the FBI has been engaged in a dedicated effort to transform its Security Program and we very much appreciate the help and guidance of Judge Webster's staff regarding these efforts. The severity of the shortcomings and corresponding vulnerabilities dictated that we proceed even while this outside review was ongoing. Because of their help, the two efforts were complimentary, which allowed much progress to be made. As Judge Webster points out, much more progress is still required. The Webster Commission report and recommendations will be an extremely valuable tool in this process.

The remainder of this statement will be devoted to bringing the Committee up-to-date on what has already been accomplished and a brief description of the additional Security Program improvements we plan on making in the future, guided, of course, by the recommendations and observations reflected in the report.

Status of the Interim Security Improvements

In late March 2001, former Director Louis J. Freeh took a number of internal security-related actions designed to immediately improve the internal security of the FBI. These steps included the appointment of a task force of Assistant Directors (ADs) to ensure the complete identification and effective implementation of the interim security improvements, the removal of the Security Program from the National Security Division (NSD) and its establishment as a stand-alone entity reporting to then Deputy Director Thomas J. Pickard, my appointment as the executive manager responsible for the direction of the Security Program, and the adoption of a detailed security policy process.

The following additional interim security changes were initiated:

Enhanced Computer Audit Procedures: The Webster Commission report describes how Robert Hanssen easily compromised the information contained on approximately 26 computer diskettes, representing about 6000 pages of material, much of it obtained through his exploitation of a critical FBI investigative database, the Automated Case Support (ACS) system. Hanssen did not need to "hack" inside the computer system. His "legitimate" permissions allowed him to surf the system and find information of value to support his continuing espionage.

Shortly after Hanssen's arrest, former Director Freeh instructed our personnel to implement regular reviews on our most sensitive cases -- reviews that can highlight all individuals who have looked at the case files -- so that the case agents and their supervisors can be responsible for assuring these cases are being accessed by only those with a need to know. A process was established, using the regular file review mechanism whereby agents discuss investigative progress with their supervisors every 90 days, to review the Document Access Report within the Electronic Case File segment of ACS. Through this review, case agents assigned to the most sensitive investigations are responsible for resolving potential unexplained accesses.

Initiation of this process is an excellent start, but remains inadequate. One major shortcoming of ACS is the complexity of its operation and the lack of user friendliness. The Webster Commission report highlights that while ACS contained these case audit and tracking tools from its inception, few users knew they were available or did not understand how to access them. Ultimately, this vulnerability will be mitigated through the implementation of a new case management system called the Virtual Case File (VCF) and the application of robust Information Assurance (IA) principles which will be described in greater detail below. Both of these were discussed at a recent hearing before this Committee. With the funding Congress has provided, the FBI will make a giant leap forward on both managing information and managing the security of information.

To address this issue until the VCF and IA Program is viable, the FBI's Information Resources Division developed a user friendly application called the Case Document Access Report (CDAR) which will facilitate the case auditing process and provide the case agent and his or her supervisor more oversight capabilities. The CDAR has just finished the certification and accreditation process, required of all new software applications, and deployment will begin soon. In conjunction with this deployment, more focused education and awareness will be provided to ACS users on the security associated with the ACS investigative database.

Expanded Polygraph Program: During the course of Hanssen's Bureau career, he never took a polygraph examination. In 1994, the FBI established a requirement to test all new employees prior to them beginning their service. Additionally, individuals with access to certain sensitive programs or cases were polygraphed and it was also used during serious internal inquiries to resolve unexplained anomalies and ambiguities.

Former Director Freeh ordered after Hanssen's arrest periodic polygraph examinations for those individuals, who by the nature of their assignment, have broad access to our most sensitive information. Polygraph examinations were also ordered for those employees serving in overseas assignments.

Since the limited polygraph expansion became effective, close to 700 counterintelligence (CI) - focused examinations have been conducted. While the initial population of employees occupying positions with access to the most sensitive information was estimated to be close to 550, this population is dynamic. For example, as employees have retired, new incumbents for these positions were chosen and, ultimately, polygraphed. The vast majority of employees who were polygraphed have successfully completed the process. We are continuing to work with slightly more than one percent of the tested population to resolve anomalies. We developed a process for attempting to resolve anomalous outcomes which takes into account the fact that polygraph is only one element of a healthy personnel security vetting program and assures that, while it may be necessary to modify the sensitivity of an employee's access to information during the inquiry, no adverse action will be taken against the employee based on polygraph results alone. While no admissions have been surfaced during the polygraph examinations to date that are of a seriousness equivalent to that of the Hanssen case, the process has identified lesser security transgressions and other behavior that has resulted in referrals to the FBI's Office of Professional Responsibility (OPR) for appropriate disciplinary considerations. This is a necessary component of changing to a culture of security awareness.

FBI Director Robert S. Mueller, III, recently agreed to a new risk-based framework for the Polygraph Program and slightly expanded the pool of employees subject to CI-focused examinations. I will discuss this in greater detail later in my statement.

Enhanced Reinvestigation Analysis: The Webster Commission report identified a number of issues that surfaced during Hanssen's 1996 security reinvestigation that should have been recognized as "red flags." Statements were made by some references that did not appear to have been pursued by investigators and there was no indication that security clearance adjudication personnel did much more than complete a "check list" when deciding to favorably rule on the case. There were other questionable incidents during Hanssen's career that were never integrated into a rigorous analytical process which could have resulted in a decision to further scrutinize his trustworthiness.

Former Director Freeh mandated in March 2001 that an enhanced analysis capability within the Security Program be established to conduct security adjudications and to resolve any anomalies resulting from the reinvestigations of persons with access to the most sensitive information. We established a separate unit within the Security Program for this purpose. The unit also serves as the point for CI-security integration. It is staffed by an agent Unit Chief and two agent supervisors. Fourteen contractors (retired FBI agents) are conducting analysis. Additional staff resources have been allocated to establish an enhanced financial analysis capability. Their mission is simple: ensure that pieces of information that are potential "red flags," regardless of how disparate they may be, get fully analyzed, investigated and resolved in an expeditious fashion. That did not happen in the past.

As with the expanded use of polygraph, we have identified some security transgressions via the enhanced analysis process and other behavior that has resulted in referrals to the OPR. Additionally, in at least one instance, this new unit identified poor operational practices that could have negatively impacted our ability to conduct effective CI investigations. As a result of this discovery, remedial actions were taken. Again, these referrals, while addressing individual

shortcomings, are an important part of changing the culture to one that accepts security and security awareness as a fundamental element of conducting the business of the day.

Other Measures Implemented: During my testimony in July 2001, I described a number of other initiatives directed by former Director Freeh to facilitate the continued incorporation of security into the FBI culture so that it is recognized as an integral part of operations. These initiatives included:

? Elevating the role of the Security Officer in the field by requiring that they have a direct reporting capability to the Assistant Directors in Charge or Special Agents in Charge.
? Requiring that each Assistant Director in Charge or Special Agent in Charge establish a Security Council.
? Developing and conducting training for FBI employees and, in relation to job-specific requirements, Security Officers.
? Receiving security expertise and support from the Intelligence Community.
? Improving the security of Sensitive Compartmented Information (SCI).

Significant additional progress was made in these areas as well as others since July. This progress will be further developed later in my statement.

Status of the Transformation of the FBI Security Program

I previously described to the Committee the fragmentation and disarray of the FBI Security Program which were captured in the seven critical focus areas. The Webster Commission report clearly illuminates the degree to which security was "broken". If there was ever any question, it should now be obvious that what is required is not a "band aid" approach, but a complete transformation of the Security Program. During the July testimony, the Committee learned about a prioritized list of 15 initiatives that would serve as the roadmap for the transformation. I indicated that while the categories were prioritized, it would not be effective to cut the proposal into pieces. I also stressed that a transformation of this magnitude will take time. It must be carefully planned and executed and it must be inculcated into our employees.

So as to give the Committee a better perspective of the full range of security improvements initiated during the last year, our accomplishments are arrayed, along with some of those efforts we plan on completing in the future, against the groupings used by the Webster Commission.

Organizational Structure: Prior to Hanssen's arrest, there was no integrated FBI security architecture or structure. Elements of the Security Program were disseminated within eight different organizational components. This fostered an organizational disregard for security and a culture at the FBI that did not react to symptoms of Hanssen's activities. In response to this, since July 2001, the FBI:

?
Established a Security Division which, for the first time in FBI history, will serve as a point of integration for all Bureau security matters.
‣ Moved the programmatic responsibility for facility protection and police services to Security

Division, as well as the operational responsibility for protecting FBI headquarters and the Washington Field Office.

- Moved the Polygraph Unit to the Security Division.
- Started the development of a joint "business plan" with the Laboratory Division to ensure technical security resources are properly directed against Security Division requirements.

? Appointed a Director of Security, at the Assistant Director level, who serves as the senior security executive. This AD has the full support of and direct access to Director Mueller who has strongly communicated his support for the Security Program to all FBI employees.

? Provided needed infrastructure support to the Security Program by:

- Shifting internal resources to the Security Division as part of the on-going FBI restructuring plan.
- Establishing additional "detail" assignments to the Security Division from the Central Intelligence Agency (CIA) and the National Security Agency (NSA).
- Applying resources received in the fiscal year 2002 budget process to security requirements.
- Submitting a fiscal year 2003 budget request that includes significant resources for the Security Division and its mission.

? Initiated a comprehensive review of national, Director of Central Intelligence, Department of Justice, and FBI policy directives to establish a traceability matrix that will be used to gauge the effectiveness of existing security policy.

? Initiated the development of a comprehensive security education, awareness, and training program. The initial objective of this program will be to address information systems security issues followed by an expansion to all other elements of the Security Program.

Some of the initiatives the FBI intends to accomplish in the future include:

? Evaluating the need for and developing resource requests to mitigate security vulnerabilities to a level where the risk is acceptable.

? Seeking to further consolidate security functions within the Security Division.

? Developing a professional Security Officer cadre through the establishment of a comprehensive career program that identifies and hires candidates with appropriate skills, successfully retains them via a competitive pay and reward structure, builds expertise through appropriate training and assignment opportunities, and prepares them to assume program and management roles of increasing responsibility. Elements of this initiative will include:

- Establishment of a Security Career Service Board that focuses executive attention on all elements of the professional Security Officer career track.
- Certification of proficiency for security professionals and key non-security personnel, such as system administrators, in critical job-related skills.

? Re-designing the field Security Officer program to:
‣ Rely less on agents and more on the professional Security Officer cadre we intend to build over time.
‣ Restructure the field offices so that all security responsibilities fall under the control of the Security Officer.
‣ Direct more resources to the field to support the Security Program.
? Modifying the operation of the FBI Security Council to ensure it is appropriately staffed by senior executives and addresses security policy issues of significance to the Bureau.

Information Systems Security: Under the earlier section addressing the interim measures taken to enhance the computer audit procedures, I described how Hanssen exploited ACS to compromise FBI information. Protection of information within Bureau information systems is a particularly critical issue. Of the 15 initiatives that comprise the FBI's security roadmap, six directly relate to information systems security or information assurance (IA).

The Webster Commission report accurately points out that the FBI's information technology (IT) recapitalization effort, Trilogy, includes funding for only the foundational elements of IA. At rollout, Trilogy will provide more security than the FBI's current IT backbone and the five investigative applications it addresses, to include the ACS. However, the goal is to develop the IA Program to be on par with other world-class information systems security efforts. Significant coordination has taken place between the Trilogy Program and personnel assigned to the IA Program to ensure that the Trilogy security architecture will support the utilization of the future IA technologies we plan to employ, such as public key infrastructure (PKI).

In order to address security vulnerabilities impacting FBI information systems, since July 2001, the FBI:

? Established an IA Program within the Information Resources Division.

? Developed a detailed spending plan for executing IA Program resources received as part of the FY 2002 Counterterrorism supplemental appropriations bill.

? Developed a fiscal year 2003 budget request to continue development and implementation of a robust IA Program.

? Sought and received Director Mueller's commitment to appropriately address the delinquent certification and accreditation (C&A) status of many FBI IT systems.

? Implemented an aggressive C&A effort to discover and address vulnerabilities within existing and proposed FBI IT systems.

? Collaborated with the Trilogy Program to immediately deliver enhanced security measures and to provide the framework for improved information systems security measures in the future.

? Initiated the modernization of cryptographic key management to improve the security of FBI information and to facilitate the immediate deployment of Trilogy infrastructure.

Some of the initiatives the FBI intends to accomplish in the future include:

? Assigning an experienced IA professional from the Intelligence Community (IC) to run the FBI's IA Program and adding strategic "consulting" resources from the IC, as appropriate.

? Designing a comprehensive IT security architecture for FBI systems. As part of this architecture, identifying the baseline for IA tools or techniques, such as PKI, virtual private networks and LANs, single sign-on, intrusion detection, network scanning, auditing, and other methods to identify anomalous activity and system vulnerabilities.

? Establishing an Enterprise Security Operations Center to centrally manage the security of FBI IT systems and networks.

? Re-evaluating and improving the certification and accreditation process so that it mirrors best practices and is tied to the IT system development life cycle.

? Establishing a number of experienced Information Systems Security Managers as customer focal points for expeditious handling of IT security questions and issues.

? Continuing the close collaboration between IA and Trilogy Program personnel to implement improved IT system security as part of the on-going Trilogy effort.

Personnel Security: The Webster Commission report identifies many shortfalls in the processes used to assess Hanssen's continued trustworthiness. I described some of these deficiencies earlier in my statement when discussing the interim steps we have taken to expand the Polygraph Program and to conduct enhanced reinvestigation analysis. In order to improve our Personnel Security Program, since July 2001, the FBI:

? Implemented a written case summary format for reviewing security adjudication recommendations.

? Moved Polygraph Unit from the Laboratory to the Security Division.

? Continued to conduct polygraph examinations according to the criteria established in March 2001 as part of the limited expansion.

? Received conceptual approval by Director Mueller to continue with a limited and careful expansion of the polygraph program. The formal decision memo has been generated for his signature. The proposal:
‣ Expands the population already subject to CI-focused polygraph examinations to all personnel involved in the CI, CT, and Security Programs.
‣ Establishes a risk-based program comprised of four elements -- for both employees and non-Bureau personnel -- with access to the most sensitive FBI information. The elements include:
d03; Examinations as part of initial applications for employment or access.
d03; Periodic examinations tied to security reinvestigations.
d03; Aperiodic or random examinations.

d03; Compelled examinations if necessary to resolve issues that impact trustworthiness as defined by Executive Order 12968 and the Adjudication Guidelines that implement it.

Some of the initiatives the FBI will accomplish in the future include:

? Defining the requirements for an integrated security information management system and data integration efforts, as well as, executing a limited number of "pilot" efforts using funds received in the fiscal year 2002 appropriation.

? Working with the Records Management Division to improve control of FBI security files and ensure they contain the necessary information. Eventually, as part of the effort to develop an integrated security management system, transitioning to an electronic security file.

? Automating security data collection processes in a web-enabled environment.

? Identifying new sources of information that add value to the vetting process and assist in the determination of trustworthiness of employees.

? Establishing a broad based Financial Disclosure Program and developing the capability to conduct security-related financial analysis.

? Exploring the use of a specific-issue polygraph examination to address the concern of deliberate unauthorized disclosure of FBI information.

Document Security: The Webster Commission report depicts an environment where Hanssen was able to perpetrate his espionage with impunity. In one anecdote, the report describes how Hanssen is able to walk into an office area where he used to be assigned without being challenged and log onto a computer system to retrieve sensitive information which he ultimately compromised to the Russians. The Commission indicates that even recently, based on the personal experiences of their investigative staff, FBI employees still leave secure areas unattended at times potentially providing unfettered and unauthorized access to sensitive documents.

In order to continue improving the protection we afford to documents containing sensitive information, since July 2001, the FBI:

? Reassessed access procedures for FBI facilities eliminating special exemptions afforded executives.

? Established the position of Special Security Officer for the FBI and selected an Intelligence Community officer to serve in this role as a detailee.

? Completed a review of SCI handling procedures.

? Conducted a comprehensive review of sensitive accesses resulting in a net decrease of FBI employees with SCI.

? Conducted a "Back-to-Basics" day for all employees where security was one of the key areas of focus.

Some of the initiatives the FBI will accomplish in the future include:

? Establishing a Security Incident Reporting Program that includes management of all potential information compromises through a central, Security Division component. This component will ensure the security incidents are properly investigated; assessments are conducted of potential damage to the national security or FBI operations; remedial action is taken, as necessary, to ensure the compromise does not happen again; and personal accountability is assigned, if appropriate.

? Establishing a capability to resolve security anomalies, no matter their source, and to integrate information resulting from the investigation of these anomalies into the FBI CI Division.

? Developing an enhanced capability to securely process SCI electronically.

? Developing an appropriate accountability and tracking system for sensitive hard copy documents.

? Investigating technology to better account for and track sensitive information and the media, paper or magnetic, on which it is stored.

? Developing and conducting training on the proper classification of, accounting for, and control of classified information.

? Developing a more robust set of FBI classification guides.

Summary

We have made a great deal of progress in improving security at the FBI over the last year. This is particularly true considering the crisis faced by the FBI in responding to the September 11, 2001, terrorist attacks. Response to this unprecedented crisis taxed the entire FBI, to include the immature security infrastructure.

In the end, however, the most important change that must take place is a dramatic adjustment in the security "culture". Continuing security education, wide-spread security awareness and making security accepted as a normal part of everyday business is a cultural hurdle that must be overcome. A number of the efforts I have already discussed are designed to effect this adjustment. These include a strong statement of support for the Security Program by Director Mueller along with tangible consequences for failing to comply with security policies; consideration of security as a critical element of all operational programs; a robust security education, awareness, and training program; and, the development of understandable, relevant, and enforceable security policies.

There also must be no mistake about the fact that we are only beginning a journey that will take significant time and the future support of this Committee along with the rest of Congress to ensure success. We will continue to carefully examine the classified annexes of the Webster

Commission report so that we can benefit from their comprehensive study and strengthen our action plan. We also will review the Department of Justice Inspector General report on Hanssen, expected later this year, to evaluate their conclusions and recommendations.

The Webster Commission report recognizes that the FBI, or any agency that processes sensitive information, can never totally prevent espionage. There will be, at some point in time, another FBI employee or contractor who betrays our trust. Therefore, as Judge Webster suggests, we will strive to deter those rational persons who may be contemplating a compromise of sensitive Bureau information, minimize the time between their "defection and detection", and take whatever steps possible to minimize the resulting damage.

Mr. Chairman, I appreciate the opportunity to address this Committee and all of the support you and your colleagues have provided to the FBI so that we are able to faithfully discharge our important duty and help safeguard the interests of our great nation.