United States General Accounting Office

GAO

Report to the Chairman, Information, Justice, Transportation and Agriculture Subcommittee, Committee on Government Operations, House of Representatives

September 1993

DOCUMENT SECURITY

Justice Can Improve Its Controls Over Classified and Sensitive Documents

149940

RESTRICTED--Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations. 557973 RELEASED

GAO/GGD-93-134

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-253841

September 7, 1993

The Honorable Gary A. Condit
Chairman, Information, Justice,
Transportation and Agriculture Subcommittee
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

Safeguarding classified and sensitive information is an absolute necessity in the law enforcement area. The lives of law enforcement officers, victims, witnesses, judicial personnel, and persons who are the subjects of investigations could be placed in jeopardy if highly sensitive information on an investigation were inappropriately released. Likewise, national security could be compromised with the release of classified information. External and internal studies over the last few years, however, have identified document security problems at the Department of Justice.

At the request of the former Chairman of the Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, we reviewed the Department of Justice's protection of classified and sensitive documents. With the increasing strength and boldness of drug trafficking cartels, organized crime families, and terrorist groups, the Chairman wanted to know if Justice was doing all it could to provide the type and degree of security necessary to protect its operations. The Chairman was generally interested in what policies, procedures, and controls are in place within Justice to safeguard classified and sensitive documents; who administers and enforces compliance with these policies and procedures; how well Justice ensures that its security policies and procedures are implemented departmentwide; and what problems have arisen.

As agreed with the Subcommittee, we examined Justice's ability to monitor and enforce its security policies departmentwide. We specifically focused on (1) the security compliance review activities of the Security Compliance Review Group (SCRG), which is within Justice's Office of Security and Emergency Planning Staff (SEPS); (2) the Federal Bureau of Investigation's (FBI) nightly security inspections of its headquarters building; and (3) the controls placed on classified documents sent between the Justice and FBI headquarters buildings. See appendix I for the detailed objectives, scope, and methodology of this report.

Results in Brief

Justice has established and distributed regulations, directives, and policies implementing national security requirements that govern the handling of classified information. Justice also has issued regulations on safeguarding sensitive documents regarding grand jury, tax, and privacy matters. Moreover, it routinely reviews compliance with its policies and procedures and identifies security deficiencies within its offices.

However, we found areas where actions could be taken to better ensure that Justice's classified and sensitive documents are properly controlled. First, while Justice has initiated corrective actions through the efforts of SCRG, SCRG should consider alternatives for increasing the number of reviews it can do each year. For example, in addition to detailing employees from other Justice units to SCRG, SCRG should routinely receive and consider internal inspection or security violation reports from Justice agencies. These reports could be used by SCRG to target locations for and determine the scope of security compliance reviews. Also, the FBI needs to continue to cooperate with SCRG security compliance reviews of FBI facilities. Second, while the FBI has identified numerous security violations within its headquarters building, disciplinary actions taken against violators have not been in full compliance with its internal guidance. The FBI needs to ensure that it follows its internal guidance to determine the actions taken against security violators. Third, to ensure that all classified documents are delivered properly via the interoffice courier mail systems, established controls for sending classified documents should be followed more closely.

Because of its current staffing levels, SCRG recognizes that it will not be able to initially review the majority of all Justice locations in a reasonable time frame. During its first 2 years (1991 and 1992), SCRG did security compliance reviews at 54 locations and identified numerous security deficiencies. About 72 percent of these deficiencies dealt with either information or computer security matters. Corrective actions either have been taken or are planned for the majority of the deficiencies found, according to the SCRG reports and the responses from the locations reviewed. SCRG's plans to reinspect some previously reviewed locations could decrease the number of new locations reviewed each year. Given its current pace and staffing level, it will take SCRG several years to initially cover the majority of the 1,300 Justice locations and conduct necessary follow-up reviews unless SCRG finds other ways to increase the number of yearly security compliance reviews.

Moreover, contrary to SCRG's plans, none of its 54 security compliance reviews done during 1991 and 1992 included any FBI offices. At that time, the FBI objected to SCRG security compliance reviews of FBI offices because it believed that SCRG's reviews duplicated reviews done by the FBI's Office of Inspections. In view of its departmentwide responsibility for security and in keeping with the Attorney General's intentions when SCRG was formed, Justice believed that it was necessary for SCRG to conduct security compliance reviews of FBI field offices independent of the FBI's inspection process. Accordingly, SCRG scheduled security compliance reviews of other FBI facilities for 1993. Although initially opposed to the planned 1993 security compliance reviews, the FBI agreed to allow SCRG to review one of the FBI field offices in early 1993. As a result of that review, Justice and the FBI recently agreed to SCRG reviews of other FBI facilities.

During 1990 through 1992, the FBI nightly security patrols reported approximately 4,400 security violations within the FBI headquarters building. Each night, the security patrols check the offices within the FBI's headquarters building for unsecured classified and sensitive materials. About 68 percent of the 4,400 violations found by the security patrols involved unsecured classified documents. Despite the volume of violations reported, disciplinary actions were not taken against FBI personnel in accordance with established guidelines. The FBI Manual of Administrative Operations and Procedures requires that incidents of security violations be reported to, and handled by, the FBI's Administrative Summary Unit (ASU). Currently, security violations within the FBI headquarters building are being handled at the supervisory level and staff are not officially reprimanded, nor are records kept on the disciplinary actions. Lack of disciplinary actions, or inconsistent actions, could give FBI employees the impression that the security of classified and sensitive information is not a high priority.

Finally, we tested the interoffice courier mail systems controls for sending classified documents between the Justice and FBI headquarters buildings. Our limited test showed that the transmittal forms did not always contain sufficient descriptions of the documents that were sent to allow us to track them. Therefore, we cannot be certain that all classified documents reached the intended recipients.

Background

The Justice Management Division is responsible for formulating policies and procedures regarding the security of classified and sensitive documents for Justice's 31 agencies, bureaus, and offices (i.e.,

components). These 31 components have about 1,300 entities or locations (e.g., Criminal Division, Civil Division, FBI field office, U.S. Attorney office). The Assistant Attorney General for Administration directs all Justice security programs, including those relating to personnel, physical, document, computer, and telecommunications security. The Justice Security Officer, who is the Director of SEPS, develops, supervises, and administers Justice's security programs for the Assistant Attorney General for Administration. The heads of Justice's various components have ultimate responsibility for implementing, within their respective organizations, all security programs, policies, and procedures. Also, at the component level, security program managers coordinate and manage all Justice security programs and plans promulgated by Justice orders or directives.

Justice's document security program was established pursuant to Executive Order 12356, dated April 2, 1982, which outlines general sanctions for losing or compromising classified information. The order states that each agency head, or a designated senior official, shall ensure that prompt and appropriate corrective actions are taken whenever a security violation occurs. These actions range from reprimands to removal.

In January 1991, the Attorney General directed the Assistant Attorney General for Administration to establish SCRG to review security practices in all Justice components. SCRG is part of SEPS and is headed by an Assistant Director for Security. During the period from 1991 through 1992, SCRG was comprised of 6 security specialists who reviewed 54 department locations.[1]

Justice established SCRG in response to concerns about Justice's ability to maintain adequate document security. These concerns were brought on by the recent growth of Justice; increased use of computers to store and process classified information; and GAO reports highlighting Justice's need to improve security awareness, training, and practices.[2] According to Justice officials, before the formation of SCRG, security reviews were done on an ad hoc basis by SEPS. These ad hoc reviews usually were done in

[1]During part of this time, the number of SCRG staff decreased to five because the first Assistant Director left in October 1992. Another Assistant Director was appointed in January 1993 but did not take over the position until March 1993.

[2]Justice Automation: Tighter Computer Security Needed (GAO/IMTEC-90-69, July 30, 1990) and Justice's Weak ADP Security Compromises Sensitive Data (GAO/T-IMTEC-91-6, Mar. 21, 1991).

response to a report of a security leak or a request to review the security of a particular facility.

SCRG's mission is to ensure that Justice security policies and procedures are implemented within Justice and its component agencies, bureaus, and offices. SCRG conducts systematic security reviews of various Justice locations to monitor their compliance with security requirements. The security specialists conduct a detailed review of Justice locations for compliance with departmental security policies and procedures in five general areas: physical, personnel, information, computer, and communication security.[3] In conducting its compliance reviews, SCRG also examines whether contractor personnel have been cleared to work at Justice facilities and whether appropriate security requirements have been included in contracts and implemented.

The FBI Manual of Administrative Operations and Procedures sets forth the FBI's rules and regulations relating to personnel and administrative matters. Part I, section 13 of the administrative manual covers disciplinary matters, including matters relating to the loss or mishandling of classified information. The administrative manual defines the mishandling of classified information as the improper removal; storage (including unlocked/unsecured safes, vaults, or cabinets); disposal; transportation; reproduction; or transmittal of or access to such information.

The administrative manual states that all allegations of employee misconduct must be reported to the FBI's ASU, Administrative Services Division, and that allegations of criminal or other serious misconduct must be reported simultaneously to the FBI's Office of Professional Responsibility, Inspection Division. According to the administrative manual, minor personal misconduct infractions will continue to be handled by the Administrative Services Division. The administrative manual, however, lists several minor offenses, such as absence without leave or sleeping on duty, for which an assistant director of a headquarters division or a special agent-in-charge of a field office is authorized to orally reprimand or censure employees under their supervision below the GM-14 level. The loss or mishandling of classified information is not one of the offenses listed that can be handled at the assistant director or special agent-in-charge level.

[3]It takes a team of two or three SCRG staff members about 1 week to do a security compliance review at each entity. Additional time—usually about 2 to 4 weeks—is needed to draft and process a report on the team's findings. Moreover, time is required for the SCRG staff to make preparations for upcoming security compliance reviews, review responses to SCRG reports from locations already reviewed, and handle other administrative matters.

Also, as a guide for determining appropriate discipline, the administrative manual sets forth a range of disciplinary actions to be taken for a variety of misconduct offenses, including the loss or mishandling of classified information. The disciplinary actions that may be taken range from oral reprimand to removal, depending on the seriousness of the violation and the number of prior violations, if any.

An important aspect of document security at Justice is the transmittal of classified and sensitive documents. In the Washington, D.C., area, both Justice and the FBI send classified documents to each other and to other local federal agencies through an interoffice courier mail system. The number of documents sent is unknown because Justice headquarters and the FBI do not routinely record the number of classified documents sent through their courier systems.

SCRG Needs to Consider Ways to Best Target Its Limited Resources

Justice's creation of the relatively new SCRG was an important step in the right direction to ensure that Justice's components are in compliance with established security policies and procedures. SCRG has identified and invoked corrective actions for numerous security deficiencies at the locations already reviewed. However, SCRG can only review a limited number of Justice locations each year. Thus, it would take several years for SCRG, at its current pace and staffing level, to initially review the majority of the 1,300 Justice locations and conduct necessary follow-up reviews.

SCRG Reviewed 54 Justice Locations in 1991 and 1992

As discussed in appendix II, SCRG conducted security compliance reviews of 54 Justice locations between January 1991 and December 1992. In those reviews, SCRG identified numerous and recurring security weaknesses and incidents of noncompliance with security policies. Of the 54 locations reviewed, we examined the 35 SCRG reports that had been completed at the time we did our work. About 72 percent of SCRG's findings at these locations involved deficiencies in information and computer security. For example, SCRG cited 7 out of 10 U.S. Attorney offices they reviewed for improperly storing and transmitting grand jury information. Other findings made by SCRG at the various locations, which are discussed further in appendix II, included

- grand jury information not having been properly destroyed;
- classified information not having been properly marked;

- classified information not having been properly processed on computer systems or stored on nonremovable hard drives;
- individual computer user passwords and unique user identification numbers not having been used or changed as required;
- no records for opening, closing, and end of the day security checks of security containers having been used to store classified documents;
- combinations to security containers having been changed by contractor personnel without security clearances;
- building contractor personnel with unescorted access to office space not having required FBI name and fingerprint checks; and
- janitorial personnel, who clean office space during nonduty hours, not having required FBI name and fingerprint checks.

SCRG Has Limited Resources

SCRG will not be able to review all 1,300 Justice locations in a reasonable time frame, according to Justice officials. During 1991 and 1992, SCRG conducted about 27 compliance reviews a year with its staffing level of 6 security specialists. In addition, the current Assistant Director, SCRG, said that he plans to reduce the number of initial compliance reviews each year to about 20 but at the same time conduct about 20 follow-up reviews. Justice requested, but was not authorized, additional staffing for SCRG for fiscal year 1993.

SCRG officials told us that their inability to review every Justice location within a reasonable period of time has compelled SCRG to review those Justice locations with the greatest security needs. SCRG officials realize that because of limited staffing they must selectively target offices for compliance reviews. Consequently, SCRG officials said that they select and schedule locations for security compliance reviews on the basis of the following criteria: whether the locations within Justice components have already been reviewed by SCRG, the volume of classified and sensitive information handled by the locations, and whether the locations have requested security compliance reviews.

SCRG currently does not use components' internal documentation about security practices to decide what locations to review. According to SCRG officials, SCRG does not routinely get copies of internal inspection reports from the various agencies (i.e., the FBI's Inspection Division). Moreover, agency summaries of security violations, such as the FBI's monthly security violation reports, are not sent to SCRG. The Assistant Director for Security Compliance said that the issue of getting internal agency reports has been discussed in the past but never pursued. It was his opinion that this was

not pursued because of the perceived difficulty in getting internal documents and the fact that SCRG is still a relatively new entity. The Assistant Director also indicated that he thought internal reports would be beneficial to SCRG in planning and scheduling its compliance reviews.

During our exit conference, Justice officials expressed concern about getting copies of agencies' internal inspection reports because these reports may contain some very sensitive information that the agencies might not want to release to anyone outside of the component. However, it was acknowledged that, for SCRG's purposes, information could be redacted from copies given to SCRG and that this probably would not occur very often.

SCRG officials said they considered temporarily detailing personnel from other Justice agencies to help conduct security compliance reviews. Until recently, they had not done this because they believed that other staff could not do as thorough a job as the SCRG staff. Everyone at SCRG is a security expert whose professional background and experiences relate to security matters. For example, although agents from the FBI or the Drug Enforcement Administration (DEA) might have a general knowledge about security, they are trained as law enforcement officers, not security experts. Thus, it was the opinion of SCRG officials that they probably could not do as good a job as SCRG personnel.

At our exit conference, SEPS officials said that they recently reorganized SEPS, to some extent, to add another staff member to SCRG, giving them the capability to have three review teams (as opposed to the previous two). SEPS officials also said that they plan to start using agency security personnel in conducting security reviews at the agency's component. For example, when they conduct a security review at an Immigration and Naturalization Service (INS) facility, they plan to have a staff member from INS' security unit assist with the review. They also have reached agreement with the Department of the Treasury to use Treasury personnel for security reviews at certain Justice locations where Treasury personnel also are located; for example, at locations where there are Organized Crime and Drug Enforcement Task Forces. With these changes, SCRG hopes to be able to do about 60 reviews annually, including initial, follow-up, and unannounced reviews.

SCRG recognizes that it cannot review each and every Justice location in the near future. Therefore, its philosophy is to promote voluntary compliance with the myriad of security regulations, policies, and

procedures. It believes that this goal can be achieved through its constructive approach to its security compliance reviews and disseminating information on the results of its reviews. In addition to its scheduled compliance reviews, SCRG also believes that voluntary compliance will be enhanced through follow-up reviews and unannounced reviews. The Assistant Director said that about half of the security compliance reviews done by SCRG would be follow-up reviews. He said that the follow-up reviews do not take as long—about 1 day—as the full compliance reviews because the review team is only checking to see if previously identified deficiencies have been corrected. Moreover, he said that he plans to minimize travel costs by scheduling compliance reviews in locations where SCRG has done other compliance reviews to facilitate doing the follow-up reviews. The Assistant Director also said that SCRG has already done one unannounced compliance review and plans to do at least one more in 1993. He added that he expects the number of unannounced compliance reviews to increase in the future.

During our exit conference, Justice officials emphasized that it was not intended that SCRG conduct a security compliance review at all of Justice's 1,300 locations. Rather, it was intended that publicizing the results of SCRG reviews of some locations would have a deterrent effect on other locations that have not been reviewed.

In this regard, the Justice officials indicated that they have done several things to achieve this deterrent effect. For example, SEPS has only recently begun issuing "common findings" letters to the heads of the Justice components outlining the common, repetitive findings they have noted in their reviews at the agencies' field and headquarters locations. Justice officials believe this can have a multiple deterrent effect on components within a Justice agency without SCRG's actually reviewing each and every location.

Another recent change to achieve this deterrent effect involves more in-depth reviews of computer systems. In this regard, after SCRG completes a security compliance review, it plans to routinely inform the Computer and Telecommunications Security Staff group of all computer-related security findings. On the basis of these findings, the computer group plans to do a more detailed follow-up review of the subject component's computer system security.

The FBI Was Reluctant to Allow SCRG Compliance Reviews

During 1991 and 1992, no SCRG compliance reviews were done at any FBI facilities because it opposed reviews by SCRG. SCRG did not schedule reviews at any FBI facilities during 1991 because SCRG officials believed that (1) the FBI probably was the most security conscious of the various Justice components, (2) the Justice Inspector General's Office had approved the FBI's inspection procedures, and (3) there were other agencies that SCRG believed needed to be reviewed before the FBI.

SCRG had planned to review an FBI field office in January 1992. However, the FBI informed Justice that it had done its own inspection of that office in November 1991 and that SCRG's scheduled compliance review would be a duplication of effort and would not be cost effective to Justice. SCRG's compliance review of the FBI's field office was canceled. But Justice advised the FBI that it was necessary for SCRG to conduct security compliance reviews of FBI field offices independent of the FBI's inspection process. The FBI objected to this decision and reiterated its belief that SCRG's security compliance reviews duplicated reviews done by its own Office of Inspections. Justice responded that its planned actions were in keeping with the Attorney General's intentions when SCRG was established in early 1991. That is, that SCRG security compliance reviews would complement Justice components' responsibility for conducting security inspections. Justice also stated that allowing the FBI to do all of its own inspections might leave both the FBI and Justice open to the criticism that the FBI is not in compliance with all of Justice's security compliance initiatives.

Further, Justice contended that whatever benefits accrue from the SCRG's security compliance reviews at other Justice locations would not be readily or equally available to the FBI. SEPS' Deputy Director said that Justice would have been more assertive in its right to inspect FBI facilities had SCRG been aware of significant problems or security violations at any FBI location, such as those discussed in the next section of this report.

Accordingly, SCRG scheduled compliance reviews of other FBI offices for 1993. Initially, FBI officials told us that the FBI also was opposed to these compliance reviews. However, during the course of our audit, the FBI agreed to let SCRG conduct a security compliance review at a FBI field office in March 1993. SCRG's compliance review resulted in 19 findings of security deficiencies at the FBI field office. Some of the findings were similar to those SCRG had found at other Justice components. According to the FBI's Chief of the Security Countermeasures Section, the compliance review benefited the FBI because it pointed out some security areas that the FBI

does not cover during its own inspections. He also said that SCRG is dedicated to reviewing only security matters, and that it has demonstrated the ability to do this very well.

During the exit conference, Justice and FBI officials stated that, as a result of the SCRG's review of an FBI field office in March 1993, Justice and the FBI have been working together to change some of the FBI's policies and procedures for inspecting security operations at its facilities. The officials also pointed out that SCRG plans to do security compliance reviews at two or three FBI facilities each year.

FBI Security-Related Disciplinary Actions Were Not in Accordance With Agency Guidance

Security violations uncovered during nightly security patrols of the FBI headquarters building were not being reported to the ASU, nor were employees officially reprimanded in accordance with FBI guidelines. None of the security violations reported for the 3-year period we examined was referred to the ASU for consideration. Instead, security violations were handled at the divisional supervisory level. Moreover, records were not kept of the disciplinary actions that reportedly were taken at the supervisory level. Thus, there was no assurance that disciplinary actions were taken against security violators or that actions, if taken, were in accordance with the FBI Manual of Administrative Operations and Procedures and consistent among FBI divisions.

The FBI's J. Edgar Hoover Building, which is a controlled-access facility, is inspected nightly for security and safety violations by the FBI's Security Unit, Administrative Services Division. The security and safety checks are usually done by two or three patrol persons. Detected violations are recorded on a security violation notification card, which identifies the type and location of each violation. The notification card is filed in the Security Patrol Office and copies are left both inside and on top of the safe, file cabinet, or desk found unsecured. Once a month, a synopsis of the daily reports is prepared by the Security Patrol Office and sent to the assistant director of each division and to the Security Program Manager. According to an FBI official, these monthly synopses are not sent to Justice because the reports are used only for internal tracking purposes.

During 1990 through 1992, FBI security patrols reported approximately 4,400 security violations, ranging from Top Secret documents found unsecured to safes found open to office keys found in open desks. About 68 percent of the reported security violations involved unsecured classified documents. About 24 percent of the security violations involved

unsecured FBI files, evidence, and other sensitive documents. The remaining 8 percent involved such things as alarmed doors left open, unsecured office keys, badges and credentials found in or on desks, secure telephones with security keys still inserted, etc. See appendix III for additional details on these violations.

Despite the volume of violations reported, disciplinary actions were not being taken against FBI personnel in accordance with established guidelines. The administrative manual states that allegations of employee misconduct, including security violations, must be reported to, and that appropriate disciplinary action must be determined by, the ASU. It also outlines actions to be taken for various types of employee misconduct. As shown in table 1, the administrative manual sets forth, as a guide in determining appropriate discipline, a range of disciplinary actions to be taken depending on the severity of the violations and number of prior violations.

Table 1: Disciplinary Actions for Security Violations as Outlined in the FBI Administrative Manual

	Range of disciplinary actions for all personnel		
Security violations	**First offense**	**Second offense**	**Third offense**
Loss of classified information	Censure to removal	Suspension to removal	Suspension to removal
Mishandling classified information by: improper storage (to include unlocked or unsecured safes, vaults, or cabinets); disposal; transporting; reproduction; transmittal; or access.	Oral reprimand to removal	Censure to removal	Suspension to removal

Source: FBI Manual of Administrative Operations and Procedures.

ASU is the only office in the FBI that can decide on official disciplinary actions to be taken for security violations.[4] The administrative manual provides, and the ASU Chief confirmed, that the level of the discipline to be meted out for employee misconduct, including the loss or mishandling of classified information, is to be determined by ASU. Yet, according to officials within ASU, none of the security violations found within the FBI headquarters building were referred to their unit for a determination of disciplinary action. The Chief also said that ASU had no way of knowing about security violations if the divisions did not refer them to ASU.

[4]A disciplinary action is considered official when a record is made of the offense and the action taken and is placed in the employee's official personnel file.

Instead of referring security violations to ASU, they were handled at the supervisory level and disciplinary actions were not determined by ASU, according to FBI officials. We discussed the issue of security violations with security officers from five FBI divisions. All of them indicated that security violations were not forwarded to ASU, not even those for repeat offenders. As seen in table 1, the severity of disciplinary actions generally increases as the number of offenses increase. Officials in one division said that there were many employees who received multiple security violation notices. The security officer for this division also said that when he has suggested that a particular incident be referred to ASU, he was advised that this was not how the division wanted to handle these matters.

All of the security officers to whom we spoke said that they tried to watch for any employee with repeated violations over about a 3- or 4-month period. None of the security officers could remember an occasion when a security violation was referred to ASU. They said that the employees' supervisors were notified of the violations and that the supervisors usually counseled or admonished the employees. One problem noted by the security officers, however, was that since the violations often occurred within other sections of their divisions, they have no way of knowing what, if any, actions were taken by the supervisors.

Since the administrative manual is clear that repeat offenders should receive more severe disciplinary actions, and thus properly should have been reported to ASU, we attempted to determine the magnitude, if any, of repeat security violations by the same FBI employee. However, we could not make this determination because the FBI did not give us complete access to all of the information in the monthly security violation reports maintained by the Security Patrol Office. We were given copies of the reports but the employee names were deleted. We had specifically asked that the names of the employees be left on the monthly reports for 1992 so that we could gain a sense of the number of repeat offenders. But FBI officials denied our request. Thus, we could not confirm or refute the existence of repeat offenders or determine the magnitude of their existence. Senior level FBI officials acknowledged, however, that there had been FBI personnel who have had multiple security violations and that these repeat offenders were not referred to ASU, as required by the administrative manual.

Controls for Sending Classified Documents Through Interoffice Mail Should Be Followed More Closely

We reviewed the adequacy of the controls for sending classified documents between the Justice and FBI headquarters buildings. On the basis of a limited test of the interoffice courier mail systems, we cannot be certain that all documents sent via the systems reached the intended recipients. To ensure that all classified documents are delivered properly, established controls for sending classified documents should be followed more closely.

Both Justice and the FBI have controls for sending classified documents through their own interoffice courier mail systems. Justice requires that a Classified Document Receipt (DOJ Form 34) accompany each piece of classified mail for delivery via the courier mail system. The form, to be completed and attached by the sender, is supposed to include the name and address of both the sender and the recipient, subject and description of the document, date of the document, number of pages, and the document's classification level. Upon delivery, the recipient is supposed to sign and date the receipt. The signed receipt is then supposed to be returned to the sender and a carbon copy sent to Justice's Mail Management Unit.

The FBI's Mail Service Unit prepares all classified documents for delivery outside of the main headquarters building. Once a document is ready for delivery, a Courier Receipt Card (FBI Form 4-54) is to be completed by the mail room staff. The receipt card is supposed to include the name and agency of the addressee, date, courier identification information, document classification level, and signature of the recipient. The FBI also requires the mail room staff to record all documents delivered by the courier service in a courier log. Further, after the delivery the signed receipt is supposed to be returned to the mail room and a record of the delivery is supposed to be entered onto a computer by mail room staff.

Justice and FBI officials told us that they did not know the total number of classified documents sent through the interoffice mail systems. We determined that there were approximately 2,700 receipts for classified documents sent from Justice headquarters to other federal agencies throughout the Washington, D.C., area between January and September 1992. Likewise, we determined that there were about 900 deliveries of classified documents sent from the FBI headquarters to other federal agencies in the Washington, D.C., area during the same period. The total number of classified documents sent is not known because each delivery could have involved several documents.

To test the adequacy of the controls used to send classified documents between the Justice and FBI headquarters buildings, we attempted to trace a number of documents sent from Justice to the FBI and vice versa. We tried to locate all 14 classified documents that were sent from Justice to the FBI between January and September 1992. Eight of the 14 documents could not be located because the receipts that accompanied them were not properly completed. For three of these eight receipts, the descriptions of the documents were left blank. The remaining five receipts had only a general description of the documents (e.g., referrals, package).

We found similar problems, although to a lesser degree, when we attempted to locate a random sample of 10 classified documents that was sent from the FBI to Justice during the same period. In this case, we could not trace 3 of the 10 documents. Two of the three had control receipts that only indicated that the documents were sealed envelopes. The third document, which was appropriately described on the control receipt, could not be found in the files at the recipient's office. All of the receipts for the documents we traced were signed by Justice and FBI personnel, although not always by the named recipient.

We did not formally test receipts for documents delivered from Justice to other agencies, nor did we tabulate the number of documents sent to other locations. Nevertheless, as we were attempting to identify receipts for classified documents sent from Justice to the FBI, we did observe deficiencies in the manner in which the receipts were completed for classified documents sent to other Justice components and other federal agencies. For example, many of the receipts were not filled out completely and/or properly. That is, the descriptions of the documents often were vague or were left blank. Further, many of the receipts were not signed for by the named recipient. In addition, the writing on many of the receipts was illegible. These deficiencies possibly could have hampered the delivery of classified documents to the intended recipients.

In addition to the deficiencies noted above, we observed other factors that could affect the ability of Justice (or anyone else) to verify whether classified documents reached their intended recipients. We found that Justice's Mail Management Unit did not control the receipts of documents delivered by the couriers in an organized manner. These receipts would allow Justice to trace the delivery of classified documents. We observed that the receipts were in bundles, by month, and kept together by rubber bands. However, receipts from one month were intermingled with receipts from other months. Further, many receipts were torn in a manner that

made it impossible to determine who had sent the document or where the document had been sent. In addition, when we attempted to select a sample of classified documents at the FBI, the Information Services Section was unable to locate courier cards or find the computer records for some of the deliveries. Thus, we were unable to obtain specific information on all of the deliveries made by the FBI's courier service during this period.

Conclusions

Justice has set forth policies and procedures governing security issues for all of its offices and agencies to follow and it has systems in place for reviewing compliance. In addition, Justice has established SCRG to conduct security compliance reviews of department components to ensure compliance with its security policies and procedures. However, during 1991 and 1992 SCRG had only six staff members to conduct security compliance reviews and was not granted a requested increase in staff for fiscal year 1993. At its current pace and staffing level, it will take several years for SCRG to initially review the majority of the 1,300 locations within Justice's 31 component agencies, bureaus, and offices. The time needed to initially review the majority of the locations will likely increase as SCRG begins to conduct more needed follow-up reviews.

On the basis of our review, we believe that establishing SCRG was an important step to ensure that Justice's components are in compliance with security policies and procedures. Even though its efforts have been limited because of its small staff, SCRG has identified and invoked corrective actions for many security deficiencies and problem areas that otherwise might not have been identified.

We agree with Justice officials that it would be a formidable task to review all 1,300 locations. Thus, we believe that SCRG should focus on increasing the number and mix (new, follow-up, and unannounced) of reviews done annually. We further believe that SCRG needs to seek alternate ways to plan, scope, and conduct its security compliance reviews to ensure that it is making efficient and effective use of, and having maximum impact with, its limited resources. In this regard, we noted that SCRG did not receive copies of inspection reports from Justice's component internal review units (e.g., the FBI's Inspection Division). SCRG also did not receive copies of security violation reports from the FBI concerning the nightly security patrols done within the FBI headquarters building. Internal inspection reports and security violation summaries from Justice components could be used by SCRG to assist in planning and scoping its compliance reviews, thereby maximizing the use of its limited resources. For example, SCRG

might be in a better position to determine the need for a security compliance review at a particular FBI field office after SCRG has reviewed the FBI's Inspection Division report of its latest inspection of that field office.

SCRG's plan to begin using staff members from other Justice components to assist in conducting security compliance reviews is another positive alternative way for SCRG to more efficiently and effectively achieve its mission. Using detailees from other Justice components should assist SCRG in increasing the number of reviews done each year. Additional benefits also might accrue as staff from other components are detailed to SCRG to assist with security compliance reviews. For example, detailees would develop a better understanding of all Justice security policies and procedures and they could use this knowledge to improve security throughout their own organizations. Also, detailees could help internal review groups in their home components do more comprehensive security inspections, thereby further augmenting SCRG's work.

In addition, prior to March 1993 SCRG had not reviewed any of the FBI's facilities because FBI officials resisted the SCRG compliance reviews. Further, SCRG had not routinely received the results of the FBI's own internal inspections or the reports of violations by the FBI's security patrols. Thus, Justice did not know to what extent, if at all, the FBI was in compliance with Justice security policies and procedures. During our audit, the FBI agreed to a security compliance review of one of its field offices in March 1993 and, after that review, it agreed to additional inspections at other FBI locations. We think that this is a step in the right direction and it should be continued. Independent inspections of FBI facilities are essential if Justice is to fulfill its oversight responsibilities for ensuring that all Justice components are adhering to its security policies and procedures. Moreover, Justice security compliance reviews of FBI facilities could have other benefits. For example, better coordination and cooperation with future compliance reviews would allow the FBI and Justice to maximize use of their resources. Also, the FBI could benefit from additional security compliance reviews by having outside security experts identify potential areas for improving security. The FBI could also apply what it learns from the SCRG compliance reviews to its own inspections, thereby expanding, and complementing, Justice's overall security compliance review efforts. In this regard, as previously noted, Justice and FBI officials indicated that they have been working together to change some of the FBI's policies and procedures for inspecting security

operations at its facilities as a result of SCRG's review of the FBI field office in March.

As noted previously, the FBI's current procedures for handling security violations did not comply with its administrative manual. Also, given the decentralized manner in which security violations were handled, the FBI had no way of knowing if disciplinary actions were being taken completely and consistently among its divisions. Thus, employees may be misinterpreting the importance and seriousness of safeguarding classified and sensitive materials. Conversely, if disciplinary actions taken for security violations were more uniform and consistent, as set forth in the administrative manual, employees might better understand that security of classified and sensitive documents is a serious matter. Thus, the FBI should reinforce and follow its existing requirements for centrally administering disciplinary actions for security violations, unless it can demonstrate that these requirements should be changed.

Controls for sending classified documents from Justice to other federal agencies should be followed more closely. We could not be certain that all classified documents sent via the interoffice courier mail systems reached the intended recipients. Many documents could not be located because the receipts that accompanied them were not properly completed. Thus, the receipts may not be an effective internal control mechanism. To ensure that all classified documents are delivered properly, established controls for sending classified documents should be followed more closely.

Recommendations

We recommend that the Attorney General direct

- SCRG to explore other alternatives for selecting and conducting the number of security compliance reviews done each year. For example, internal inspections reports and security violations summaries done by Justice components could be used by SCRG in its deliberations on what locations should be reviewed, and when and to what extent, thereby maximizing the use of its limited resources.
- the FBI to continue to work with SCRG in its efforts to review other FBI facilities to ensure that all FBI facilities are in full compliance with Justice security policies and procedures.
- the FBI to begin imposing disciplinary actions for security violations in accordance with its own internal guidelines.

- both the Justice and FBI mail management units to more strictly enforce the established procedures for sending classified documents through the interoffice courier mail systems.

Agency Comments

At the request of the Subcommittee, we did not obtain formal written agency comments. However, we held an exit conference with Justice and FBI officials to discuss the report's findings. While these officials were in general agreement with our findings, they noted some recent actions that have been taken. The information the officials provided during the exit conference has been incorporated into the report where appropriate.

Unless you publicly announce the contents earlier, we plan no further distribution of this report until 30 days from the date of issuance. At that time, we will send copies of the report to the Attorney General and the FBI Director. Upon request, we will send copies to other interested parties.

The major contributors to this report are listed in appendix IV. Please contact me on (202) 512-5156 if you have any questions concerning this report.

Sincerely yours,

Henry R. Wray
Director, Administration
of Justice Issues

Contents

Letter		1
Appendix I Objectives, Scope, and Methodology		22
Appendix II SCRG Findings of Security Deficiencies		24
	SCRG Identified Numerous Security Problems	24
Appendix III Security Violations Within the FBI's Headquarters Building		30
	Security Patrols at FBI Headquarters	30
	Security Violations From 1990 Through 1992	30
	Examples of Violations Reported by the FBI Nightly Security Patrols	39
Appendix IV Major Contributors to This Report		42
Tables	Table 1: Disciplinary Actions for Security Violations as Outlined in the FBI Administrative Manual	12
	Table II.1: Number of Inspections of Justice Components During 1991 and 1992	24
	Table II.2: Number of SCRG Findings at the Bureau of Prisons, by Security Findings Category	26
	Table II.3: Number of SCRG Findings at the Drug Enforcement Administration, by Security Findings Category	27
	Table II.4: Number of SCRG Findings at the Immigration and Naturalization Service, by Security Findings Category	27
	Table II.5: Number of SCRG Findings at Justice Headquarters Divisions and Offices, by Security Findings Category	28
	Table II.6: Number of SCRG Findings at U.S. Attorney Offices, by Security Findings Category	28
	Table II.7: Number of SCRG Findings at the U.S. Marshals Service, by Security Findings Category	29

Table II.8: Number of SCRG Findings at Community Relations Service and U.S. Trustees Office, by Security Findings Category 29
Table III.1: Number of Security Violations Reported by the FBI During 1990, 1991, and 1992, by Division 32
Table III.2: Number of Security Violations Reported by the FBI During 1990, by Division 33
Table III.3: Number of Security Violations Reported by the FBI During 1991, by Division 34
Table III.4: Number of Security Violations Reported by the FBI During 1992, by Division 35

Figures

Figure II.1: Percentage of SCRG Findings at Selected Justice Components 26
Figure III.1: Number of Security Violations Reported by the FBI, by Types of Violations and Years 37
Figure III.2: Percentage of Security Violations Reported by the FBI During 1990, 1991, and 1992 Combined, by Types of Violations 38

Abbreviations

ASU	Administrative Summary Unit
DEA	Drug Enforcement Administration
DOJ	Department of Justice
EEO	Equal Employment Opportunity
FBI	Federal Bureau of Investigation
INS	Immigration and Naturalization Service
OCA	Office of Public Affairs
OLIA	Office of Liaison and International Affairs
OPA	Office of Public Affairs
SCRG	Security Compliance Review Group
SEPS	Security and Emergency Planning Staff

Objectives, Scope, and Methodology

On March 12, 1991, the former Chairman of the Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, requested that we review the Department of Justice's protection of classified and sensitive documents. With the increasing strength and boldness of drug trafficking cartels, organized crime families, and terrorist groups, the Chairman wanted to know if Justice was doing all it could to provide the type and degree of security necessary to protect its operations and asked that we examine Justice's control over classified and sensitive documents. The Chairman was generally interested in what policies, procedures, and controls were in place within Justice to safeguard classified and sensitive documents; who administers and enforces compliance with these policies and procedures; how well Justice ensures that its security policies and procedures are implemented departmentwide; and what problems have arisen.

As agreed with the Subcommittee, we focused on Justice's ability to monitor and enforce its security policies departmentwide. Specifically, we agreed to evaluate and report on

- Justice's ability to monitor and enforce its security policies and procedures by focusing on the security compliance review activities of the Justice Management Division's Security Compliance Review Group (SCRG),
- the FBI's compliance with security policies and procedures by reviewing the FBI's nightly security patrols' inspections of its headquarters building, and
- the controls for sending classified documents by courier mail system between the Justice and FBI headquarters buildings.

To obtain an overall understanding of Justice's security program, we reviewed the directives, policies, and regulations issued by Justice to implement security regulations that govern the handling of classified and sensitive information departmentwide. Also, we interviewed Justice and FBI officials responsible for security matters.

To evaluate Justice's ability to monitor and enforce its security policies, we interviewed members of SCRG. When we were doing this part of the audit, SCRG had completed and reported on 35 security compliance reviews. We analyzed these 35 reports to determine the number and type of security deficiencies uncovered by SCRG. In addition, we examined agency responses that addressed deficiencies documented in the compliance review reports. We did not verify that corrective actions outlined in agency responses had been implemented.

To evaluate compliance with security policies at the FBI, we reviewed the monthly security reports for 1990, 1991, and 1992 that listed the violations uncovered during the FBI's nightly security patrols. We analyzed these reports to determine the number and types of security violations reported. We interviewed FBI security patrol officials, division security officers, and Administrative Summary Unit officials to determine the procedures for and practice of disciplining staff members who receive security violations. We did not review the accuracy or reliability of information generated by the nightly security patrols. Further, we could not verify the existence or determine the magnitude, if any, of repeat offenders because the FBI denied us access to the names of the employees identified in the security violation reports.

To test the adequacy of the controls used to send classified documents by courier between the Justice and FBI headquarters buildings, we selected a number of documents to trace from Justice to the FBI and vice versa. First, we searched through Justice records for deliveries of classified documents made between January and September 1992. During this period, we identified 14 receipts for the delivery of classified documents from the Justice headquarters building to the FBI. We reviewed all 14 receipts of classified documents sent from the Justice headquarters building to the FBI. We attempted to trace these documents to the recipients to determine if the documents were received and properly controlled. We also interviewed Justice officials responsible for mail management matters.

Second, we reviewed the FBI courier logs for deliveries of classified documents made to Justice between January and September 1992. During this period, we identified 83 receipts for deliveries from the FBI to Justice headquarters offices. We selected and reviewed a random sample of 10 receipts of classified documents. We attempted to trace these documents to the recipients to determine if the documents were received and properly controlled. We also interviewed FBI officials in the Information Service Section, Information Management Division, who are responsible for mail management matters.

We did our review from August 1991 through March 1993 in accordance with generally accepted government auditing standards.

SCRG Findings of Security Deficiencies

Established in January 1991 by the Attorney General to ensure that Justice security policies and procedures were implemented departmentwide, the Security Compliance Review Group (SCRG) inspected 54 Justice offices and entities between January 1991 and December 1992, as shown in table II.1. Table II.1 also shows the number of SCRG inspection reports we reviewed during our work.

Table II.1: Number of Inspections of Justice Components During 1991 and 1992

Justice component	Number of offices inspected	Number of SCRG reports GAO reviewed
Bureau of Prisons	3	2
Community Relations Service	1	1
Drug Enforcement Administration	10	7
Executive Office of U.S. Trustees	1	1
Immigration and Naturalization Service	5	3
INTERPOL	1	0
Justice divisions and offices	12	5
U.S. Attorney offices	15	12
U.S. Marshals Service	5	4
U.S. Parole Commission	1	0
Total	**54**	**35**

Legend

INTERPOL = International Criminal Police Organization

Source: Office of Security and Emergency Planning Staff (SEPS), Justice.

Security compliance review results are documented in reports that present the SCRG findings and observations about security practices and weaknesses at the inspected agency. The SEPS Director signs each report and copies are sent to the head and the security officer of the Justice location visited. Each report also includes recommendations, where appropriate, to remedy security deficiencies and improve compliance with security requirements. Agencies have 60 days to respond to the recommendations made in the report and must outline the corrective actions they have taken or plan to take.

SCRG Identified Numerous Security Problems

In its inspections of Justice components, SCRG identified and reported on numerous security weaknesses and incidents of noncompliance with security policies and procedures. The security compliance review reports contained findings and recommendations that addressed security

deficiencies in five general areas: physical, personnel, information, computer, and communication security.

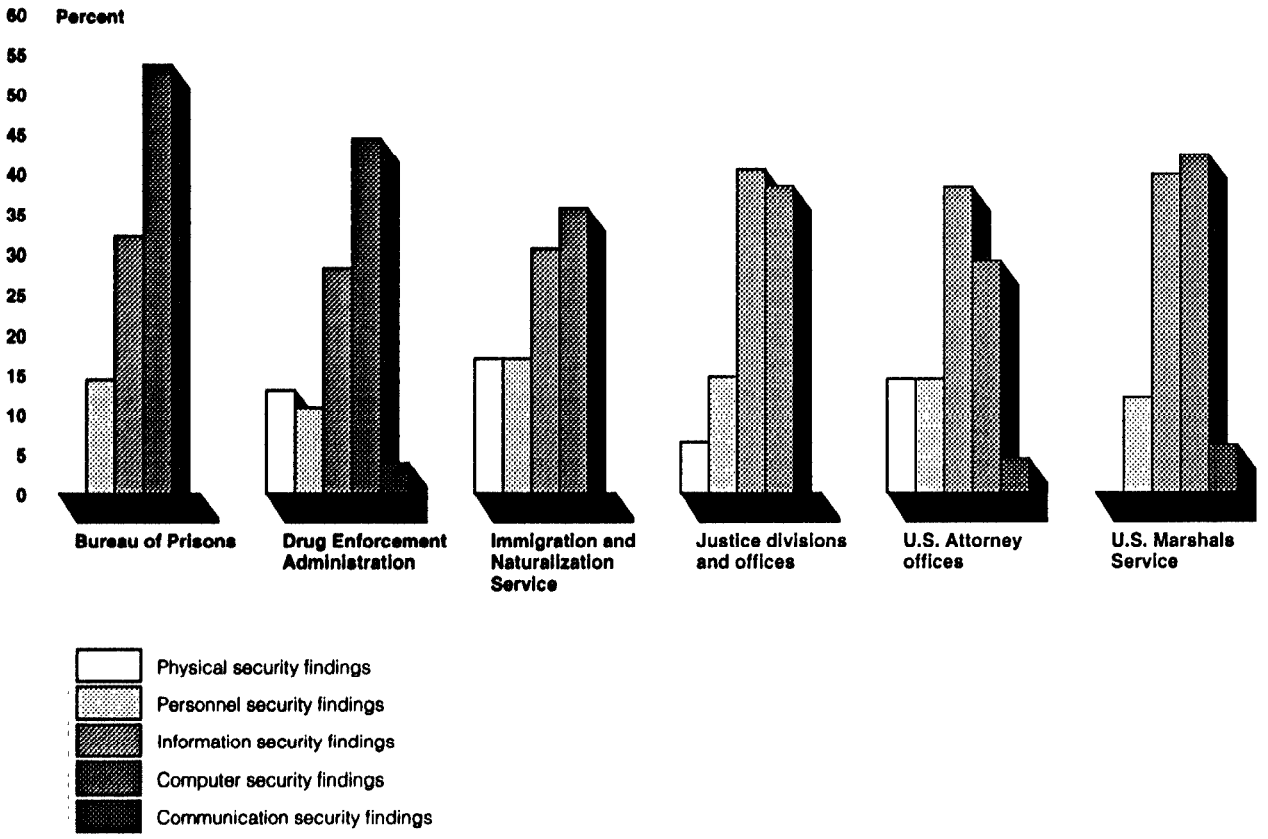
Each security deficiency uncovered by SCRG was placed in one of the five categories. Many of the SCRG reports showed that agencies shared common problems, especially those that pertained to information and computer security issues. Some of the problems dealt with the storage and handling of classified documents, processing classified information on computers that were not properly cleared, and inadequate password protection. Some examples of deficiencies in the five categories include the following:

- Physical security. No intrusion detection system, personnel bypassed card-key entry system to enter offices, and locks to offices and file cabinets were not functional.
- Personnel security. Unnecessary clearances were issued to staff, security clearance reinvestigations were not done, contractor staff lacked FBI background checks, and safe combinations were given to uncleared staff.
- Information security. Classified documents were not properly marked or left unsecured; combinations to safes were improperly stored or were not changed as required; and classified documents, including grand jury information, were improperly destroyed.
- Computer security. Unique user identification numbers and passwords were not used on specialized computer systems; classified and sensitive information, including grand jury information, was improperly processed on computers with hard drives; no risk analysis was done on computer systems; and diskettes containing classified information were not properly marked or secured.
- Communication security. Communication keying material was destroyed with no record of a witnessing official, crypto ignition key was found unattended, and secure telephones were not used.

As shown in table II.1, we reviewed 35 compliance review reports completed by SCRG of selected Justice components. Figure II.1 shows the percentage of SCRG's findings for each of these 35 Justice components. The number of SCRG findings by security categories for these offices are presented in tables II.2 through II.8.

The majority of the overall findings reported by SCRG for the 35 compliance reviews dealt with computer security (38 percent) and information security (34 percent) issues. The remaining percentage of the findings were: 10 percent for physical security issues, 13 percent for personnel security issues, and 4 percent for communication security issues.

Figure II.1: Percentage of SCRG Findings at Selected Justice Components



Source: Data calculated from security compliance reports provided by Justice.

Table II.2: Number of SCRG Findings at the Bureau of Prisons (Bop), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
BOP 1	0	3	7	6	0
BOP 2	0	1	2	9	0
Total	**0**	**4**	**9**	**15**	**0**
Percent	0.0	14.3	32.1	53.6	0.0

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.3: Number of SCRG Findings at the Drug Enforcement Administration (DEA), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
DEA 1	2	1	8	15	0
DEA 2	2	2	2	11	1
DEA 3	11	7	14	10	3
DEA 4	2	4	11	12	1
DEA 5	1	2	4	14	0
DEA 6	3	1	11	10	1
DEA 7	2	3	2	9	1
Total	**23**	**20**	**52**	**81**	**7**
Percent	12.6	10.9	28.4	44.3	3.8

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.4: Number of SCRG Findings at the Immigration and Naturalization Service (INS), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
INS 1	5	5	10	8	0
INS 2	4	3	5	8	0
INS 3	1	2	3	6	0
Total	**10**	**10**	**18**	**22**	**0**
Percent	16.7	16.7	30.0	36.7	0.0

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.5: Number of SCRG Findings at Justice Headquarters Divisions and Offices, by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
CRD	1	4	6	12	0
OIG	0	1	2	0	0
OPR	0	0	2	0	0
SEPS	1	0	8	4	0
TAX	1	2	1	2	0
Total	**3**	**7**	**19**	**18**	**0**
Percent	6.4	14.9	40.4	38.3	0.0

Legend

CRD = Civil Rights Division
OIG = Office of Inspector General
OPR = Office of Professional Responsibility
SEPS = Security and Emergency Planning Staff
TAX = Tax Division

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.6: Number of SCRG Findings at U.S. Attorney Offices (Usao), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
USAO 1	2	2	1	4	0
USAO 2	1	5	17	6	1
USAO 3	2	3	12	2	1
USAO 4	0	2	13	6	0
USAO 5	1	2	5	1	0
USAO 6	2	0	1	3	1
USAO 7	15	2	5	10	2
USAO 8	5	3	4	14	3
USAO 9	0	4	7	6	0
USAO 10	1	3	1	5	0
USAO 11[a]	0	0	14	0	0
USAO 12[b]	1	4	0	5	1
Total	**30**	**30**	**80**	**62**	**9**
Percent	14.2	14.2	37.9	29.4	4.3

[a]The review of this U.S. Attorney office was focused on the activities of the Bank Fraud Task Force located in the office. This review focused only on safeguarding grand jury information.

[b]The review of this U.S. Attorney office was focused on the activities of the Organized Crime Drug Enforcement Task Force located in the office.

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.7: Number of SCRG Findings at the U.S. Marshals Service (Usms), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
USMS 1	0	1	3	7	0
USMS 2	0	5	27	14	5
USMS 3	0	1	2	7	0
USMS 4	0	3	1	7	0
Total	**0**	**10**	**33**	**35**	**5**
Percent	0.0	12.0	39.8	42.2	6.0

Source: GAO analysis of security compliance review reports provided by Justice.

Table II.8: Number of SCRG Findings at Community Relations Service (Crs) and U.S. Trustees Office (Ust), by Security Findings Category

	Security findings category				
	Physical	Personnel	Information	Computer	Communication
CRS	0	2	1	4	0
Percent	0.0	28.6	14.3	57.1	0.0
UST	6	4	5	6	0
Percent	28.6	19.0	23.8	28.6	0.0

Source: GAO analysis of security compliance review reports provided by Justice.

Security Violations Within the FBI's Headquarters Building

The Security Unit, Facilities Management and Security Section, Administrative Services Division, is responsible for the physical security of the FBI's J. Edgar Hoover Building. This unit provides the armed guards and security patrols, and controls the security control badges used to enter the building. The Security Unit is also responsible for controlling access into the FBI headquarters building and conducting security and safety checks.

Security Patrols at FBI Headquarters

Between the hours of 6 p.m. and 5 a.m., FBI security patrol personnel are supposed to check every room in the J. Edgar Hoover Building for security and safety violations. If a patrol finds a violation, they are to write up the circumstances on a Security Patrol Violation Report form. The report includes the location of the violation, the violation that was discovered, any file or control numbers of documents found unsecured, safe numbers of safes left unsecured, serial numbers of weapons found unsecured, etc. The patrol is to submit all violation reports to the Security Unit. Also, the patrol is to leave a security violation notification card both inside and on top of the safe, file cabinet, or desk found unsecured. If the violation involves unsecured documents or weapons, the patrol is supposed to secure the documents or weapon in a safe, file cabinet, or desk. If the document or weapon cannot be secured, the patrol is to bring the item to the Security Unit, where it is to be secured in the Security Unit's safe. When the responsible employee finds the violation notice, he or she is required to call the Security Unit and come down to retrieve the item.

Once a month, a summary of all violations found is prepared by the FBI's Security Unit and sent to the assistant director of each division and to the Security Program Manager. These monthly reports are a synopsis of the daily reports and, while every violation found is noted on the monthly report, it may only list a representative sample of files or control numbers of documents found unsecured. The daily reports contain the numbers of all documents and files found unsecured.

Security Violations From 1990 Through 1992

On the basis of the monthly security reports prepared by the Security Unit for 1990, 1991, and 1992, we determined that there were approximately 4,400 security violations reported within the FBI's headquarters building. About 68 percent of these violations were reports of classified materials (top secret, secret, and confidential) being left unsecured within FBI offices. The remaining 32 percent of the reported security violations involved Bureau files and other sensitive documents left unsecured;

cabinets, safes, and offices unlocked; keys to offices and cabinets left out; and secure telephones, badges, and credentials left unsecured within the building.

Overall, the number and percentage of material reported unsecured in any one category varied from year to year. The total number of security violations reported increased from 1990 to 1991 but decreased in 1992. The percentage of unsecured classified documents reported, however, increased each year—58.9 percent in 1990, 70.1 in 1991, and 74.4 percent in 1992. Likewise, the total number of violations reported by division varied from year to year. That is, the rankings of the division by total number of violations changed. But Divisions 6, 3, 5, and 7 had the highest number of violations reported each year.

Tables III.1 through III.4 show the number of violations by FBI division and types of violations for all 3 years combined and for each year 1990, 1991, and 1992, respectively. Figure III.1 shows a comparison of the different types of violations for each of the 3 years, while figure III.2 shows the percentage of each type of violations for all 3 years combined.

Table III.1: Number of Security Violations Reported by the FBI During 1990, 1991, and 1992, by Division

	Materials/documents unsecured					Unlocked safes, cabinets, desks, etc.	Total
	Top Secret	Secret	Confidential	Bureau files	Other sensitive		
Division 1	1	32	0	11	4	5	**53**
Division 3	12	510	23	133	54	60	**792**
Division 4	2	121	7	67	3	11	**211**
Division 5	49	328	8	38	3	81	**507**
Division 6	65	851	135	232	81	129	**1,493**
Division 7	4	117	8	185	65	28	**407**
Division 8	2	158	11	14	10	20	**215**
Division 9	8	128	6	72	2	12	**228**
Division 10	0	82	1	9	1	7	**100**
OCA[a]	0	117	5	8	0	6	**136**
OLIA	1	90	13	7	0	6	**117**
OPA[a]	0	62	3	35	7	6	**113**
OPCA	0	7	0	4	0	0	**11**
EEO	0	18	1	7	1	0	**27**
Total	**144**	**2,621**	**221**	**822**	**231**	**371**	**4,410**
Percent	3.3	59.4	5.0	18.6	5.2	8.4	**100.0**

Legend

EEO = Equal Employment Opportunity
OCA = Office of Congressional Affairs
OLIA = Office of Liaison and International Affairs
OPA = Office of Public Affairs
OPCA = Office of Public and Congressional Affairs

[a]In late 1992, these two offices were combined. The new office is called the Office of Public and Congressional Affairs.

Source: GAO analysis of FBI data.

Table III.2: Number of Security Violations Reported by the FBI During 1990, by Division

	Materials/documents unsecured					Unlocked safes, cabinets, desks, etc.	Total
	Top Secret	Secret	Confidential	Bureau files	Other sensitive		
Division 1	1	3	0	2	3	5	**14**
Division 3	1	100	2	50	28	23	**204**
Division 4	1	76	4	23	2	9	**115**
Division 5	19	79	5	4	0	17	**124**
Division 6	31	232	29	116	56	38	**502**
Division 7	2	20	1	56	26	17	**122**
Division 8	1	47	3	5	7	2	**65**
Division 9	3	26	1	30	1	8	**69**
Division 10	0	39	1	4	1	3	**48**
OCA	0	30	4	3	0	2	**39**
OLIA	0	23	2	0	0	1	**26**
OPA	0	15	0	5	7	4	**31**
EEO	0	4	0	2	1	0	**7**
Total	**59**	**694**	**52**	**300**	**132**	**129**	**1,366**
Percent	4.3	50.8	3.8	22.0	9.7	9.4	**100.0**

Legend

EEO = Equal Employment Opportunity
OCA = Office of Congressional Affairs
OLIA = Office of Liaison and International Affairs
OPA = Office of Public Affairs

Source: GAO analysis of FBI data.

Table III.3: Number of Security Violations Reported by the FBI During 1991, by Division

	Materials/documents unsecured					Unlocked safes, cabinets, desks, etc.	Total
	Top Secret	Secret	Confidential	Bureau files	Other sensitive		
Division 1	0	16	0	6	0	0	**22**
Division 3	5	229	11	54	21	24	**344**
Division 4	1	45	3	41	1	2	**93**
Division 5	20	127	0	13	2	36	**198**
Division 6	25	377	51	72	22	56	**603**
Division 7	1	79	4	98	30	8	**220**
Division 8	0	93	4	6	2	9	**114**
Division 9	2	67	2	27	1	2	**101**
Division 10	0	40	0	4	0	2	**46**
OCA	0	58	0	5	0	3	**66**
OLIA	1	39	5	3	0	1	**49**
OPA	0	34	3	20	0	1	**58**
EEO	0	7	0	4	0	0	**11**
Total	**55**	**1,211**	**83**	**353**	**79**	**144**	**1,925**
Percent	2.9	62.9	4.3	18.3	4.1	7.5	**100.0**

Legend

EEO = Equal Employment Opportunity
OCA = Office of Congressional Affairs
OLIA = Office of Liaison and International Affairs
OPA = Office of Public Affairs

Source: GAO analysis of FBI data.

Table III.4: Number of Security Violations Reported by the FBI During 1992, by Division

	Materials/documents unsecured					Unlocked safes, cabinets, desks, etc.	Total
	Top Secret	Secret	Confidential	Bureau files	Other sensitive		
Division 1	0	13	0	3	1	0	**17**
Division 3	6	181	10	29	5	13	**244**
Division 4	0	0	0	3	0	0	**3**
Division 5	10	122	3	21	1	28	**185**
Division 6	9	242	55	44	3	35	**388**
Division 7	1	18	3	31	9	3	**65**
Division 8	1	18	4	3	1	9	**36**
Division 9	3	35	3	15	0	2	**58**
Division 10	0	3	0	1	0	2	**6**
OCA[a]	0	29	1	0	0	1	**31**
OLIA	0	28	6	4	0	4	**42**
OPA[a]	0	13	0	10	0	1	**24**
OPCA	0	7	0	4	0	0	**11**
EEO	0	7	1	1	0	0	**9**
Total	**30**	**716**	**86**	**169**	**20**	**98**	**1,119**
Percent	2.7	64.0	7.7	15.1	1.8	8.8	**100.0**

Legend

EEO = Equal Employment Opportunity
OCA = Office of Congressional Affairs
OLIA = Office of Liaison and International Affairs
OPA = Office of Public Affairs
OPCA = Office of Public and Congressional Affairs

[a]In late 1992, these two offices were combined. The new office is called the Office of Public and Congressional Affairs.

Source: GAO analysis of FBI data.

Methodology for Categorizing Security Violations Shown in Tables III.1 Through III.4:

We grouped the security violations reported by the FBI in its monthly reports into one of following categories: (1) Top Secret; (2) Secret; (3) Confidential; (4) Bureau files; (5) other sensitive; or (6) unlocked safes, cabinets, desks, etc., using the following rationale.

We placed each violation in the category that corresponded to the level of the documents and/or material found unsecured. For example, if it was reported that Bureau files #1234 and #5678 were found on a desk, we

recorded the violation in the Bureau files category; if it was reported that a bar lock cabinet was found open with Secret material inside, we recorded the violation in the Secret category. However, for any incident reported that had more than one classification of items found unsecured, we recorded the violation in the highest security classification noted. For example, if a safe was found unlocked containing Secret, Confidential, and Bureau files, we recorded this in the Secret category.

If more than one violation was found within a room and reported as being from two different locations (such as an unlocked cabinet and someone's desk), we recorded each violation as a separate incident.

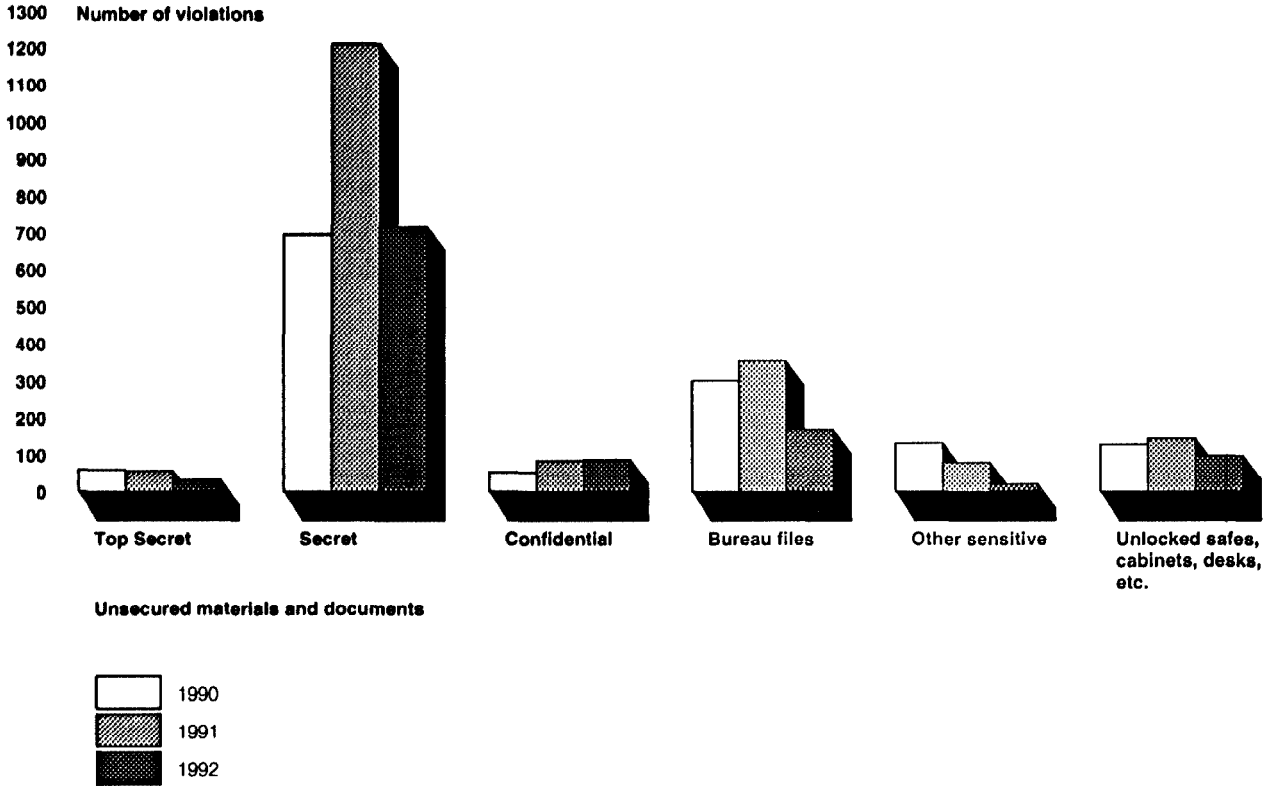
Any report of information identified as being Sensitive Compartmented Information or Special File Room Material that was found unsecured was recorded in the Top Secret category. This was done because the procedures for handling documents classified at these levels are the same.

We recorded incidents of unsecured official trash in the other sensitive category if the level of classification of the material found was not identified. However, if the level of classification of the unsecured official trash was identified, we recorded this incident in the corresponding category.

The other sensitive category also included reports of incidents of documents and/or materials found unsecured and identified as DEA Sensitive, evidence, drug matters, classification matters, signature disk, performance appraisals, or similar items.

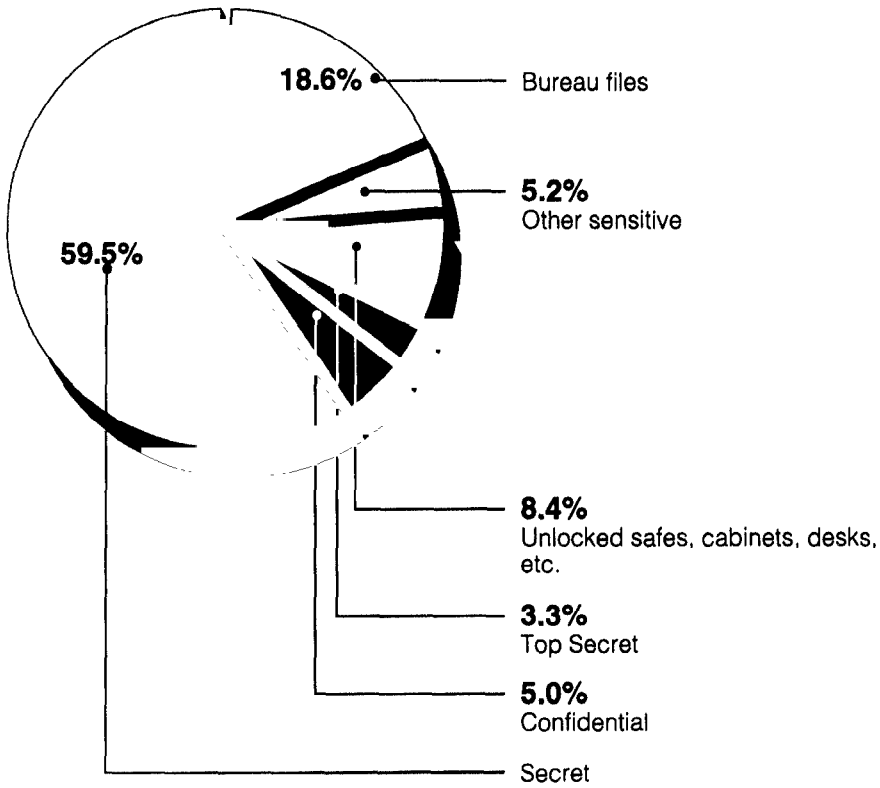
In the unlocked safes, cabinets, desks, etc., category, we included reports of incidents such as when office keys or other special keys, safe combinations, Security Access Control System badges, Special Agent credentials, etc. were found unsecured in open safes, cabinets, desks, or lying about in offices. We also included in this category other incidents such as doors with special "MEDECO" locks being left unsecured or secure telephones found unsecured with keys left in the telephone.

Figure III.1: Number of Security Violations Reported by the FBI, by Types of Violations and Years



Source: GAO analysis of FBI data.

Figure III.2: Percentage of Security Violations Reported by the FBI During 1990, 1991, and 1992 Combined, by Types of Violations



Source: GAO analysis of FBI data.

Examples of Violations Reported by the FBI Nightly Security Patrols

The following are examples of the types of security violations identified and reported by the FBI security patrols during their nightly checks of the FBI headquarters building. These examples are given only as a means for the reader to gain a sense of the types of violations found within each category used in the tables and figures in this appendix.

Top Secret

In May 1992, a safe containing materials marked Top Secret was found unsecured in Division 3.

In February 1992, it was reported that a safe containing Top Secret material was found unsecured in Division 6. In that same month, it also was reported that Top Secret material was found unsecured in another office within Division 6 on four separate occasions.

In August 1991, a cabinet containing Bureau files marked Special File Room was found unsecured in Division 4. In that same month, it was reported that a safe with materials marked Top Secret next to an individual's desk was found unsecured in Division 5.

In February 1991 within Division 3, it was reported that the right side of a credenza containing materials marked Top Secret was found unsecured. In OLIA that same month, it was reported that a cabinet with materials marked Top Secret and a Bureau file marked Special File Room Material were found unsecured in a room with the copy machine.

In February 1990, it was reported that an office door with a special MEDECO key way was found unsecured and that numerous Top Secret materials with Sensitive Compartmented Information control numbers (21 in total) were unsecured on the top of a desk in a Division 6 office.

Secret

In October 1992, a safe and a cabinet in two separate offices in Division 9 were found unsecured, both contained materials marked Secret.

In February 1992, material marked Secret was reported found unsecured on the top of a desk of an individual in the EEO.

Twice in January 1992 and again in February 1992, material marked Secret was found unsecured on the top of one or more desks within the same office in the OCA.

In October 1991, it was reported that an office door with a special key way to Division 8 space was found unsecured and that Secret materials were left unsecured within that office.

On two separate occasions in May 1991, it was reported that a walk-in vault in Division 7 was found unsecured with materials marked Secret. Also in May 1991, it was reported that material marked Secret was found on the desk of a Division 1 employee.

In April 1991, it was reported that a cabinet containing Secret materials was found unsecured in an office in OPA.

In December 1990 within the OCA, it was reported that the desk of an individual was found unsecured with material marked Secret.

On January 10, 11, and 25, 1990, it was reported that materials marked Secret were found unsecured in boxes under a desk in a Division 6 office.

Confidential

In August 1992, material marked Confidential was found unsecured on the top of a desk of an individual in OLIA.

In July 1991 in Division 9, it was reported that a cabinet containing Confidential material was found unsecured.

In June 1991, it was reported that material marked Confidential was found unsecured on the top of an individual's desk in Division 3. In that same report, it was noted that Confidential material was also found unsecured in the outgoing box on the top of a desk of another individual in the same office.

In December 1990, it was reported that a desk of an individual in Division 10 was found unsecured with material marked Confidential.

Bureau Files

In November 1992, Bureau files were found unsecured on the floor beside the desk of an individual in Division 6.

In May 1991, it was reported that a cabinet containing Bureau files was found unsecured at an individual's work station in Division 6.

In September 1990, it was reported that eight bulky Bureau files were found unsecured in an office in Division 7.

In June 1990, it was reported that a cabinet with Bureau files was found unsecured in Division 1.

Other Sensitive Materials

In April 1992, it was reported that unsecured official trash was found near the desk of an individual in Division 1.

In December 1991, it was reported that material marked DEA Sensitive was found unsecured on the top of an employee's desk in Division 6.

In June 1991, it was reported that an evidence room with a special MEDECO key way was found unsecured in Division 7.

In April 1991, it was reported that performance appraisals were found in an unsecured cabinet in Division 3.

Unlocked Safes, Cabinets, Desks, Etc.

In March 1992, it was reported that a secure telephone was found unsecured with the key left in the telephone in a Division 5 office.

In June 1991, it was reported that Security Access Control System badges were found unsecured on the desk of a Division 6 employee.

In August 1990, it was reported that a cabinet containing a Security Access Control System badge and keys to another office cabinet were found unsecured in Division 1.

In May 1990, it was reported that an alarmed door to the Special Records and Filing Unit in Division 4 was found unsecured.

Major Contributors to This Report

General Government Division, Washington, D.C.

Daniel C. Harris, Assistant Director, Administration of Justice Issues
Tim Outlaw, Evaluator-in-Charge
Eduardo N. Luna, Staff Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100