

GAO

United States General Accounting Office

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

July 1990

JUSTICE AUTOMATION

Greater Computer Security Needed



127565

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~document~~ material has been granted by

Public Domain

U.S. General Accounting Office
to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~document~~ owner.

127565

**Information Management and
Technology Division**

B-233809

July 30, 1990

The Honorable Bob Wise
Chairman, Subcommittee on Government Information,
Justice, and Agriculture
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

This report responds to your July 6, 1989, request for information on the Department of Justice's computer security program. Your request was prompted by our earlier review of Project EAGLE, an effort to supply office automation systems to Justice employees. In that review, we found that Justice lacked risk analyses and security plans for the EAGLE systems.¹ Accordingly, you asked us to conduct a more extensive review to determine whether and how Justice is complying with the Computer Security Act of 1987, and other applicable laws and regulations in securing its computer systems.

As agreed with your office, this review focused on security programs in Justice's litigating organizations, which include 94 U.S. Attorney Offices and six divisions—Antitrust, Civil, Civil Rights, Criminal, Land and Natural Resources, and Tax. Because some of the organizations rely on computers at Justice's main data center in Rockville, Maryland, to help perform their legal and prosecutorial functions, we also conducted a limited assessment of security conditions at this facility.

Justice's litigating organizations rely on computer systems to process a variety of highly sensitive information. This information includes the names of defendants, witnesses, informants, and undercover law enforcement officials cited in grand jury proceedings, witness identification programs, and criminal investigations. The dependence on computer systems to process this information presents considerable risks. If the systems fail to protect the information from unauthorized access and disclosure, individuals could be harmed and public trust eroded. Justice must ensure, therefore, that its computer systems have stringent security provisions and effective oversight.

¹Justice Automation: Security Risk Analyses and Plans for Project EAGLE Not Yet Prepared (GAO/IMTEC-89-65, Sept. 19, 1989).

Results in Brief

Justice is not ensuring that its highly sensitive computer systems are adequately protected. We identified many disturbing weaknesses in existing security which, if not corrected, could severely compromise both the computer systems and the sensitive information they process. These weaknesses reflect a lack of effective leadership and oversight by the Justice Management Division, headed by the Assistant Attorney General for Administration. This division is responsible for developing and directing Justice's computer security programs.

Within Justice's seven litigating organizations, for example, we found that contingency plans necessary if services are disrupted either had not been prepared or were not tested, and that no mandatory computer security training was being provided for all employees. We also identified several material weaknesses in physical and other operational security at Justice's main data center in Rockville, Maryland. For example, access to the data center was not properly controlled, and software documentation and utility programs that could be used to bypass normal system security safeguards were available to all employees having access to the data center.

Department security staff in the Justice Management Division do not monitor the organizations' compliance with computer security requirements, or certify sensitive system safeguards as required by federal regulations. Justice management and security officials told us there are not enough staff to oversee the computer security practices of each organization.

We believe the extensive weaknesses we identified are serious enough to be reported under the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512 (1982)). This act states that agencies must establish internal controls, and annually report material weaknesses and the status of corrective actions taken.

This report contains recommendations to the Attorney General to (1) ensure that the computer security weaknesses we found are properly corrected, (2) strengthen the Justice Management Division's leadership and oversight of departmental computer security programs, and (3) report the computer security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act.

Background

Through its litigating organizations, Justice represents the government in federal legal matters that include performing investigations, conducting grand jury proceedings, and preparing and trying cases and appeals. To perform these functions, the litigating organizations rely on their computer systems to process a variety of sensitive information, including the names of defendants, witnesses, informants, and undercover law enforcement officials. Some litigating organizations also use Justice's main data center in Rockville, Maryland, to process sensitive information. Justice moved to this data center in September 1989, in part to improve the security of its computer operations. Approximately 18,000 users, including employees in the Criminal and Land and Natural Resources Divisions, Drug Enforcement Administration, and Bureau of Prisons, access the data center through dedicated leased lines, dial-up lines, and commercial computer networks.

Because the computer systems contain sensitive information, they are subject to the requirements of the Computer Security Act of 1987 (PL 100-235). The Computer Security Act requires federal agencies to identify and develop security plans for computer systems that they designate as containing sensitive information,² and to establish mandatory computer security training to make employees aware of their specific responsibilities and how to fulfill them.

The Federal Information Resources Management Regulation (FIRMR) (41 C.F.R. part 201-7) and Office of Management and Budget (OMB) policies³ further require agencies to protect access to and operation of computer systems by (1) conducting risk analyses, (2) preparing and testing contingency plans, and (3) conducting security certifications and audits.

Justice directives establish uniform policy for protecting computer systems and classified or sensitive information stored, processed, or handled by these systems, and assign responsibilities for implementing

²In response to the Computer Security Act of 1987, Justice's litigating organizations identified and prepared security plans for 19 computer systems that they designated as containing sensitive information.

³Office of Management and Budget Circular No. A-130, App. III., Management of Federal Information Resources, Dec. 12, 1985.

computer security.⁴ The department security staff in the Justice Management Division is responsible for establishing and enforcing compliance with Justice's computer security programs. This responsibility includes ensuring the adequacy of security safeguards in each organization.

Computer Security Weaknesses Identified in the Litigating Organizations

Our review identified many disturbing weaknesses in computer security programs being implemented by Justice's litigating organizations. Collectively, these weaknesses pose a significant risk to the integrity of computer systems and sensitive information in the organizations.

Risk Analyses for Three Organizations May Not Adequately Assess Security Deficiencies

Three of Justice's litigating organizations—the U.S. Attorney Offices and Criminal and Tax Divisions—have begun performing risk analyses that may not adequately assess computer security vulnerabilities and threats. Risk analyses are a critical step for ensuring that adequate security safeguards exist in these organizations.

In our September 1989 report on Project EAGLE, we pointed out that the U.S. Attorney Offices and Criminal and Tax Divisions planned to acquire EAGLE systems. At that time, however, we noted that these organizations had not conducted risk analyses to ensure that sensitive information in the EAGLE systems would be adequately protected against unauthorized access and disclosure. We pointed out, and Justice officials agreed, that risk analyses should be performed before installing the EAGLE systems.

During this review, these organizations began performing risk analyses for their EAGLE systems, using automated risk analysis software.⁵ Justice officials explained that this software will provide a simple and inexpensive approach to assessing risks. However, we identified various limitations in the software, which may prevent an adequate assessment of vulnerabilities and threats:

⁴U.S. Department of Justice, Automated Information Systems Security (DOJ 2640.2B), Nov. 16, 1988; and U.S. Department of Justice, Security Programs and Responsibilities, (DOJ 2600.2B), July 10, 1989.

⁵This software is a commercially marketed survey, on microcomputer diskette, which is designed to be completed by a user of the computer system under review. It is used to collect baseline information about the computer and its environment, and identify security measures in place.

- The software determines whether computer security controls exist, but does not measure the quality of the controls. For example, the risk analysis survey asks if a contingency plan has been prepared, but does not evaluate the plan's adequacy. Thus, a poorly prepared plan is considered the same as a well-designed plan. Without measuring quality, Justice may obtain misleading assessments of actual security conditions in its organizations.
- The software is designed to provide only a general assessment of security risks. To perform the assessment, Justice officials specified a limited number of security safeguards that the risk analysis survey will look for in each facility. However, the assessment will not consider any other safeguards not specified on the survey. For example, the software will not assess network controls and, therefore, will not measure the vulnerability of a networked system. The basic EAGLE architecture features microcomputers connected via a local area network to minicomputers. A risk analysis should examine the total security posture of a facility to point out existing vulnerabilities and risks. It then assembles the basic facts necessary for selecting the required protective measures. By following this generalized approach, Justice stands to overlook critical security vulnerabilities and risks, and may not recognize the need for protective measures that might be found during a more extensive analysis.
- Justice, in using this software, cannot estimate the cost of potential damages resulting from unfavorable events, or their likelihood of occurrence, because the software does not provide this capability. This information is fundamental to deciding how much to spend on computer security, as the cost of security measures should relate to the potential losses they protect against. Moreover, the aim of a risk analysis is to help management strike an economic balance between the impact of risks and the cost of protective measures.
- Justice has not sufficiently tested the software to ensure that it will provide a reliable risk assessment. Such a test would include, for example, comparing the results obtained using the software to results obtained from a traditional, nonautomated analysis of security risks. However, Justice intends to use only this software to assess security in the three organizations. According to an official at the National Institute of Standards and Technology, an automated risk analysis such as the one being performed by Justice is designed to complement, rather than replace, other traditional risk analysis techniques. By relying solely on this software, Justice cannot be certain that all computer security vulnerabilities and risks will be detected. Consequently, threats may be understated and sensitive information may be compromised.

We are also concerned about separation of duties because the same Justice officials responsible for managing computer security in these organizations also will be responsible for performing the risk assessments and analyzing the results. A separation of duties, such as by requiring officials outside these organizations to perform independent assessments, would better ensure the integrity of the risk analysis results.

Security Deficiencies in Four Organizations Need to Be Corrected

Four of Justice's litigating organizations—the Antitrust, Civil, Civil Rights, and Land and Natural Resources Divisions—completed risk analyses during our review. Each of the analyses pointed out serious computer security vulnerabilities that need to be corrected. Among other things, the analyses revealed that Justice

- had not conducted periodic audits and reviews of sensitive applications and certified the adequacy of security safeguards,
- did not have a formal automated data processing (ADP) security awareness training program, and
- had not adequately trained its information and computer security officers to perform their security duties.

Security officials in these organizations corrected some of the deficiencies identified in the risk analyses, such as installing fire alarms in computer rooms and labeling communications equipment. However, other deficiencies, including those mentioned above, need to be addressed by the department security staff in the Justice Management Division. At the time of our review, the department security staff were unaware of the need to address these deficiencies because they had not reviewed the risk analyses.

Contingency Plans Not Prepared or Tested

Within the litigating organizations, we found that contingency plans documenting emergency response, backup, and recovery procedures either had not been prepared or were not tested to ensure that data processing would continue if services were disrupted. As previously noted, FIRMR and OMB policies require agencies to develop and maintain contingency plans to provide continuity of data processing if normal operations are interrupted. Justice's security directive further requires the organizations to review, modify, and test their contingency plans at least once every year. Given recent hostile attacks on Justice organizations, such as the March 1990 firebombing of a Drug Enforcement Administration office in Fort Myers, Florida, Justice needs to establish effective procedures for continuing operations.

At the time of our review, two organizations—the Tax Division and U.S. Attorney Offices—had not prepared contingency plans for their computer systems. Officials in these organizations recognized the requirement for preparing and maintaining contingency plans, but had not yet established timeframes for doing so. One organization—the Antitrust Division—initiated, but had not completed, preparation of a contingency plan. According to a division official, the plan is expected to be completed by October 1990.

Four organizations—the Civil, Civil Rights, Criminal, and Land and Natural Resources Divisions—completed contingency plans during our review. However, none of the plans met federal guidelines requiring detailed emergency response, backup, and recovery procedures. For example, these plans lacked such details as names and telephone numbers of key personnel to be notified during an emergency, lists of critical hardware and software needed, and procedures for switching to a backup processing system. Moreover, none of the organizations tested their contingency plans to ensure their effectiveness during a disaster. Officials in one organization, the Civil Division, explained that their practice is to study the effectiveness of the plan when an actual problem occurs. By not maintaining and regularly testing their contingency plans, the litigating organizations risk prolonged service disruptions from natural disasters, power outages, fire, or other unplanned events, and increase the potential for compromising sensitive information.

Security Training Not Provided

At the time of our review, none of Justice's litigating organizations had established mandatory computer security training for their employees. The Computer Security Act of 1987 requires each agency to implement a computer security training program to ensure that all employees are aware of their responsibilities and how to fulfill them.

With the exception of some new system users, who generally receive security awareness briefings as part of their introductory system training, we found little evidence that employees are being trained in computer security. Officials responsible for computer security in three of the organizations explained that they do not have enough funds to provide training courses, and as an alternative rely on periodic bulletins and memorandums to keep employees informed of security policies and procedures. Without identifying the frequency and levels of training needed, and providing appropriate computer security training courses to meet these needs, Justice cannot be assured that its employees are

aware of their responsibilities, and are capable of detecting and preventing computer security violations.

Computer Security Weaknesses Identified at Justice's Main Data Center

Our limited assessment of Justice's main data center in Rockville, Maryland, identified several material security weaknesses that could adversely affect the center's operations and pose significant risks to sensitive data used by the litigating organizations. These weaknesses are particularly significant since the data center is, according to Justice, a new, state-of-the-art facility. Justice moved its main data center operations from an older facility in September 1989, as one of several actions taken to improve the security of its computer operations. However, some of the same security weaknesses identified at the old data center still exist at the new facility.

Physical Security Inadequate

We observed inadequate physical security provisions, including a lack of surveillance devices such as cameras or motion sensors, to monitor activities in critical areas of the data center. Guards were not positioned to visually survey activities in the center, and video monitors, where used, lacked recording mechanisms to store and replay information should it be needed. An electronic card key device that records when employees enter and exit the data center was inadequate in that it did not record, store, and generate reports on activities of card holders; therefore, center officials could not reconstruct these events if they needed to investigate a security problem.

We also found magnetic tapes containing sensitive data stored in an open area of the data center and directly along the path of individuals entering and exiting the center through the main door. In addition, we found numerous other uncontrolled entrances to the center through which individuals could easily remove sensitive data. These weaknesses decrease Justice's ability to monitor activities of the data center staff and detect unauthorized access to or destruction of critical computer systems and sensitive information.

Contingency Planning and Risk Assessment Inadequate

We observed a lack of effective contingency planning and risk assessment at the main data center, rendering the center's operations vulnerable to disasters and prolonged disruptions of service. Specifically, at the time of our review, the data center operated without a contingency plan detailing emergency response, backup, and recovery procedures. According to the director of the data center, a contingency plan has been

outlined; however, the plan is not scheduled for completion until September 1991.

A risk assessment of the data center, completed by its staff in September 1989, did not fully measure computer security vulnerabilities and threats. For example, in outlining potential threats and their probabilities of occurrence, the assessment did not consider threats that may be made by data center employees. Moreover, in analyzing physical security vulnerabilities, the assessment did not address critical features such as the lack of cameras, security of data center entrances, and internal physical accessibility to sensitive computer equipment and data. Risks associated with the lack of adequate contingency planning and continuity-of-operations procedures also were not considered. By not considering these vulnerabilities and threats, Justice may have overlooked critical factors that could compromise security at the data center.

Computer Operation Weaknesses

We observed a number of security weaknesses in the data center's computer operations. For example, systems programmers with extensive knowledge of hardware and operating procedures had unescorted access to the data center and were capable of issuing critical computer commands that should have been limited to computer operators. In addition, alternate consoles, which could be used to access sensitive computer systems, were located in unsecured and unmonitored areas of the data center. Software documentation and utility programs that could be used to bypass normal system safeguards were available to all employees having access to the data center. These security weaknesses increase the potential for unauthorized access to and alteration of data files and software, and disclosure of sensitive information.

Security Weaknesses Are Long-standing

The security weaknesses we identified at Justice's main data center reflect long-standing concerns that need to be addressed. Many of these types of weaknesses were identified during Justice's internal audit of its prior data center in 1986, well before its move to the new facility. The audit report recommended among other things that Justice (1) develop contingency plans to ensure continuity of data processing operations, (2) upgrade the card key access control system, and (3) establish appropriate access restrictions to utility programs. Justice agreed that the weaknesses identified highlighted the need for increased attention and oversight by high-level management in ensuring that departmental computer resources are operated in a secure and effective manner.

In discussing security conditions at the main data center, the director of the center agreed that many of these conditions currently exist, but did not agree that they pose a considerable risk to the center's operations and to the compromise of sensitive data processed there. Management and security staff in the Justice Management Division told us they intend to correct the data center security problems. According to these officials, Justice has asked the National Security Agency to survey security at the data center and recommend improvements, in anticipation of Justice's future plans to process classified information at this facility.

Inadequate Oversight Contributes to Computer Security Deficiencies

The computer security weaknesses we identified reflect a lack of adequate leadership and oversight for computer security operations by department security staff in the Justice Management Division. The department security staff is not performing several critical enforcement functions to ensure that adequate computer security controls exist in the litigating organizations and main data center. For example, the security staff does not independently audit and evaluate computer security in these organizations or certify the adequacy of their safeguards. FIRM and OMB policies require agencies to periodically audit and evaluate the adequacy of security safeguards for each sensitive application.

In addition, the security staff has provided the organizations only minimal guidance on training employees to fulfill their computer security responsibilities, and does not have information to assure itself that all Justice employees are receiving the necessary training required by the Computer Security Act. In response to the act, the Justice Management Division prepared and disseminated memorandums suggesting various actions the organizations could take to fulfill their training needs. However, the security staff has not followed up to ensure that each organization has implemented a training program, and computer security training requirements have not been incorporated in Justice's security directive.

In discussing the need for improved leadership and oversight, the department security officer explained that with only three staff currently assigned, he does not have enough staff to perform the required oversight and training functions. According to the department security officer, positions and funding to support increases in the security staff were requested in fiscal years 1989 and 1990. However, an official overseeing Justice's budget told us that these requests were not approved by

the Office of Management and Budget. Nonetheless, management and security staff in the Justice Management Division believed security controls in the litigating organizations were effective for several reasons. First, they believed that Justice employees, having been selected on the basis of background investigations and security clearances, are generally honest and perform in an ethical and trustworthy manner. Second, the officials explained that each organization is required to annually review and report its computer security status to the department security staff, and certify the adequacy of its security safeguards. These requirements, in the opinion of Justice officials, force the organizations to (1) perform an accurate assessment, and (2) ensure that adequate controls are in place. Third, although the officials did not know how many computer security violations had occurred in these organizations, they told us few violations have been reported to the security staff. The department security officer believed a low number of reported violations was evidence that existing security controls are an effective deterrent.

We do not believe these reasons justify the department security staff's failure to comply with Justice's directives requiring it to monitor and enforce security policies. As pointed out earlier in this report, Justice's litigating organizations and main data center have not adhered to various federal requirements for ensuring that sensitive computer systems are adequately protected. Although employee honesty and integrity are critical to protecting organizational assets, these traits should not and cannot be relied upon as a primary security control, and as a substitute for appropriate operational and system safeguards. Given that the main data center can be accessed through dial-up lines and commercial computer networks, Justice also needs to consider those threats that could be generated by outsiders gaining unauthorized access to sensitive systems. For example, dial-up lines and commercial computer networks may enable remote users to introduce viruses and other disruptive software (e.g., time bombs) into vulnerable computer systems.

In addition, the practice of requiring organizations to evaluate and certify the adequacy of their computer security safeguards does not in itself guarantee an adequate assessment of Justice's security. Our review found, for example, that none of the litigating organizations had performed such certifications, although the department security officer stated that this responsibility had been delegated to them. Furthermore, even though the organizations submitted annual status reports documenting their security, the department security staff concluded from its

review of the reports that it could not determine whether all facilities had adequate security, without performing on-site assessments of each facility's security program. In addition, such evaluations, without benefit of an independent assessment by the department security staff, do not adhere to federal requirements. Federal regulations stipulate that persons independent of the facility users and management must conduct periodic audits and evaluations of security safeguards for each sensitive application.

Justice management and security staff also should not assume that a low number of reported computer security violations proves there is effective security in the organizations. According to the department security officer, there is no formal system for specifically tracking computer security violations, and the security staff were unable to provide documentation and specific details on the few incidents they said had occurred. In addition, according to the department security officer, Justice cannot be certain that all identified security violations are reported. The department security officer and an official overseeing reviews of employee misconduct in Justice's Office of Professional Responsibility told us that many staff may not have the technical knowledge to recognize violations when they occur. Moreover, skillful, unauthorized users with valid passwords and prescribed procedures could enter and exit a computer system without ever being detected. This danger is particularly critical at Justice's main data center, where dial-up lines and commercial computer networks provide the capability for unauthorized access to sensitive information without detection.

Security Weaknesses Need to Be Disclosed Under the Financial Integrity Act

The computer security weaknesses identified during our review decrease Justice's ability to provide adequate protection of highly sensitive computer systems and information. These types of weaknesses require review, disclosure, and corrective actions under the provisions of the Federal Managers' Financial Integrity Act (31 U.S.C. 3512 (1982)). Under this act, federal department and agency managers are required to evaluate whether internal control systems have weaknesses that can lead to fraud, waste, and abuse in government operations. The act is a key mechanism that the Congress has put in place to ensure that management controls, including those over automation efforts, are effective, and to hold managers accountable for correcting identified deficiencies. Federal managers are required to annually review their

internal controls and report to the President and the Congress any material weaknesses identified in these controls, along with the status of corrective actions.⁶

In its fiscal years 1985 through 1989 Financial Integrity Act reviews, Justice noted several significant concerns regarding its computer security. However, Justice did not disclose as material weaknesses any of the computer security deficiencies found during our review. Justice was aware of several of these deficiencies following its 1986 internal audit of the data center operations. These weaknesses are important enough to warrant inclusion as material internal control weaknesses that require corrective actions.

Conclusions and Recommendations

Justice is not fulfilling its obligation to ensure that sensitive information and computer systems are protected from unauthorized access and disclosure. We found that (1) the litigating organizations either have not prepared contingency plans or have not tested them; (2) three litigating organizations are performing risk analyses using software that may not adequately assess all of their computer security threats and vulnerabilities; (3) some significant deficiencies identified in risk analyses performed for the four other litigating organizations have not been corrected; and (4) legislatively mandated computer security training is not being provided to ensure that employees in the litigating organizations are aware of their responsibilities. Justice's main data center stands vulnerable to unauthorized access because of deficiencies in physical security. In addition, if operations are disrupted intentionally or accidentally, the center has no contingency plan for providing backup support. The center's overall vulnerability to security violations cannot be determined because a risk assessment completed in 1989 did not consider several weaknesses, such as threats to physical security and continuity of operations.

The lack of active leadership and oversight by department security staff in the Justice Management Division, coupled with a lack of security awareness in Justice's litigating organizations and main data center,

⁶The Office of Management and Budget has defined a material weakness as a specific instance of noncompliance with the Financial Integrity Act of sufficient importance to be reported to the President and the Congress. Such weaknesses would significantly impair the fulfillment of an agency component's mission; deprive the public of needed services; violate statutory or regulatory requirements; significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property, or other assets; or result in a conflict of interest.

have contributed to serious and long-standing computer security weaknesses that may compromise sensitive information. Given the highly sensitive nature of data processed and the current heightened awareness of computer security in general, Justice needs to be more proactive in protecting its computer systems. Moreover, because such weaknesses collectively could affect Justice's ability to carry out its mission, as well as protect its sensitive information, they should be reported as material internal control weaknesses under the Federal Managers' Financial Integrity Act.

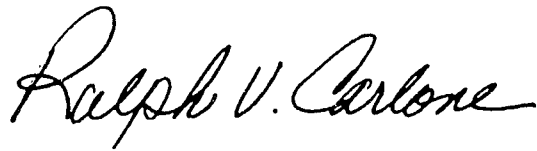
Accordingly, we recommend that the Attorney General take the following actions:

- Immediately correct the security weaknesses described in this report; specifically, ensure that all litigating organizations prepare and test contingency plans, perform thorough risk analyses, correct the problems identified, and establish mandatory computer security training programs.
- Immediately initiate steps at the main data center to ensure that (1) a contingency plan is completed, and physical and computer operation weaknesses we identified are corrected; and (2) a full-scope risk assessment of overall physical, system, and telecommunication security is conducted, and any weaknesses found are corrected.
- Improve the Justice Management Division's leadership and oversight of departmental computer security programs by ensuring that the security staff (1) perform periodic audits and reviews of sensitive systems, (2) certify the adequacy of security safeguards, and (3) monitor the litigating organizations' compliance with computer security training requirements.
- Report the computer security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act, and discuss the actions that will be taken to correct the weakness.

As requested by your office, we did not obtain formal agency comments on this report. However, we discussed the information in the report with Justice officials responsible for agencywide security and program management, and have incorporated their views as appropriate. Additional information on our objectives, scope, and methodology is contained in appendix I. As agreed with your office, unless you publicly announce the report's contents earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies to the Attorney General of the United States and other interested parties.

This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who may be reached at (202) 275-3455. Other major contributors are listed in appendix II.

Sincerely yours,

A handwritten signature in cursive script that reads "Ralph V. Carlone".

Ralph V. Carlone
Assistant Comptroller General

Objectives, Scope, and Methodology

In a July 6, 1989, letter, the Chairman, Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, requested that we determine whether and how Justice is complying with the Computer Security Act of 1987 and other applicable laws and regulations in securing its computer systems. The request was prompted by our earlier review of Project EAGLE, in which we found that Justice did not adhere to the act and Office of Management and Budget policies and guidelines requiring risk analyses and security plans for the EAGLE systems.

Our review focused on security programs in Justice's litigating organizations, which include 94 U.S. Attorney offices and six divisions— Anti-trust, Civil, Civil Rights, Criminal, Land and Natural Resources, and Tax. We also conducted a limited assessment of computer security controls at Justice's main data center in Rockville, Maryland, which is used by some of the litigating organizations to process information.

To assess Justice's efforts to comply with federal computer security laws and regulations, we examined its policies and procedures for securing automated information resources and other relevant documents describing computer security requirements, responsibilities, and practices in the litigating organizations. We interviewed security program officials in each litigating organization and officials responsible for agencywide security and program management in the Justice Management Division. To assess the extent of reported computer security violations, we also interviewed responsible staff in the Offices of Inspector General and Professional Responsibility.

Our assessment of Justice's main data center was limited to a review of existing physical and other operational security controls. The review did not examine technical and system controls such as data encryption and user identification and authentication.

We performed our work between September 1989 and June 1990, in accordance with generally accepted government auditing standards. As requested by your Office, we did not obtain formal comments on a draft of this report. We did, however, discuss the information in this report with Justice officials and have included their comments where appropriate.

Major Contributors to This Report

Information
Management and
Technology Division,
Washington, D.C.

Stephen A. Schwartz, Assistant Director
William D. Hadesty, Technical Assistant Director
Valerie C. Monroe, Senior Evaluator-in-Charge
Richard L. Sumner, Senior Evaluator

Particulars of the ...

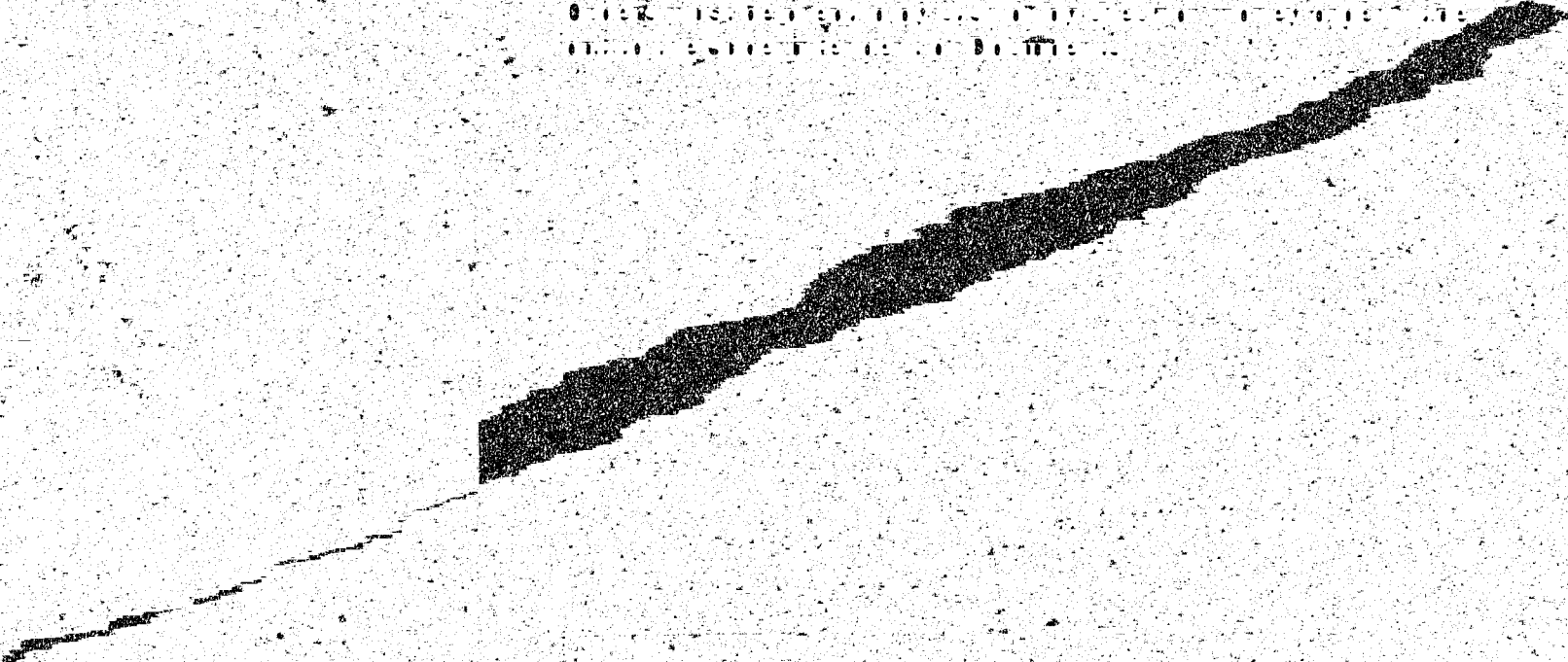
By ...
...
...

...

...

...

...



U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON, D.C. 20540

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G-100

