United States Government Accountability Office

GAO

Report to the Honorable F. James Sensenbrenner Jr., House of Representatives

April 2007

INFORMATION SECURITY

FBI Needs to Address Weaknesses in Critical Network

GAO
Accountability * Integrity * Reliability

GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-368, a report to F. James Sensenbrenner Jr., House of Representatives

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) relies on a critical network to electronically communicate, capture, exchange, and access law enforcement and investigative information. Misuse or interruption of this critical network, or disclosure of the information traversing it, would impair FBI's ability to fulfill its missions. Effective information security controls are essential for ensuring that information technology resources and information are adequately protected from inadvertent or deliberate misuse, fraudulent use, disclosure, modification, or destruction.

GAO was asked to assess information security controls for one of FBI's critical networks. To assess controls, GAO conducted a vulnerability assessment of the internal network and evaluated the bureau's information security program associated with the network operating environment. This report summarizes weaknesses in information security controls in one of FBI's critical networks.

What GAO Recommends

GAO recommends several actions to fully implement an information security program. In a separate classified report, GAO makes recommendations to correct specific weaknesses. FBI agreed with many of the recommendations but disagreed with the characterization of risk to its information and noted that it has made significant strides in reducing risks. GAO believes that increased risk remains.

www.gao.gov/cgi-bin/getrpt?GAO-07-368.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

April 2007

INFORMATION SECURITY

FBI Needs to Address Weaknesses in Critical Network

What GAO Found

Certain information security controls over the critical internal network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources. Specifically, FBI did not consistently (1) configure network devices and services to prevent unauthorized insider access and ensure system integrity; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, these weaknesses place sensitive information transmitted on the network at risk of unauthorized disclosure or modification, and could result in a disruption of service, increasing the bureau's vulnerability to insider threats.

These weaknesses existed, in part, because FBI had not fully implemented key information security program activities for the critical network reviewed. FBI has developed an agencywide information security program, which includes an organization to monitor and protect the bureau's information systems from external attacks and insider misuse and to serve as the central focal point of contact for near-real-time security monitoring. However, shortcomings exist with certain program elements for the network, including an outdated risk assessment, incomplete security plan, incomplete specialized security training, insufficient testing, untimely remediation of weaknesses, and inadequate service continuity planning. Without a fully implemented program, certain security controls will likely remain inadequate or inconsistently applied.

Contents

Abbreviations

C&A	certification and accreditation
DOJ	Department of Justice
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

G A O
Accountability * Integrity * Reliability

**United States Government Accountability Office
Washington, DC 20548**

April 30, 2007

The Honorable F. James Sensenbrenner Jr.
House of Representatives

The Federal Bureau of Investigation (FBI) relies on automated systems and networks to electronically communicate, capture, exchange, and access law enforcement and investigative information. As part of its ongoing efforts to improve information technology capabilities, the bureau deployed and began operating a network in April 2004 as part of its Trilogy modernization effort. Misuse or interruption of this network, or disclosure of the information traversing it, would impair FBI's ability to fulfill its missions. Prior to this network's deployment, misuse was illustrated by former agent Robert Hanssen, who exploited information security weaknesses at the bureau to track the FBI's most sensitive espionage investigations.

In response to your request as Chairman of the House Judiciary Committee for the 109th Congress, we assessed whether FBI has effectively implemented appropriate information security controls on a critical internal network, deployed as part of the Trilogy modernization effort, to protect the confidentiality, integrity and availability of its law enforcement and investigative information. Such controls are essential for ensuring that information technology resources and information are adequately protected from inadvertent or deliberate misuse, fraudulent use, disclosure, modification, or destruction.

This report summarizes shortcomings identified in information security controls on this critical internal network. It does not always contain specific examples of the weaknesses identified due to the sensitive nature of the information discussed.

Results in Brief

Certain information security controls over the critical internal network were ineffective in protecting the confidentiality, integrity, and availability of law enforcement and investigative information. Specifically, FBI did not consistently (1) configure network devices and services securely to prevent unauthorized insider access; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply

strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, these weaknesses place sensitive information transmitted on the network at increased risk of unauthorized disclosure or modification, and could result in a disruption of service.

These weaknesses existed, in part, because FBI had not fully implemented key information security program activities for the network reviewed. FBI has developed an agencywide information security program, which includes an organization to monitor and protect the bureau's information systems from external attacks and insider misuse and to serve as the central focal point of contact for near-real-time security monitoring. However, shortcomings exist with certain program elements for the network, including an outdated risk assessment, incomplete security plan, incomplete specialized security training, insufficient testing, untimely remediation of weaknesses, and inadequate service continuity planning. Also, although the bureau had documented information security policies and procedures, it lacked detailed standards that addressed some of the weaknesses identified. Without a fully implemented program, security controls will likely remain inadequate or inconsistently applied.

We are making recommendations to the FBI Director to take several steps to fully implement key activities of the bureau's information security program for the network. These activities include updating assessments and plans to reflect the bureau's current operating environment, providing more comprehensive coverage of system tests and correcting weaknesses in a timely manner. In a separate classified report, we are making recommendations to address the specific control weaknesses identified.

In commenting on a draft of this report, the FBI Chief Information Officer concurred with many of our recommendations, but did not believe that the bureau had placed sensitive information at an unacceptable risk for unauthorized disclosure, modification, or insider threat exploitation. He cited significant strides in reducing risk since the Robert Hanssen espionage investigation. However, we believe that until weaknesses identified in network devices and services, identification and authentication, authorization, cryptography, audit and monitoring, physical security, and patch management are addressed, increased risk to FBI's critical network remains. Further, until the bureau fully and effectively implements certain information security program activities for the network, security controls will likely remain inadequate or inconsistently applied.

Background

Information security is critical for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. These concerns are well founded for a number of reasons, including a dramatic increase in reports of security incidents, ease of obtaining and using hacking tools, a steady advance in the sophistication and effectiveness of attack technology, and dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are similarly at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, or inappropriate disclosure of sensitive data. We have designated information security as a governmentwide high-risk area since 1997[1]—a designation that remains today.[2]

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA)[3] in December 2002 to strengthen the security of information and systems within federal agencies. FISMA requires each agency, using a risk-based approach to information security management, to develop, document, and implement an agency-wide information security program to provide information security for the information and systems that support the operations and assets of the agency—including those operated or maintained by contractors or others on behalf of the agency.

[1] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[2] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[3] Title III, E-Government Act of 2002, P.L. 107-347 (Dec. 17, 2002).

FBI Operations

The Federal Bureau of Investigation (FBI), which is a component of the Department of Justice (DOJ), has mission responsibilities that include investigating serious federal crimes, protecting the nation from foreign intelligence and terrorist threats, and assisting other law enforcement agencies. Over 12,000 special agents and 16,000 analysts and mission support personnel are located in the bureau's Washington, D.C., headquarters and in more than 70 offices in the United States and 50 offices in foreign countries.

Mission responsibilities at the bureau are divided among the following five major organizational components.

- Administration: manages the bureau's personnel programs, budgetary and financial services, records, information resources, and information security.
- National Security: integrates investigative and intelligence activities against current and emerging national security threats, and provides information and analysis for the national security and law enforcement communities.
- Criminal Investigations: investigates serious federal crimes and probes federal statutory violations involving exploitation of the Internet and computer systems.
- Law Enforcement Services: provides law enforcement information and forensic services to federal, state, local, and international agencies.
- Office of the Chief Information Officer: develops the bureau's information technology strategic plan and operating budget and develops and maintains technology assets.

The organizational components are further organized into subcomponents, such as divisions, offices, and other groups.

The FBI Security Division, within the Administration component, and the Office of the Chief Information Officer collaborated to establish information security initiatives. One initiative included the establishment of the Enterprise Security Operations Center (ESOC), which monitors and protects FBI's systems from external attacks and insider misuse and ensures the availability, confidentiality, and nonrepudiation of FBI information. A second initiative was the deployment of a Public Key

Infrastructure, which provided strong authentication of users' identification to applications.

To execute its mission responsibilities, FBI relies extensively on information technology. The bureau operates and maintains hundreds of computerized systems, networks, databases, and applications. Recognizing the need to modernize its computer systems and networks, FBI proposed a major technology upgrade plan to Congress in September 2000. The Information Technology Upgrade Project, which FBI subsequently renamed Trilogy, was FBI's largest automated information systems modernization initiative to date. Trilogy consisted of three parts: (1) the information presentation component to upgrade computer hardware and software, (2) the transportation network component to upgrade the communication network, and (3) the user application component to upgrade and consolidate the most important investigative applications.

FBI completed the first two components—the information presentation and the transportation network—in April 2004, upgrading its information technology infrastructure with new desktop computers and deploying a wide area network to enhance electronic communication among offices and with other law enforcement organizations. The data traversing the network includes privacy act and sensitive investigative information.

Previously Reported Information Security Weaknesses

FBI information system security weaknesses have been exploited by insiders in the past. The U.S. Secret Service, along with CERT® Coordination Center,[4] studied insider threats, and stated in a May 2005 report that "insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases." The espionage of Robert Hanssen, a former FBI agent, illustrated how an insider can take advantage of inadequacies in the bureau's information system security controls. After discovery of Hanssen's espionage, in 2001, the Attorney General commissioned an outside review of FBI's security program. The commission found significant deficiencies in bureau information security policies and practices, in areas such as certification and accreditation

[4] CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

(C&A),[5] physical security, security awareness training, access control, and auditing. The report stated that those deficiencies flow from a pervasive inattention to security, which had been at best a low priority. Additionally, shortly after Hanssen's arrest in 2001, the Senate Select Committee on Intelligence and the Attorney General requested that the DOJ Office of Inspector General (OIG) review FBI's performance in deterring, detecting, and investigating the espionage activities. The report pointed out that the agent exploited serious weaknesses in FBI's information security and made a specific recommendation on detecting improper computer usage and enforcing "need to know"—granting access only when it is an operational necessity. According to agency officials, the bureau is addressing this and other recommendations.

Objective, Scope, and Methodology

The objective of our review was to determine whether the FBI has effectively implemented appropriate information security controls on a critical internal network, deployed as part of the Trilogy modernization effort, to protect the confidentiality, integrity, and availability of its law enforcement and investigative information.

To evaluate the effectiveness of the security controls over this critical network, we examined routers, network management servers, switches, firewalls, and controlled interfaces at FBI headquarters. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*,[6] which provides guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data; (2) previous reports from the DOJ OIG; and (3) the Federal Information Security Management Act, which establishes key elements that are required for an effective information security program.

Specifically, we evaluated information system controls that are intended to

- limit, detect, and monitor access to sensitive network computing resources, thereby safeguarding them from misuse and protecting them

[5] Certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system to determine the effectiveness of these controls and identify existing vulnerabilities. Accreditation is the official management decision to authorize operation of an information system. Authorization explicitly accepts the risk remaining after the implementation of an agreed-upon set of security controls.

[6] GAO, *Federal Information System Controls Audit Manual, Volume I–Financial Statements Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

from unauthorized disclosure and modification;

- encrypt sensitive data on the network;
- prevent the introduction of unauthorized changes to application or system software;
- protect physical access to network resources; and
- ensure completion of appropriate background investigations of bureau personnel with privileged access on the network.

In addition, we evaluated FBI's information security program as it related to the network operating environment. Such a program includes key activities such as assessing risk; developing and implementing policies, procedures, and security plans; providing security awareness and training; testing and evaluating control effectiveness; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

To evaluate these controls and activities, we identified and examined pertinent DOJ and FBI security policies and procedures. In addition, to determine whether network security controls were in place, adequately designed, and operating effectively, we conducted vulnerability assessments of the network's key servers, routers, and switches. These assessments included discussions with agency staff to gain an understanding of FBI's processes and controls. In order to take advantage of prior work in this area, we also held discussions with OIG staff and reviewed information security reports pertaining to FBI networks and information systems.

We performed our review at FBI headquarters in Washington, D.C., from March 2006 through December 2006 in accordance with generally accepted government auditing standards.

Certain Controls over FBI's Network Were Ineffective

Weaknesses existed in certain access controls and other controls intended to protect the confidentiality, integrity, and availability of the law enforcement and investigative information transmitted by a critical internal network. Our review of the network revealed weaknesses in access controls and patch management. A key reason for these weaknesses was that, although FBI had developed an information security program, it had not effectively or fully implemented key activities of this program for the network. As a result, sensitive data traversing this network were vulnerable to unauthorized access, disclosure, and modification and these weaknesses could lead to disruptions in FBI operations.

Access Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Access controls include those related to network devices and services, user identification and authentication, authorization, cryptography, audit and monitoring of security-related events, and physical access to information resources. Inadequate controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information, and of disruption of service.

Specific examples associated with the weaknesses reported below are described in more detail in a classified version of this report.

Network Devices and Services

Networks are collections of interconnected computer systems and devices that allow individuals to share resources, such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network, (2) routers that filter and forward data along the network, (3) switches that forward information among segments of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between network devices. The National Security Agency (NSA) offers guidance for securely configuring devices and services. Insecurely configured network devices and services can make a system vulnerable to internal or external threats. Because networks often include both external and internal access points for electronic information assets, failure to secure these assets increases the risk of unauthorized access to sensitive information and systems, or disruption of service.

FBI used various devices to secure its network; however, it did not consistently configure network devices and services to prevent unauthorized access to, and ensure the integrity of, the network.

User Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system needs to be able to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. DOJ policy requires that systems control and limit user access based on identification and authentication of the user, and that each user is authenticated before access is permitted. FBI policy addresses identification and authentication as the foundation for information system access control and for user accountability, with passwords being a means of authentication.

FBI did not adequately control user identification and authentication to ensure that only authorized individuals were granted access to its network devices. As a result, increased risk of unauthorized access to servers and other network devices exists, particularly by insiders.

Authorization

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and data. It means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those programs and files that they need in order to do their work, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory and regulate which users can access it—and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. DOJ policy requires that each individual be granted access to information only when such access is an operational necessity, sometimes referred to as "need to know." Also, the policy requires that system security features have the technical ability to restrict the user's access to only that information which is necessary for operations. Further, FBI policy defines least privilege as determining the minimum set of privileges required to perform job functions, and restricting the user to those privileges and nothing more.

FBI granted rights and permissions to network devices that allowed more access to these devices than users needed to perform their jobs. As a result, increased risk exists that users could perform inappropriate activities.

Cryptography

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Encryption—one type of cryptography—is the process of converting readable or plaintext information into unreadable or ciphertext information using a special value known as a key and a mathematical process known as an algorithm. The strength of a key and an algorithm is determined by their length and complexity—the longer and more complex they are, the stronger they are. FBI policy requires that passwords be encrypted before being transmitted over the network. It also requires that sensitive and classified information be safeguarded such that it is accessible to only those individuals with a "need to know."

FBI did not always safeguard sensitive data using encryption. As a result, sensitive information may be disclosed to unauthorized individuals who do not have a legitimate need for the information.

Audit and Monitoring of Security Relevant Events

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that the audit trails can provide. DOJ policy requires that audit records, including all system transactions, be subject to recording and routine review for inappropriate or illegal activity, and that audit trails should be sufficient in detail to facilitate reconstruction of events if compromise or malfunction occurs. Further, FBI policy requires that audit trails be monitored and reviewed for suspicious activity.

FBI established the Enterprise Security Operations Center (ESOC) to monitor and protect the bureau's information systems from external attacks and insider misuse, and to serve as the central point of contact for near real-time security monitoring.

Although ESOC had established audit and monitoring capabilities, it did not always effectively audit and monitor security-relevant system activity on the network reviewed. As a result, increased risk exists that suspicious activities may not be detected.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. DOJ physical security policy requires that physical access to facilities where information is stored, processed, or transmitted be restricted to cleared and authorized personnel.

FBI did not always effectively implement physical controls. For example, in some instances, personnel did not follow physical security policies and procedures for areas containing sensitive information, creating the potential for unauthorized individuals gaining access to these resources and data.

Other Information Security Controls

In addition to access controls, other important security controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information and systems. These controls include techniques designed to ensure the implementation of secure configurations on network devices and the timely completion of background investigations for personnel with access to information systems.

Patch Management

To protect an organization's information, it is important to ensure that only authorized applications and programs are placed in operation. This process consists of instituting policies, procedures, and techniques to help ensure that all programs and program modifications are properly authorized, tested, and approved. Patch management is an important element in mitigating the risks associated with software vulnerabilities. Up-to-date patch installation could help mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage—including the loss of control of entire systems—thereby enabling malicious individuals to read, modify, or delete sensitive information or disrupt operations. FBI policy recognizes the need to establish management controls to ensure timely and effective implementation of security patches and software upgrades. It also specifies that critical patches be evaluated within 24 hours and installed immediately after being tested, with moderate level of criticality considered within 10 days and installed immediately after testing, and with low level of criticality considered within 10 days and installed with the next standard build of the system.

The bureau's patch management for the network was ineffective. ESOC evaluated and provided patches to operations staff for installation on systems; however, patches were not installed in a timely manner and legacy devices contained obsolete software.

FBI has recognized deficiencies in its patch management process and has identified missing elements needed to implement a more effective patch management process. Also, according to agency officials, the bureau plans to eventually remove legacy devices containing obsolete software from the network. However, until FBI implements an effective patch management program, it is unable to assure the confidentiality, integrity, and availability of devices on its network.

Background Investigations

According to Office of Management and Budget (OMB) Circular A-130,[7] it has long been recognized that the greatest harm to computing resources has been done by authorized individuals engaged in improper activities—whether intentionally or accidentally. Personnel controls (such as screening individuals in positions of trust) supplement technical, operational, and management controls, particularly where the risk and magnitude of potential harm is high. Background screenings (or investigations) help an organization to determine whether a particular individual is suitable for a given position by attempting to ascertain the person's trustworthiness and appropriateness for the position. The exact type and rigor of screening that takes place depends on the sensitivity of the position and applicable regulations by which the agency is bound. FBI policy requires that employees and contractors with access to the network have a top secret clearance, and that individuals with a top secret clearance undergo periodic reinvestigation every 5 years.

FBI generally complied with background investigation requirements. Of the 44 individuals reviewed, 41 had current background investigations that had been completed within the last 5 years. Three individuals' investigations were more than 5 years old by a few months, and re-investigations were in process at the time of our review.

[7] Office of Management and Budget, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (Nov. 28, 2000).

Information Security Program

Weaknesses in access controls and patch management existed, in part, because FBI had not yet effectively or fully implemented key security activities associated with its agencywide information security program for the critical internal network reviewed. Although FBI has developed an information security program, shortcomings exist with certain key elements.

FISMA[8] requires agencies to implement an agencywide information security program that includes

- periodic assessments of the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel—including contractors and other users of information systems—of information security risks and of their responsibilities in complying with agency policies and procedures;
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major information system that is identified in the agencies' inventories;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in their information security policies, procedures, or practices; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[8] FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management.

However, FBI did not fully or effectively implement many of these activities for the critical internal network reviewed.

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. Further, OMB Circular A-130, appendix III, prescribes, as does FBI policy, that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years. The bureau's *Certification & Accreditation Handbook* incorporates a risk management process by requiring documentation in a risk management matrix throughout the lifecycle of a system. This matrix is to address such topics as threats, vulnerabilities, impact of a particular threat exploiting a particular vulnerability, existing or recommended countermeasures to mitigate the risk, business impact of implementing the countermeasures, and a schedule for implementing the recommended countermeasures.

The risk assessment for the network was outdated and incomplete. In 2004, as part of its C&A process, FBI assessed risk for the network and documented threats and vulnerabilities in a risk management matrix, which addressed many of the weaknesses described in this report. However, the bureau had not updated the matrix to reflect significant changes, such as additional connectivity, in the network operating environment. In addition, FBI did not have a comprehensive inventory—an enterprisewide view—that reflected the current operating environment, including new connections as well as interfaces with legacy systems; as such, although individual risk assessments may have existed for these connections or legacy systems, the bureau may not be able to determine how any risks associated with them affect the overall network. Further, the existing matrix did not address business impact or schedule. Inadequately assessing risk can lead to implementing inadequate or inappropriate security controls that might not address the system's true risk; it also can lead to costly efforts to subsequently implement effective controls. Also, other organizations connected to the bureau depended on a risk assessment that was outdated and incomplete.[9]

Policies and Procedures

Another key task in developing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Technical configuration standards provide consistent implementing guidance for each computing environment. Because security policies and procedures are the primary mechanisms by which management communicates its views and requirements, it is important that policies and procedures be established and documented.

FBI has developed and documented high-level information security guidance, but specific guidance did not always exist for the network environment. The bureau's *Security Policy Manual* and *Certification & Accreditation Handbook* provided guidance on topics such as security officer roles and responsibilities, personnel security, badges, identification and authentication, and system certification requirements. However, although technical configuration standards existed for topics such as Windows configuration, other detailed standards did not always exist. Without effectively developing, documenting, and implementing policies, procedures and standards, the bureau has less assurance that its systems and information are protected from unauthorized access.

Security Plans

The objective of system security planning is to improve the protection of information technology resources. A system security plan is intended to provide a complete and up-to-date overview of a system's security requirements and describe the controls that are in place or planned to meet those requirements. FISMA requires that agency information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. OMB Circular A-130 specifies that agencies develop and implement system security plans for major applications and for general support systems and that these plans address policies and

[9] In an Interconnection Security Agreement, documenting whenever a direct connection is made between two or more information systems that are owned and operated by other authorities/organizations, each organization is required to provide and update the C&A approval for the interface systems. Reciprocal acceptance of these documents is expected and any questions or concerns documented and addressed.

procedures for providing management, operational, and technical controls. The National Institute of Standards and Technology (NIST) recommends that security plans include, among other topics, existing or planned security controls, the individual responsible for the security of the system, description of the system and its interconnected environment, and rules of behavior. FBI policy requires that system security plans be developed as part of its C&A process.

FBI had documented a system security plan for the network, but it was incomplete and not up to date. The network security plan included many elements required by NIST, such as the description of individuals responsible for security and rules of behavior. Although the plan addressed management, operational, and certain technical controls, other specific technical controls, such as for communication protection, were not included. Further, the plan did not reflect the current operating environment because it did not completely address system interconnectivity. As a result, FBI and other agencies that connect to the network cannot ensure that appropriate controls are in place to protect their systems and critical information.

Security Awareness Training

Another FISMA requirement for an information security program is that it promote awareness and provide required training for users so that they can understand the system security risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees and contractors who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as their roles and responsibilities, and what they need to do to protect the confidentiality, integrity, and availability of that information. FISMA mandates that all federal employees and contractors who use agency information systems be provided with periodic training in information security awareness and accepted information security practice. DOJ policy requires all personnel who manage, operate, develop, or use automated data processing and telecommunications to take security training and refresher training at least annually. Additionally, FISMA requires agency chief information officers to ensure that personnel with significant information security responsibilities receive specialized training.

FBI provided security awareness to most, but not all, employees and contractors; however, not all individuals with security responsibilities completed the specialized training. The bureau had implemented a security awareness training program that included computer-based training and a database to track completion. In fiscal year 2006, 41 of 44 individuals reviewed completed the training. Additionally, FBI had implemented a specialized security training program that identified a number of roles with significant security responsibilities. Each role had a required computer-based specialized training curriculum, and FBI tracked users' progress and completion of courses. However, for fiscal year 2006, only 17 of 44 individuals reviewed had completed the required specialized training for their role; 11 of 44 individuals had not completed any specialized training; the remainder had completed some but not all of the training. FBI officials explained that the specialized training program was new in fiscal year 2006 and that they had initial problems identifying individuals with significant information security responsibilities along with obtaining an appropriate number of licenses for the training. Until FBI fully implements an effective security awareness and training program, it is at increased risk that individuals could accidentally or intentionally allow unauthorized access to sensitive information.

Tests and Evaluations of Control Effectiveness

Another key element of an information security program is testing and evaluating system controls to ensure they are appropriate, effective, and comply with policies. An effective program of ongoing tests and evaluations can be used to identify and correct information security weaknesses. This type of oversight demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests may encourage compliance with security policies, the full benefits of testing are not achieved unless the test results are analyzed by security specialists and business managers and used as a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls. FISMA requires that agencies test and evaluate the information security controls of their systems and that the frequency of such tests be based on risk, but occur no less than annually. Similarly, the FBI *Certification & Accreditation Handbook* requires periodic testing to ensure that the accredited system has maintained its documented configuration baseline and to identify new vulnerabilities that may be inherent in the system and not previously identified.

Although FBI had various initiatives under way to test and evaluate its network, the tests were not comprehensive. The network had undergone certification testing as part of FBI's C&A process, and ESOC conducts periodic system scans to detect vulnerabilities on its network. However, the bureau, as noted earlier, did not appropriately consider risks associated with the current operating environment. Further, the scans conducted by the monitoring group were limited in capabilities since the group had not been given administrative access to conduct these tests. As a result, certain vulnerabilities were not detected. Without appropriate tests and evaluations, the agency has limited assurance that policies and controls are appropriate and working as intended. Additionally, increased risk exists that undetected vulnerabilities could be exploited to allow unauthorized access to sensitive information.

Remedial Actions

Remedial action plans, also known as plans of actions and milestones, can assist agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses in information systems. According to OMB Circular A-123, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed and progress tracked for each deficiency. FBI's *Certification & Accreditation Handbook* requires that plans of actions and milestones serve as a management tool to address corrective actions associated with system deficiencies and any new vulnerabilities.

FBI did not address remedial actions in a timely manner. For example, the plan of actions and milestones for the network included 15 unresolved weaknesses that were over 2 years old. Eight of these outstanding weaknesses were categorized as "high vulnerability" or "very high vulnerability" weaknesses. Without an effective remediation program, identified vulnerabilities may not be resolved in a timely manner, thereby allowing continuing opportunities for unauthorized individuals to exploit these weaknesses to gain access to sensitive information and systems.

Continuity of Operations

Service continuity controls can enable systems to be recovered quickly and effectively following a service disruption or disaster. Such controls include plans and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a plan to recover critical operations should interruptions occur. These controls should be designed to ensure that when unexpected events occur, key operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. They should also be tested annually or as significant changes are made. It is important that these plans be clearly documented, communicated to potentially affected staff, tested, and updated to reflect current operations. FBI policy requires documented procedures to ensure the continuity of essential functions under all circumstances. In addition, the policy requires regularly scheduled testing of contingency plans.

FBI had not implemented comprehensive continuity of operations plans and procedures for the internal network. Although the bureau had a 2004 contingency plan that reflected the planned Trilogy network environment, the plan did not reflect the current internal network operating environment. FBI also had a contingency plan for its data center, but this plan did not cover the network. Further, there were neither documented test plans nor test results indicating continuity of operations testing had been performed specifically for the network. According to FBI officials, redundancy has been implemented in the internal network to ensure high availability. Officials also stated that recovery of the internal network has already been exercised in many real-life situations. However, until the bureau completes actions to address these weaknesses, it is at risk of not being able to recover from certain service disruptions to the internal network in a timely manner.

Conclusions

Ineffective controls threaten the confidentiality, integrity, and availability of the sensitive law enforcement and investigative information transmitted by the critical internal network. Certain information security control weaknesses existed in network devices and services, identification and authentication, authorization, cryptography, audit and monitoring, physical security, and patch management. The bureau's lack of a comprehensive inventory of the current network operating environment—an enterprisewide view—compounds the effect of these weaknesses. FBI developed an agency-wide information security program; however, key activities associated with this program had not been fully implemented for the network. Until FBI ensures that the information security program associated with the network is fully implemented, there is limited assurance that its sensitive data will be adequately protected against unauthorized disclosure or modification or that network services will not be interrupted. These weaknesses leave the bureau vulnerable to insider threats.

Recommendations for Executive Action

We recommend that the FBI Director take the following eight actions to fully implement information security program activities for the critical internal network reviewed.

- Develop a comprehensive inventory of the current network operating environment.
- Update the network's risk assessment to reflect the current operating environment and ensure that the assessment includes elements required

by the FBI *Certification & Accreditation Handbook*.

- Develop technical standards that include guidance for addressing the access control weaknesses identified.
- Update the network security plan to ensure that it reflects the current operating environment and includes sections required by the FBI *Certification & Accreditation Handbook*.
- Ensure that all network users receive security awareness training and that all users with significant security responsibilities receive specialized training as defined by their role.
- Provide comprehensive coverage of system testing and scans.
- Correct identified weaknesses in a timely manner.
- Develop a continuity of operations plan that addresses the current network environment, and periodically test the plan.

To help strengthen information security controls over the network, we are recommending in a separate classified report that the FBI Director take action to address specific weaknesses associated with network devices and services, identification and authentication, authorization, cryptography, audit and monitoring, physical security, and patch management.

Agency Comments and Our Evaluation

In providing written comments (reprinted in app. I) on a draft of the report, the FBI Chief Information Officer concurred with many of our recommendations to address the weaknesses identified, and noted some instances where weaknesses have already been addressed. However, he took exception to the report's assertion that the collective result of the weaknesses presents an increased risk to FBI information. The bureau does not believe that it has placed sensitive information at an unacceptable risk for unauthorized disclosure, modification, or insider threat exploitation. We believe that until weaknesses identified in network devices and services, identification and authentication, authorization, cryptography, audit and monitoring, physical security and patch management are addressed, increased risk to FBI's critical network remains. Further, as noted in our conclusion, the lack of a comprehensive inventory of the current network operating environment—an enterprisewide view—compounds the effect of these weaknesses.

He also stated that FBI has made significant strides in reducing risk since the Robert Hanssen espionage investigation. For example, according to the Chief Information Officer, since its inception in 2002, the bureau's Information Assurance section has taken FBI from an agency wherein only 8 percent of information systems were accredited to maintaining 100 percent accreditation of its major systems. Further, he stated that the bureau has increased its monitoring capabilities and established a comprehensive vulnerability assessment program. As stated in our report, we acknowledged that FBI has developed an agencywide information security program. However, shortcomings existed in how the bureau implemented certain elements of the program for the network. For example, the network risk assessment associated with the accreditation process was outdated and incomplete. Other shortcomings included an incomplete security plan, incomplete specialized training, insufficient testing, untimely remediation of weaknesses and inadequate service continuity planning. Although positive efforts have been made, until FBI fully and effectively implements key activities of the information security program associated with its network, security controls will likely remain inadequate or inconsistently applied, and the bureau will have limited assurance that sensitive data will be adequately protected against unauthorized disclosure or modification, or that network services will not be interrupted.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to congressional committees with jurisdiction over FBI and executive branch agencies' information security programs, the Attorney General, the FBI Director, the DOJ Inspector General, and other interested parties. We also will make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at www.gao.gov.

If you or your staff have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Keith A. Rhodes at (202) 512-6412 or rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

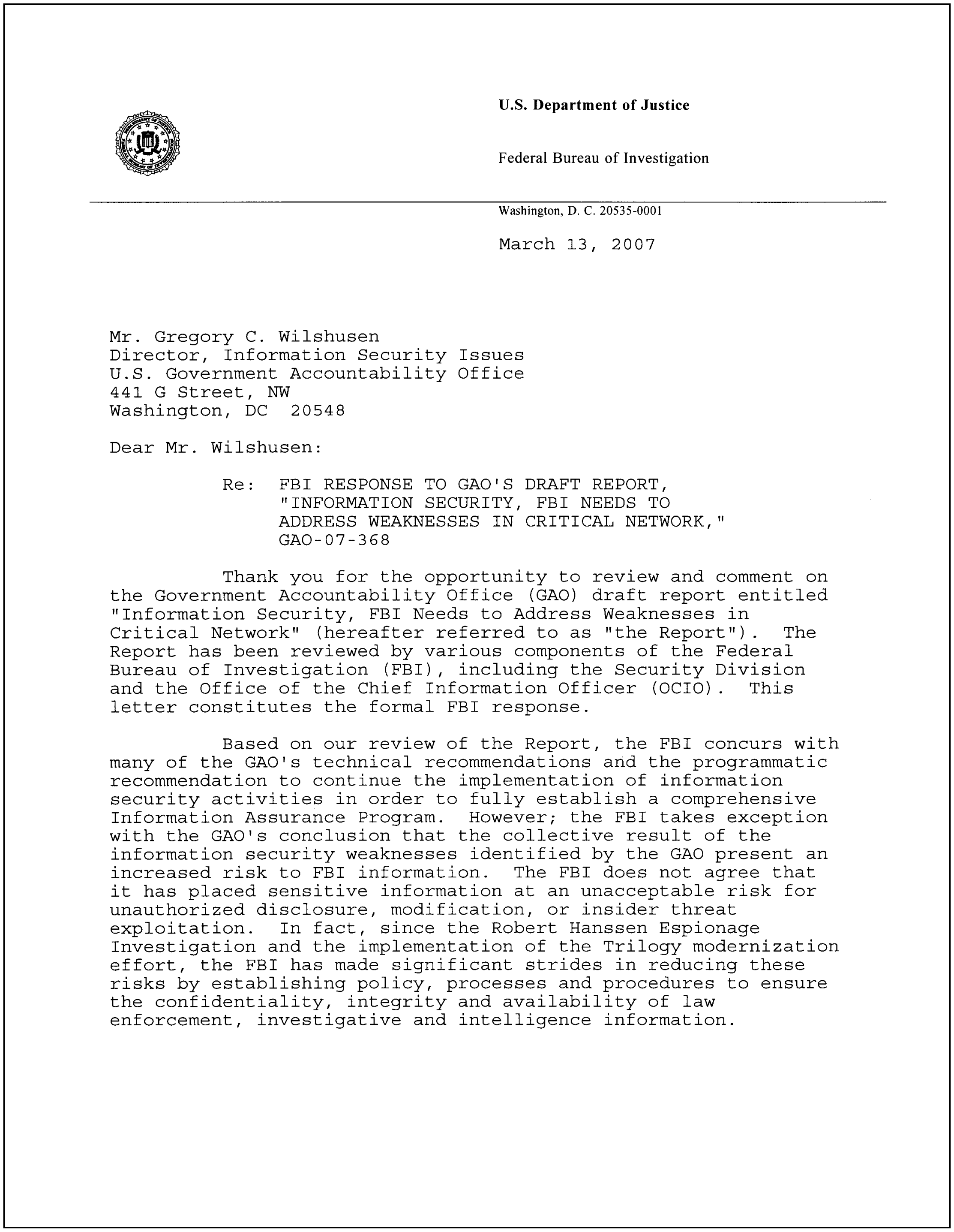
Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes
Chief Technologist

Appendix I: Comments from the Federal Bureau of Investigation



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 13, 2007

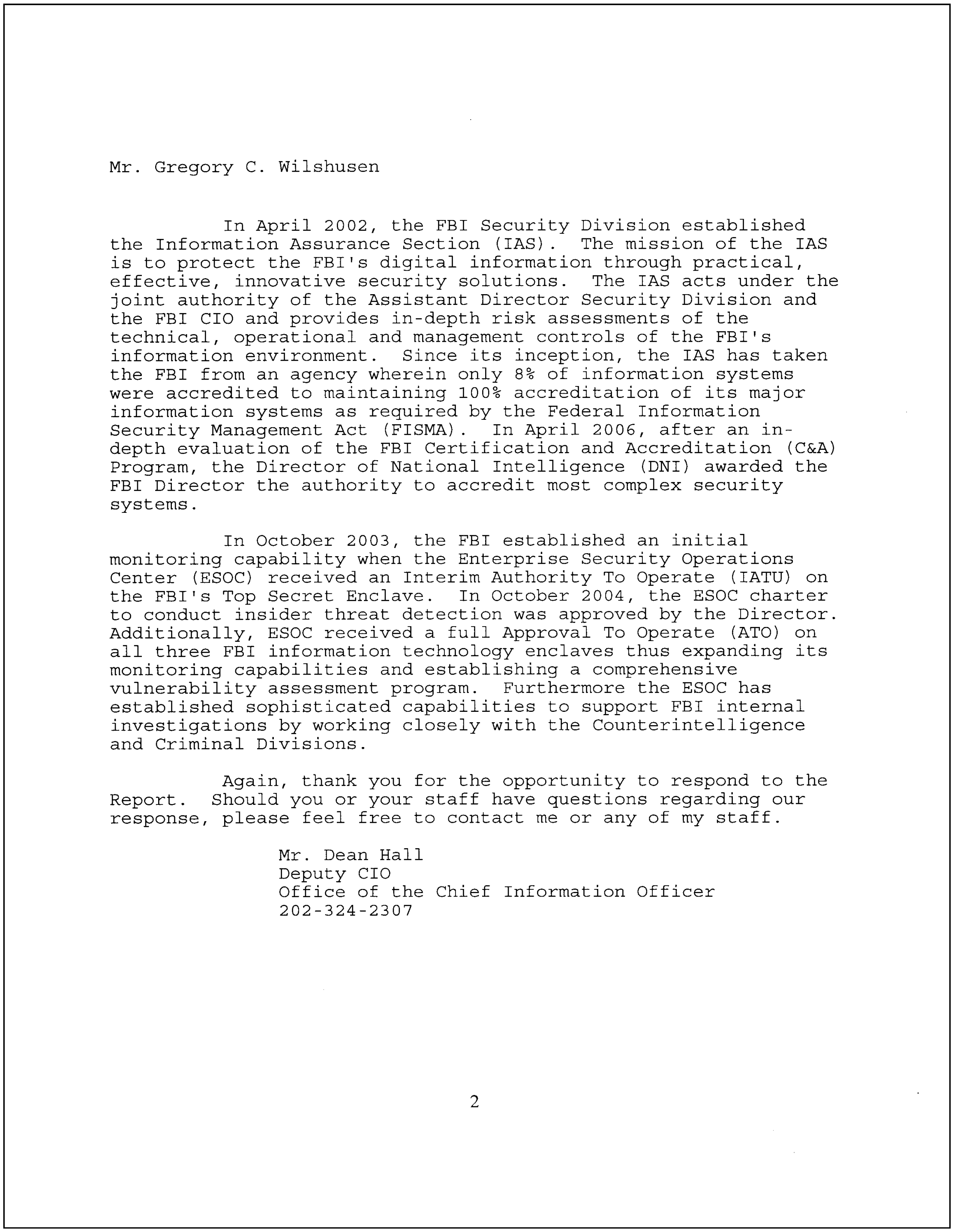
Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Re: FBI RESPONSE TO GAO'S DRAFT REPORT,
"INFORMATION SECURITY, FBI NEEDS TO
ADDRESS WEAKNESSES IN CRITICAL NETWORK,"
GAO-07-368

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled "Information Security, FBI Needs to Address Weaknesses in Critical Network" (hereafter referred to as "the Report"). The Report has been reviewed by various components of the Federal Bureau of Investigation (FBI), including the Security Division and the Office of the Chief Information Officer (OCIO). This letter constitutes the formal FBI response.

Based on our review of the Report, the FBI concurs with many of the GAO's technical recommendations and the programmatic recommendation to continue the implementation of information security activities in order to fully establish a comprehensive Information Assurance Program. However; the FBI takes exception with the GAO's conclusion that the collective result of the information security weaknesses identified by the GAO present an increased risk to FBI information. The FBI does not agree that it has placed sensitive information at an unacceptable risk for unauthorized disclosure, modification, or insider threat exploitation. In fact, since the Robert Hanssen Espionage Investigation and the implementation of the Trilogy modernization effort, the FBI has made significant strides in reducing these risks by establishing policy, processes and procedures to ensure the confidentiality, integrity and availability of law enforcement, investigative and intelligence information.



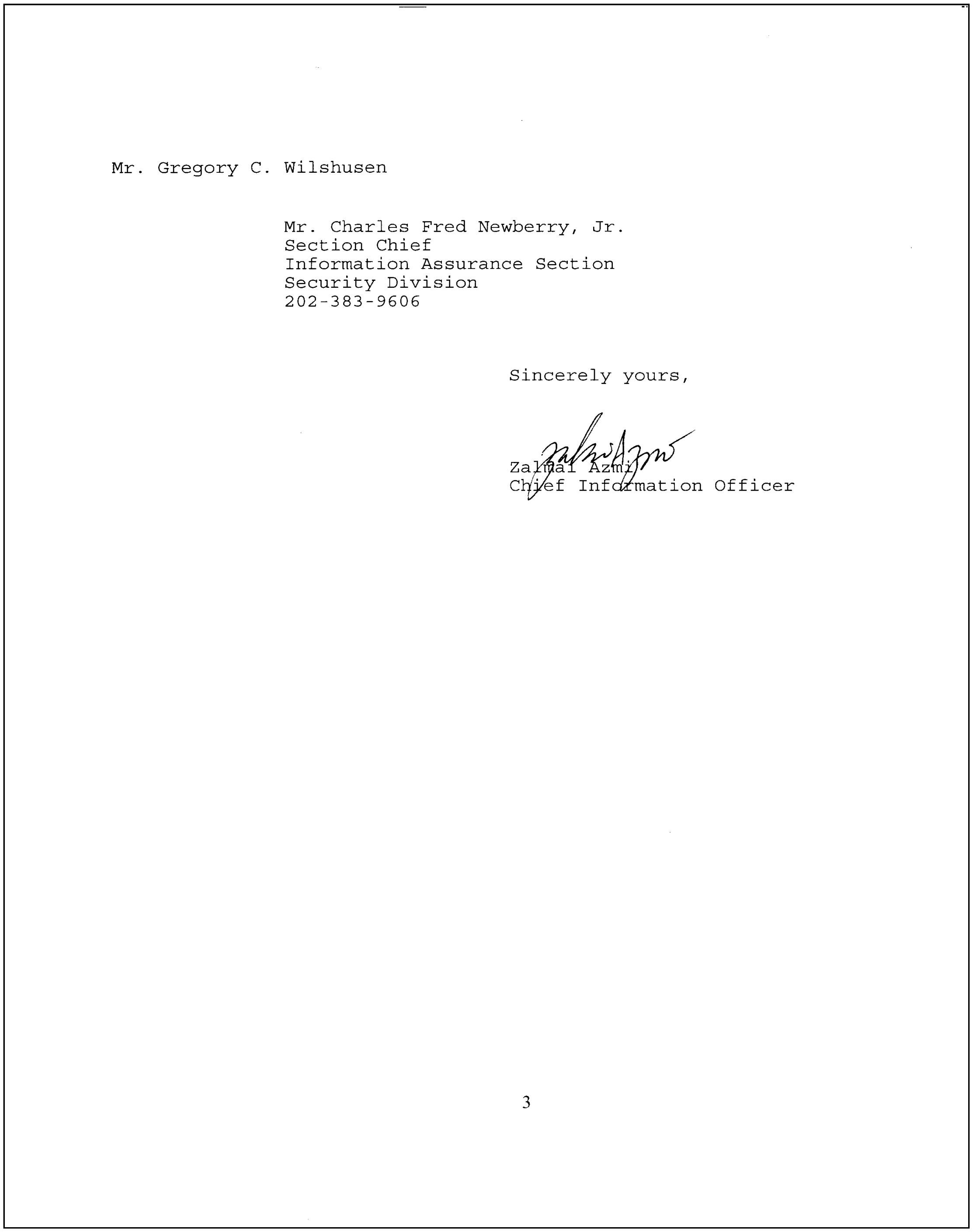
Mr. Gregory C. Wilshusen

In April 2002, the FBI Security Division established the Information Assurance Section (IAS). The mission of the IAS is to protect the FBI's digital information through practical, effective, innovative security solutions. The IAS acts under the joint authority of the Assistant Director Security Division and the FBI CIO and provides in-depth risk assessments of the technical, operational and management controls of the FBI's information environment. Since its inception, the IAS has taken the FBI from an agency wherein only 8% of information systems were accredited to maintaining 100% accreditation of its major information systems as required by the Federal Information Security Management Act (FISMA). In April 2006, after an in-depth evaluation of the FBI Certification and Accreditation (C&A) Program, the Director of National Intelligence (DNI) awarded the FBI Director the authority to accredit most complex security systems.

In October 2003, the FBI established an initial monitoring capability when the Enterprise Security Operations Center (ESOC) received an Interim Authority To Operate (IATU) on the FBI's Top Secret Enclave. In October 2004, the ESOC charter to conduct insider threat detection was approved by the Director. Additionally, ESOC received a full Approval To Operate (ATO) on all three FBI information technology enclaves thus expanding its monitoring capabilities and establishing a comprehensive vulnerability assessment program. Furthermore the ESOC has established sophisticated capabilities to support FBI internal investigations by working closely with the Counterintelligence and Criminal Divisions.

Again, thank you for the opportunity to respond to the Report. Should you or your staff have questions regarding our response, please feel free to contact me or any of my staff.

Mr. Dean Hall
Deputy CIO
Office of the Chief Information Officer
202-324-2307



Mr. Gregory C. Wilshusen

Mr. Charles Fred Newberry, Jr.
Section Chief
Information Assurance Section
Security Division
202-383-9606

Sincerely yours,

Zalmai Azmi
Chief Information Officer

3

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov
Keith A. Rhodes, (202) 512-6412 or rhodesk@gao.gov

Staff Acknowledgments

In addition to the persons named above, Edward Alexander Jr., Michael Derr, Steve Gosewehr, Jeffrey Knott, Duc Ngo, Eugene Stevens, and William Thompson made key contributions to this report.