United States General Accounting Office

GAO

Report to Congressional Requesters

January 2004

INFORMATION SECURITY

Further Efforts Needed to Address Serious Weaknesses at USDA

GAO-04-154

January 2004

INFORMATION SECURITY

Further Efforts Needed to Address Serious Weaknesses at USDA

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-154, a report to congressional requesters

Why GAO Did This Study

The U.S. Department of Agriculture (USDA) performs critical missions that enhance the quality of life for the American people, relying on automated systems and networks to deliver billions of dollars in programs to its customers; process and communicate sensitive payroll, financial, and market data; and maintain personal customer information. Interruptions in USDA's ability to fulfill its missions could have a significant adverse impact on the nation's food and agricultural production.

In addition, securing sensitive information is critical to USDA's efforts to maintain public confidence in the department. GAO was asked to evaluate the effectiveness of USDA's information security controls.

What GAO Recommends

GAO recommends that the Secretary of Agriculture direct the chief information officer (CIO) to correct a number of weaknesses, including fully implementing a comprehensive security management program. In commenting on a draft of this report, USDA concurred with our recommendations and stated that the department remains committed to improving information security. USDA plans to correct the specific information security weaknesses identified and fully implement a comprehensive security management program.

www.gao.gov/cgi-bin/getrpt?GAO-04-154.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

Significant, pervasive information security control weaknesses exist at USDA, including serious access control weaknesses, as well as other information security weaknesses. Specifically, USDA has not adequately protected network boundaries, sufficiently controlled network access, appropriately limited mainframe access, or fully implemented a comprehensive program to monitor access activity. In addition, weaknesses in other information security controls, including physical security, personnel controls, system software, application software, and service continuity, further increase the risk to USDA's information systems. As a result, sensitive data—including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, agricultural production and marketing estimates, and mission critical data—are at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected.

A key reason for the weaknesses in information system controls is that the department has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Although USDA has various initiatives under way, it has not yet fully implemented the key elements of a comprehensive security management program. For example, agency security personnel have lacked the management involvement needed to effectively implement security programs, three agencies have not completed any of the required risk assessments, and security controls have been tested and evaluated for less than half of the department's systems in the past year. USDA has recognized the need to improve information security throughout the department, including in the components that we reviewed.

Contents

Letter 1

Results in Brief 1
Background 2
Objectives, Scope, and Methodology 5
Serious Information Security Weaknesses Exist at USDA 7
Conclusions 24
Recommendations for Executive Action 25
Agency Comments 25

Appendixes

Appendix I: Comments from the Department of Agriculture 27

Appendix II: GAO Contact and Staff Acknowledgments 28
GAO Contact 28
Staff Acknowledgments 28

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act
ID	identification
IDS	intrusion-detection system
ISSPM	Information System Security Program Manager
IT	information technology
NASS	National Agricultural Statistics Service
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Actions and Milestones
TSO	Telecommunications Services and Operations
USDA	U.S. Department of Agriculture

GAO
Accountability * Integrity * Reliability

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

January 30, 2004

The Honorable Thad Cochran
Chairman
Committee on Agriculture, Nutrition, and Forestry
United States Senate

The Honorable Tom Harkin
Ranking Democratic Member
Committee on Agriculture, Nutrition, and Forestry
United States Senate

The Honorable Richard G. Lugar
United States Senate

The U.S. Department of Agriculture (USDA) performs critical missions that enhance the quality of life for the American people, relying on automated systems and networks to deliver billions of dollars in programs to its customers; process and communicate sensitive payroll, financial, and market data; and maintain personal customer information. Interruptions in USDA's ability to fulfill its missions could have a significant adverse impact on the nation's food and agricultural production. In addition, the security of sensitive information is critical to the department's efforts to maintain public confidence in the output, supply, and marketing sectors in agriculture.

At your request, we evaluated the effectiveness of USDA's information security controls. Effective controls are essential for ensuring that sensitive information and information technology resources are adequately protected from inadvertent or deliberate misuse, fraudulent use, or destruction, as well as for protecting information from disclosure.

This report summarizes the information security control weaknesses that we identified during our review. We are also issuing a report designated for "Limited Official Use Only," which describes the weaknesses in more detail.

Results in Brief

Significant, pervasive information security control weaknesses exist at USDA, including serious access control weaknesses, as well as other information security weaknesses. Specifically, USDA has not adequately protected network boundaries, sufficiently controlled network access, appropriately limited mainframe access, or fully implemented a

comprehensive program to monitor access activity. In addition, weaknesses in other information security controls, including physical security, personnel controls, system software, application software, and service continuity, further increase the risk to USDA's information systems. As a result, sensitive data—including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, agricultural production and marketing estimates, and other mission critical data—are at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected.

A key reason for the weaknesses in information system controls is that the department has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Although USDA has various initiatives under way, the key elements of a comprehensive security management program are not yet fully implemented. For example, agency security personnel have lacked the management involvement needed to effectively implement security programs, three agencies have not completed any of the required risk assessments, and security controls have been tested and evaluated for less than half of the department's systems in the past year. USDA has recognized the need to improve information security throughout the department, including the components that we reviewed.

We are making a recommendation to fully implement a comprehensive information security management program. In the separate report designated "Limited Official Use Only," we are making recommendations to correct the specific weaknesses identified during our review.

In providing written comments on a draft of this report, USDA's Chief Information Officer (CIO) concurred with our recommendations and stated that the department remains committed to improving information security. USDA plans to fully implement a comprehensive security management program as well as correct the specific information security weaknesses identified.

Background

USDA's missions are diverse, covering a wide range of responsibilities that include ensuring a safe, affordable, nutritious, and accessible food supply; caring for agricultural, forest, and range lands; providing economic opportunities for farm and rural residents; and expanding global markets for agricultural and forest products and services. To support its missions,

USDA employs approximately 114,000 people in 29 agencies and staff offices covering 7 mission areas with over 7,000 offices throughout the United States. For fiscal year 2004, its proposed budget is $74 billion, of which a little over $2 billion is for information technology (IT) spending.

The Office of the Chief Information Officer (OCIO) is responsible for establishing, implementing, and overseeing a departmentwide information security program, while the component agencies are responsible for the day-to-day management of information security for their mission-support systems. OCIO provides policy guidance, leadership, and coordination for the department's information management, technology investment, and cyber security activities in support of delivering USDA's program. OCIO also operates the National Information Technology Center (NITC), which is a centralized computing facility providing applications and technical support to USDA agencies, and the Telecommunications Services and Operations (TSO) organization, which is responsible for developing USDA telecommunications policy and guidance and leading the design of and migration to the department's future corporate telecommunications network. TSO also manages the current network and provides local telecommunications and computer support services throughout Washington D.C. The Office of Cyber Security, within OCIO, works with the CIO to develop and implement cyber security policies and standards. Its functions include analyzing agency risk assessments, monitoring system vulnerabilities, monitoring agency compliance with departmental policies, and establishing and maintaining a cyber security training and awareness program.

IT resources are essential to the success of the department's mission. To efficiently fulfill its agricultural responsibilities, USDA relies extensively on interconnected computer systems to perform various functions, such as issuing billions of dollars in payroll and loan disbursements, supplying market-sensitive data on commodities to the agricultural economy, and managing other critical departmental programs. USDA also houses and processes all types of sensitive data, including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, and mission-critical data. For example:

- Rural Development's financial programs support such essential public facilities and services as water and sewer systems, housing, health clinics, emergency service facilities, and electric and telephone service. It promotes economic development by supporting loans to businesses through banks and community-managed lending pools. In addition, it

offers technical assistance and information to help start agricultural and other cooperatives and improve the effectiveness of their member services, as well as providing technical assistance to help communities undertake community empowerment programs.

- The Farm Service Agency is responsible for the well-being of American agriculture, the environment, and the American public through efficient and equitably administering of farm commodity programs; farm ownership, operating, and emergency loans; conservation and environmental programs; emergency and disaster assistance; and domestic and international food assistance and international export credit programs.

- The Agricultural Marketing Service administers programs that facilitate the efficient, fair marketing of U.S. agricultural products, including food, fiber, and specialty crops. Its programs promote a strategic marketing perspective that adapts product and marketing practices and technologies to current issues.

- The National Agricultural Statistics Service (NASS) conducts hundreds of surveys and prepares reports covering virtually every facet of U.S. agriculture—production and supplies of food and fiber, prices paid and received by farmers, farm labor and wages, and farm aspects of the industry. NASS regularly surveys thousands of operators of farms, ranches, and agribusinesses who provide information on a confidential basis. The statistical data provided by NASS are essential to both the public and private sectors for making effective policy, production, and marketing decisions on a wide range of agricultural commodities. Data for certain commodities are particularly sensitive due to their potential impact on the futures market prices.

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. 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, these changes pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

We have reported information security as a governmentwide high-risk area since February 1997.[1] Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations, including those at USDA, at risk of disruption, fraud, and inappropriate disclosure. In August 2000, we recommended[2] that USDA (1) develop and document a strategy for improving information security; (2) provide sufficient resources and hold the OCIO accountable for implementing the strategy, as well as providing quarterly status reports; and (3) report information security as a material internal control weakness under the Federal Managers' Financial Integrity Act. According to OCIO, USDA has taken actions to address these recommendations.

Congress and the executive branch have taken action to address the risks associated with persistent information security weaknesses. In December 2002, the Federal Information Security Management Act (FISMA), which is intended to strengthen information security, was enacted as Title III of the E-Government Act of 2002.[3] In addition, the administration undertook other important actions to improve information security, such as integrating information security into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to agencies.

Objectives, Scope, and Methodology

The objective of our review was to determine the effectiveness of USDA's information security controls. These controls affect the security and reliability of sensitive data, including personnel, customer accounts, and financial information. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data; (2) previous USDA

[1]See, for example, U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

[2]U.S. General Accounting Office, *Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan*, GAO/AIMD-00-217 (Washington, D.C.: Aug. 10, 2000).

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

Office of Inspector General (OIG) reports; and (3) our May 1998 report on security management best practices[4] at leading organizations, which identifies key elements of an effective information security program.

Specifically, we evaluated information system controls intended to

- protect data and software from unauthorized access;
- prevent the introduction of unauthorized changes to application and system software;
- provide segregation of duties involving application programming, system programming, computer operations, information security, and quality assurance;
- ensure recovery of computer processing operations in case of disaster or other unexpected interruption; and
- ensure an adequate information security management program.

To evaluate these controls, we identified and reviewed pertinent USDA security policies and procedures documentation, conducted vulnerability testing and assessments of systems from both inside the USDA network and from a remote location through the Internet to assess USDA's efforts in minimizing the risk of unauthorized access, and held discussions with staff to determine if information system general controls were in place, adequately designed, and operating effectively. In addition, we coordinated our efforts with the OIG to take advantage of its prior work in this area.

We performed our review at two component agencies, four field offices, and other offices within the OCIO organization. We also performed vulnerability testing and assessments of three additional agencies' servers[5] that were physically located at one of the offices within the OCIO organization. Our review was performed from February 2003 through October 2003 in accordance with U.S. generally accepted government auditing standards.

[4]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1, 1998).

[5]A server is a computer on a network that manages network resources, such as storing files, managing printers, managing network traffic, or processing database queries.

Serious Information Security Weaknesses Exist at USDA

Significant, pervasive information security control weaknesses exist at USDA. Serious access control weaknesses included not adequately protecting network boundaries, sufficiently controlling network access, appropriately limiting mainframe access, or fully implementing a comprehensive program to monitor access activity. In addition to access controls, weaknesses existed in other control areas such as physical security, personnel controls, system software, application change control, and service continuity. As a result, sensitive data—including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, agricultural production and marketing estimates, and other mission critical data—are at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected. A key reason for USDA's weaknesses is that it has not yet fully implemented a comprehensive security management program.

Access to Sensitive Data and Programs Not Adequately Controlled

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modifications, disclosure, or deletion. The network architecture, including network boundary controls,[6] should support a secure operating environment, and network access controls should be established to restrict access to networks and systems to only authorized users. Organizations can protect critical information by granting employees the authority to read or modify only those programs and data that they need to perform their duties and by periodically reviewing access granted to ensure that it is appropriate. Effective access controls also include a program to monitor the access activities of the network and mainframe systems.

USDA's network boundary controls do not provide sufficient protection, and network and mainframe access controls were inadequate. Also, the increased risks created by the access control problems were further heightened because USDA agencies had not yet established a comprehensive program for monitoring user access.

[6]Network boundary protection defines a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology.

Network Boundary Not Secure

Networks are series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on and transmitted along networks, effectively securing networks is essential for protecting computing resources and data from unauthorized access, manipulation, and use. Organizations can secure their networks, in part, by limiting the services that are available on the network and by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests. Network services consist of protocols for transmitting data between computers. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that filter and forward data along the network, (3) switches that filter and forward information among parts of a network, and (4) servers that host applications and data. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as hackers, cyber-terrorist groups and denial-of-service attacks.[7] Since networks provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data and systems.

USDA's network does not provide a secure operating environment. USDA owns and uses a large public Internet address range to support its customers. While USDA established a restrictive policy to protect its agencies' internal networks from the Internet by using firewalls, its current network boundary controls are not configured in accordance with its security policy and do not provide adequate protection. Without a secure network boundary, USDA is at increased risk of system compromise that could include unauthorized access to sensitive data, disruption of service, and denial of service. USDA is in the process of redesigning its network architecture to create a more secure operating environment by strengthening network boundary controls.

Network Access Controls Not Sufficient

Network access controls are key to ensuring that only authorized individuals gain access to sensitive and critical agency data. Effective network access controls, such as passwords, should be established to authenticate authorized users who access the network from local and remote locations. In addition, network controls should provide safeguards

[7]A denial-of-service attack is an attack on a network that sends a flood of useless traffic that prevents legitimate use of the network.

to ensure that system software is adequately configured to prevent users from bypassing network access controls or causing network failures.

USDA did not always securely control network services or configure devices to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks. USDA's OCIO provided agencies with guidance to mitigate potential vulnerabilities on network servers. However, we identified weaknesses in the way USDA agencies managed remote access, configured certain servers, managed passwords, assigned user rights and permissions, and enabled unnecessary network services, as the following examples demonstrate.

- Default vendor accounts and passwords were being used, including for a dial-in modem account at one agency, for a server for router management at another agency, and for a database server at a third agency. Information on default vendor accounts and passwords is documented in vendor-supplied manuals and is widely available on the Internet to anyone, including hackers. With this access, a malicious user could seriously disable or disrupt network operations, or simply use it as a means to attack other internal systems.

- Certain servers were configured to allow unauthorized users to connect to the network without entering a valid user ID and password combination and obtain access to system information describing the network environment, including user IDs and password information.

- Password settings were inadequate. OCIO provided policies and guidance pertaining to password settings; however, USDA agencies did not always comply with USDA policies and guidance. For example, in some cases, password length was set to 0, meaning that a password is not required. Also, some servers did not allow for an adequate account lockout period after unsuccessful logon attempts, and servers were not configured to enforce the use of complex passwords. Further, we identified instances in which passwords were being shared among personnel, which resulted in USDA's losing accountability over individual IDs. Such weaknesses increase the risk that passwords may be compromised and unauthorized access to USDA's networks gained.

- Although USDA guidance suggests that users be assigned to system access groups on the basis of least privilege, or "need to know," users were assigned to groups that allowed more access than needed to perform their job. In some instances, this access violated the principle

of segregation of duties, in which duties are split among two or more individuals or groups to diminish the likelihood that errors and wrongful acts will go undetected.

- Potentially dangerous services, including some allowing users to remotely execute commands, were available on several network systems. Because of the availability of these services, a greater risk exists that an unauthorized user could exploit them to gain high-level access to the system and applications, obtain information about the system, or deny system services.

- Agencies did not always update software to alleviate potential vulnerabilities or detect viruses. Certain servers were vulnerable to known system exploits because patches[8] had not been installed in a timely manner. Some of these exploits had been reported in mid-2002, but at the time of our review, agencies had yet to apply available patches to correct the weaknesses. In our September 2003 testimony,[9] we noted that, according to the CERT® Coordination Center,[10] about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. Further, although USDA guidance recommends the use of antivirus software on servers, certain servers that we reviewed were not running it. By not running antivirus software, the department is at increased risk of having a virus infect its systems and potentially disabling or disrupting hardware and data.

Weak network access controls increase the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

Mainframe Access Not Appropriately Limited

Effective mainframe access controls should be designed to prevent, limit, and detect access to computer programs and data on the mainframe. These

[8]A patch is a piece of software code that is inserted in a program to temporarily correct a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

[9]U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Washington, D.C.: Sept. 10, 2003).

[10]The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie-Mellon University.

controls include assigning users access rights and permissions, appropriately configuring the security software for granting access, and ensuring that access remains appropriate on the basis of job responsibilities.

Although USDA restricted access to certain data and programs on its mainframe, we identified instances in which access to sensitive data and programs had not been sufficiently restricted. For example,

- Access to sensitive data and programs was not adequately controlled. At one agency, 143 user IDs had been granted *read* access to very sensitive data although some of them did not need this access to perform their jobs; 11 of the 143 also had the capability to modify the data. In addition, users such as secretaries and server administrators could modify system and application programs—a level of access that is typically not allowed for their job functions. Moreover, 69 mainframe users had been granted the ability to *read* all data (i.e., data of all organizations that use the mainframe).

- Certain users had unnecessary access to a powerful mainframe privilege. This privilege is intended for routine system management activities, such as backup and disk management. However, USDA had not restricted its use to its intended purpose. Ten users had been granted this privilege, allowing them to read, copy, edit, or delete any data and programs on the mainframe. Further, since its use does not create an audit trail, their activities would not be detected.

- Many users had the capability to read powerful IDs and passwords stored on the mainframe. USDA's mainframe security standards require that logons/passwords not be stored on systems; however, we observed IDs and passwords stored in files we selected. All users (approximately 17,000) on the system could view a very powerful ID and password that is used to support mainframe operations and has full access to all files stored on tape. At least 1,200 user IDs could read Job Control Language files containing network IDs and passwords, and at least 800 user IDs had the capability to read files containing database IDs and passwords.

- Password settings and software access rules were not adequate. USDA's mainframe security standards set minimum requirements for passwords. However, the mainframe configuration at the time of our review did not comply with these standards, allowing simple passwords that did not necessarily require periodic change. As a result, passwords

might be easily guessed. Additionally, because of the way that access rules are created in the mainframe security software, individuals may be unintentionally granted access to datasets.

One reason for USDA's mainframe access vulnerabilities was that access granted was not always periodically reviewed to ensure that it remained appropriate. Although USDA policy requires that users' access be annually reviewed to ensure that it remains appropriate, the policy was not always being followed or, in some cases, was not effective. For example, at one agency, there was no procedure in place to review access to ensure that it remained appropriate on the basis of job responsibilities. At another, although a procedure had been implemented to periodically review access granted, it was not working as intended; we identified instances in which access was reviewed, yet individuals had more access than needed to perform their jobs.

Comprehensive Monitoring Not Yet Fully Implemented

The risks created by these access control weaknesses were heightened because USDA had not fully established a comprehensive program to monitor user access. A successfully implemented and properly functioning monitoring program is essential to ensure that unauthorized attempts to access critical program and data are detected and investigated. Such a program would include routinely reviewing user access activity and investigating failed attempts to access sensitive data and resources, as well as unusual and suspicious patterns of successful access to sensitive data and resources. These actions are critical for ensuring that improper access to sensitive information is detected.

To effectively monitor user access, it is critical that logs of user activity be maintained for all critical system processing activities. This includes collecting and monitoring access activities on all critical systems, including mainframes, network servers, and routers. Because the security information collected is likely to be voluminous, the most effective monitoring techniques selectively target specific actions. These efforts should include provisions to identify unusual activities, such as changes to sensitive system files, updates to security files, or access to data not required to perform a user's job function. Further, a comprehensive monitoring program should include an intrusion-detection system (IDS) to automatically log unusual activity and provide timely alerts and effective responses.

While USDA had some monitoring efforts in place, it did not consistently audit or monitor computer system activity, as illustrated by the following:

- Logging features were not enabled for certain sensitive mainframe data files, as well as for numerous servers. As a consequence, adverse access events that could result in disclosure or modification of data may not be recorded or detected.

- Inappropriate mainframe configuration settings allowed audit logs to be modified, potentially without detection.

- In some cases, USDA agencies did not adequately review audit information or monitor system activity. Where audit logs existed, they were not always reviewed for certain servers to determine if violations had occurred. For example, according to OIG, one organization did not have procedures in place outlining which logs or reports to review.

- USDA had implemented IDSs on its wide area network, and some agencies implemented their own IDSs for their internal networks and servers. However, at the time of our review, one of the agencies had not yet implemented IDSs. Without full implementation of such systems, USDA reduces its ability to identify and investigate unusual or suspicious access to sensitive information in a timely manner.

As a result, increased risk exists that USDA may not detect unauthorized system activity or determine which users are responsible.

Other Information System Controls Were Ineffective

In addition to information system access controls, other important controls should be in place to ensure the integrity and reliability of an organization's data. These controls include policies, procedures, and control techniques to physically protect computer resources, restrict access to sensitive information, maintain system software integrity, prevent unauthorized changes to application programs, and ensure that computer processing operations continue in case of disaster. However, the department (1) had insufficient physical security controls, (2) had not performed appropriate background investigations, (3) had inadequate system software controls, (4) did not always have application change controls in place, and (5) had incomplete service continuity planning.

Insufficient Physical Security Controls

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls

involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which they are housed and periodically reviewing access granted to ensure that it continues to be appropriate based on criteria established for granting such access. At USDA, physical access control measures (such as guards, badges, and locks, used alone or in combination) are vital to protecting its computing resources and the sensitive data they process from external and internal threats.

USDA established a departmentwide policy for physically protecting its computing resources. The policy includes provisions for authorizing access on the basis of business need, periodically reviewing access, and securing space for computing resources by means of locks or electronic access systems. One organization used biometric systems to control access to sensitive areas. Another agency established procedures for "locking down" certain sections of its facility during sensitive deliberations.

Although USDA agencies took actions to comply with USDA's physical security requirements, certain weaknesses reduced their effectiveness in protecting and controlling physical access to sensitive work areas, as illustrated by the following examples:

- Agencies did not always ensure that access to sensitive computing resources had been granted to only those who needed it to perform their jobs. One agency had not developed a policy that included criteria for granting access to sensitive areas such as server rooms, or for periodically reviewing individual access to ensure whether it remained appropriate. We identified instances in which access cards remained active for contractors who no longer needed access to sensitive areas, and two lost cards had not been removed from the access system.

- Sensitive computing resources were not always secured. At one agency, we observed server rooms that were unlocked, including one that had a door without a lock. At another agency, server rooms in two of the four field offices that we visited were unlocked.

As a result, increased risk exists that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

Background Investigations Not Performed

According to OMB A-130,[11] it has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. Personnel controls (such as screening individuals in positions of trust) supplement other technical, operational, and management controls, particularly where the risk and magnitude of harm is high. NIST suggests first determining the sensitivity of particular positions based on such factors as the type and degree of harm that the individual can cause through misuse of the computer system, (e.g., disclosure of private information, interruption of critical processing, computer fraud), as well as more traditional factors such as access to classified information and fiduciary responsibilities. Background screenings (i.e., investigations) help 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 of screening that takes place depends upon the sensitivity of the position and applicable agency implementing regulations.

Adequate personnel controls were not always in place at USDA. USDA policy requires that agencies be responsible for determining the sensitivity of their positions and for ensuring that employees have the appropriate background investigation commensurate with the position. Nevertheless, one agency had not determined the sensitivity of positions and had conducted only a minimal agency check for each employee. Due to the sensitive information maintained by this agency and the level of system access granted to certain employees, there were instances in which individuals should have a higher-level background investigation. By granting individuals access to sensitive information or critical systems without background investigations, agencies may be at increased risk of having individuals who could cause damage or realize personal gain.

System Software Controls Not Adequate

System software controls, which limit and monitor access to the powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. To protect system software, a standard computer control practice includes (1) configuring system software to protect against security vulnerabilities, (2) periodically reviewing programs in sensitive software libraries to identify potential security weaknesses, and (3) establishing a system change management

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

process that ensures that only authorized and fully tested system software is placed in operation. We and the OIG identified instances in which current system software controls were not always adequate. For example:

- A sensitive program was configured in a way that potentially affects system integrity. As a result, an unauthorized user could introduce incorrect or malicious code. This configuration could also affect the stability and reliability of the operating system.

- Sensitive software libraries, which have the authority to perform sensitive functions that can circumvent security controls, contained duplicate names. Allowing more than one program in these libraries to have the same name could lead to inadvertent or deliberate execution of an unauthorized program that could compromise security controls. Also, USDA had not established a process to periodically review programs in sensitive libraries for security weaknesses, such as programs with duplicate names. Until it establishes such a program, USDA will not have adequate assurance that other security controls cannot be bypassed.

- According to OIG, the system software change management process had been strengthened as of October 2003 and continues to improve. However, OIG noted that approval, testing, and implementation documentation was not always maintained. Consequently, USDA faces increased risks of unintended operational problems caused by programming errors or the deliberate execution of unauthorized programs that could compromise security controls.

Application Change Controls Not Always in Place

Also important for an organization's information security is ensuring that only authorized and fully tested software is placed in operation. To ensure that software changes are needed, work as intended, and do not result in the loss of data and program integrity, such changes should be documented, authorized, tested, and independently reviewed. Before software is moved into the production environment, actual software changes should be compared to the approved request to ensure that only approved changes have been made. Further, access to software libraries should be protected, and movement among libraries (i.e., from a development environment to a production environment) should be controlled by an organization independent of both the user and programming staff. Without proper controls, there is a risk that software could be inadvertently or deliberately modified without authorization, or

that other processing irregularities or malicious code could be introduced into the production environment.

Although USDA policy requires that agencies develop plans and procedures to ensure that any changes made to systems are reviewed and approved by management, one agency lacked documented policies and procedures to ensure that application software modifications were properly authorized, tested, and approved. Although it had an ad hoc process in place for testing the functionality of application changes before putting them into the production environment, there was no process for authorizing changes, no procedures for documenting tests performed, and no review to ensure that only authorized changes were made to the application software.

Further, several USDA agencies had not adequately protected their software libraries. Although each agency had designated an independent group to control movement between the development and production environments, security software controlling access had been configured to grant similar privileges to individuals who did not need it to perform their jobs.

Service Continuity Planning Incomplete

An organization must take steps to ensure that it is adequately prepared to cope with the loss of operational capability due to earthquake, fire, accident, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested service continuity plan covering all key computer operations and including plans for business continuity. Such a plan is critical for helping to ensure that information system operations and data, such as financial processing and related records, can be promptly restored if a disaster occurs. To ensure that it is complete and fully understood by all key staff, the service continuity plan should be tested, including surprise tests, and the test plans and results documented to provide a basis for improvement. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.

Weaknesses in USDA's service continuity controls limit its ability to restore or continue data processing service after a service disruption or an emergency occurs. For example:

- Although departmentwide guidance stresses that contingency planning is an integral part of the USDA information security program, agencies

had not developed contingency plans for all operations. One agency had not developed service continuity plans; another agency's plan was outdated; and a third agency had not developed a service continuity plan for its network environment.

- Although a service continuity plan existed and had been periodically tested for the mainframe environment, there had been no unannounced tests. All previous tests had been planned, with participants fully aware of the disaster recovery scenario. In an actual disaster, of course, there is usually little or no warning.

- Contingency planning is a departmentwide weakness. In September 2003, the USDA OIG reported that eight of ten agencies that it reviewed had not prepared complete, executable disaster recovery plans.[12] Further, in the department's October 2003 FISMA report, USDA stated that only about 60 percent of its systems had a contingency plan, and about 30 percent had tested contingency plans.[13]

As a result, USDA has diminished assurance that in case of an unexpected interruption, it will be able to protect or recover essential information and critical business processes.

Initiatives Are Under Way, but a Comprehensive Security Management Program Is Not Yet Fully Implemented

USDA has recognized the need to improve information security throughout the department, including the components that we reviewed, and has initiatives under way. It identified information security as a material weakness in its fiscal year 2002 Federal Managers' Financial Integrity Act report and noted corrective actions needed to address such issues as physical and logical access, as well as service continuity. USDA also acknowledged the weaknesses that we found, developed action plans to correct them, and, in some cases, took immediate action. OIG, in its fiscal year 2002 consolidated financial statement audit, also reported information security as a material weakness. In its report, OIG stated that although most USDA agencies have taken steps to improve their security programs,

[12]U.S. Department of Agriculture, Office of Inspector General, *Audit Report: Fiscal Year 2003 Federal Information Security Management Act Report*, Report No. 50099-52-FM (Washington, D.C.: Sept. 24, 2003).

[13]U.S. Department of Agriculture, Office of the Chief Information Officer, *Federal Information Security Management Act—FY2003 Information Systems Security Program Review* (Washington, D.C.: October 2003).

it identified widespread serious weaknesses. Its audits continue to disclose that most agencies did not have adequate physical and logical access controls in place over their IT resources.

A key reason for USDA's weaknesses in information system controls is that it has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Our May 1998 study of security management best practices[14] determined that a comprehensive information security management program is essential to ensuring that information system controls work effectively on a continuing basis. The recently enacted FISMA,[15] consistent with our study, describes certain key elements of a comprehensive information security management program. These elements include

- a senior agency information security officer with the mission and resources to ensure compliance;
- periodic assessments of the risk and magnitude of the 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;
- security awareness training to inform personnel, including contractors and other users of information systems, of information security risks and their responsibilities in complying with agency policies and procedures; and
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management,

[14]GAO/AIMD-98-68.

[15]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.

operational, and technical controls of every major information system identified in agencies' inventories.

Although USDA has various initiatives under way, key elements of a comprehensive security management program are not yet fully implemented to the extent that they are effective. In recent reports, both OCIO and OIG have identified deficiencies in USDA's information security management program.

Designating an Information Security Officer

One key element of effective information security management is designating an information security officer as part of establishing a central security group with clearly defined roles and responsibilities. This group provides overall security policy and guidance, along with oversight to ensure compliance with established policies and procedures; further, it reviews the effectiveness of the security environment. The central security group often is supplemented by individual security staff designated to assist in implementing and managing the organization's security program. To ensure the effectiveness of the security program, an organization should establish clearly defined roles and responsibilities for all security staff and develop coordination responsibilities between individual security staff and central security.

USDA established a centralized security management structure, including a senior information security officer. In February 2000, USDA appointed an Associate CIO for Cyber Security to provide security expertise and oversight in establishing a new comprehensive information security program at the department. Also, USDA departmental regulations require that each agency assign an Information System Security Program Manager (ISSPM) to implement policies related to information security. The components we reviewed had established these positions and defined their roles and responsibilities.

Although USDA had this structure in place, in some cases it was not fully effective. In its September 2003 FISMA report, OIG stated that agency security personnel have not commonly been given the authority needed to effectively implement and manage their agency's security programs. Further, it reported a lack of agency management involvement and commitment in complying with federal information security guidelines. In its most recent FISMA report, OCIO agreed with the OIG's conclusion that lack of management involvement has been a key factor in agencies' poor security performance. This was also the case at one of the components that we reviewed; ISSPMs questioned whether they had the authority and

management support to enforce compliance with security policies and procedures.

Assessing Risks

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure that the policies and controls operate as intended.

USDA Cyber Security established policy that requires agencies to use a structured approach to assessing risks. This policy requires that a risk assessment of an agency's security program be conducted annually, and that a vulnerability assessment be completed for information systems whenever a major change is made to the system, or at least once every 3 years. To assist in accomplishing these assessments, Cyber Security also developed detailed checklists for various computing platforms (e.g., mainframe, Unix, Windows, etc.) that prescribe recommended secure system settings.

However, agency risk assessments had not been completed. OCIO reported that about 78 percent of its systems departmentwide had completed risk assessments. However, three agencies, including one that we reviewed, had not completed any of their risk assessments for 46 systems. The lack of risk assessments indicates that USDA had not done all that it was required to do to understand and manage risks to its systems. Inadequately assessing risk can lead to implementing inadequate or inappropriate security controls that might not address the system's true risks and to costly efforts to subsequently implement effective controls.

Establishing and Implementing Policies

Another key element of an effective information security program, as identified during our study of information security management practices at leading organizations, is establishing and implementing appropriate policies and related controls. Establishing or documenting security policies is important because they are the primary mechanism by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection provided by the security policies and controls.

The department has made some progress in developing information security policies and procedures. During fiscal year 2003, Cyber Security issued 16 additional information security guidance and policy statements. These statements provide USDA agencies with guidance on topics such as risk assessment methodology, encryption, remote access, and disaster recovery. However, many of these statements remain in draft, or interim guidance, because the department has not yet approved them.

OMB A-130 and department policy require USDA agencies to develop and implement information security plans for major applications and general support systems. These plans should address policies and procedures for achieving management, operational, and technical controls. According to OCIO, up-to-date security plans were in place for three-fourths of the department's systems. However, OIG reported that none of the agencies that it reviewed in fiscal year 2003 had prepared all required security plans or ensured that existing plans adequately addressed OMB A-130 requirements. While some plans had been developed at the agencies we reviewed, not all were complete. One agency had an overall plan, but had not completed plans for its general support systems or major applications. At the time of our review, the other agencies were in the process of completing their plans.

As noted throughout this report, some agencies lacked other policies and procedures, such as for periodically reviewing system access, granting physical access, and performing application change control.

Promoting Security Awareness

Another important element of an information security program involves promoting awareness and providing required training so that users understand the 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 who use computer systems in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. Federal information security laws mandate that all federal employees and contractors involved with the management, use, or operation of federal computer systems be provided periodic training in information security awareness and accepted information security practice.

The USDA components that we reviewed had generally established information security awareness programs for their employees and contractors. These programs included distributing security awareness bulletins and brochures; creating information security Web pages; and, at one agency, having employees sign a confidentiality statement that included acknowledgement of reading and understanding information security expectations. Agencies were also in the process of obtaining access to a Web-based security awareness training package that would also track employee participation.

Nevertheless, the OIG reported that agencies still lack the controls to ensure that all their employees receive security awareness training. In October 2003, USDA reported that only 59 percent of its employees had received security training in fiscal year 2003.

Testing and Evaluating the Effectiveness of Controls

The final key element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies, and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it 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 and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. Analyzing the results of monitoring efforts, as well as security reviews performed by external audit organizations, provides security specialists and business managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls.

USDA had some efforts under way to test and evaluate controls. During fiscal year 2003, Cyber Security reviewed compliance at five sites. It also contracted for testing of USDA's network. Agencies that we reviewed had also undertaken limited ongoing testing, such as periodically scanning their networks and servers. USDA's OCIO also initiated a formal IT certification and accreditation[16] program, including a methodology based on NIST

[16]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. This authorization explicitly accepts the risk remaining after the implementation of an agreed upon set of security controls.

guidance and contracting support for assistance with certifying and accrediting the department's major systems.

However, further efforts are needed to fully implement an ongoing program of tests and evaluations. The department reported that security controls were tested and evaluated for just over one-third of its systems in the past year. In addition, although USDA policy requires that certification and accreditation of systems should occur at least every 3 years or before a significant change in processing, the department reported in October 2003 that only about 16 percent of its systems had been certified and accredited. Further, none of the components that we reviewed had completed certification and accreditation for any of their systems. An effective program of ongoing tests and evaluations can be used to identify and correct information security weaknesses such as those discussed in this report.

Based on the results of tests and evaluations that have been conducted, agencies have developed corrective action plans (i.e., Plans of Actions and Milestones—POA&Ms), as required by FISMA. However, these plans may not be effective. In its latest FISMA report, OIG stated that its review of POA&Ms at the agency level disclosed that agencies have not prepared POA&Ms for individual systems, and the information they contain is sometimes vague and unreliable. USDA's OCIO also reported that it is unable to tie specific agency POA&Ms to identified weaknesses. Without adequate corrective action plans, the results of tests and evaluations may not be effectively used to improve the security program and correct identified weaknesses.

Conclusions

Serious information security weaknesses exist at USDA that place sensitive information at risk of disclosure, modification, or loss, and operations at risk of disruption. Specifically, USDA has not sufficiently secured its network, adequately limited mainframe access, or fully implemented a program to monitor access activity. Weaknesses in physical security, personnel controls, system and application software, and service continuity increase the level of risk.

A key reason for USDA's weaknesses in information system controls is that it has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained, and that information security receives adequate attention. Effective implementation of such a program provides for periodically

assessing risks, establishing appropriate policies and procedures, promoting security awareness, and establishing an ongoing program of tests and evaluations of the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose. Although USDA has various initiatives under way to address these areas, further efforts are needed to address its information security weaknesses.

Recommendations for Executive Action

To establish effective information security, we recommend that the Secretary of Agriculture direct the CIO to address the following action:

- Fully implement a comprehensive security management program. Specifically, this would include (1) ensuring that security management positions have the authority and cooperation of agency management to effectively implement and manage security programs, (2) completing periodic risk assessments for systems, (3) completing information security plans and establishing policies and procedures on the basis of identified risks, (4) ensuring that employees complete security awareness training, (5) implementing ongoing tests and evaluations of controls, (6) completing system certifications and accreditations, and (7) developing corrective action plans that clearly tie to identified weaknesses.

We are also making recommendations in a separate report designated for "Limited Official Use Only." These recommendations address actions needed to correct the specific information security weaknesses related to the network boundary, network access, mainframe access, physical security, background investigations, system software, application change controls, and service continuity.

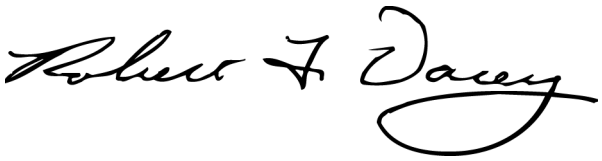
Agency Comments

In providing written comments on a draft of this report, USDA's CIO concurred with our recommendations and stated that the department remains committed to improving information security. He further stated that USDA plans to fully implement a comprehensive security management program as well as correct the specific information security weaknesses identified. USDA's comments are reprinted in full in appendix I.

As agreed with your offices, 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 agriculture and information security programs, the Secretary of Agriculture, the USDA CIO, the USDA Inspector General, and other interested parties. We also will make copies available to others upon request.

In addition, the report will be available at no charge on the GAO Web site at www.gao.gov. If you have any questions, please contact me at (202) 512-3317 or Carol Langelier, Assistant Director, at (202) 512-5079. We can also be reached at daceyr@gao.gov and langelierc@gao.gov, respectively. Key contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Information Security Issues

Comments from the Department of Agriculture

United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue S.W.

Washington, DC
20250

December 3, 2003

Robert F. Dacey, Director
Information Security Issues
U.S. General Accounting Office
441 G. Street, N.W.
Washington, D.C. 20548

Dear Mr. Dacey:

The Office of the Chief Information Officer (OCIO) has reviewed draft report number GAO-04-154 entitled "Information Security - Further Efforts Needed to Address Serious Weaknesses at USDA."

OCIO has appreciated the opportunity to work with the General Accounting Office (GAO) as we have gone through a series of reviews of the information, which has produced this draft report. We believe that the final draft accurately reflects issues and concerns identified by the GAO and offer no changes or comments.

The USDA remains committed to improving information security department-wide. As such, we concur with your recommendation to establish an effective information security control environment including correcting the specific information security weaknesses identified and fully implementing a comprehensive security management program.

If additional information is needed, please have a member of your staff contact Sherry Linkins, OCIO audit liaison, on (202) 720-9293.

Sincerely,

/s/ Ira L. Hobbs

for
Scott Charbo
Chief Information Officer

AN EQUAL OPPORTUNITY EMPLOYER

GAO Contact and Staff Acknowledgments

GAO Contact

Carol Langelier (202) 512-5079

Staff Acknowledgments

In addition to the individual named above, Edward Alexander, Gerald Barnes, Nicole Carpenter, Lon Chin, West Coile, Debra Conner, Denise Fitzpatrick, Edward Glagola, David Hayes, Jeffrey Knott, Harold Lewis, Suzanne Lightman, Leena Mathew, Duc Ngo, Kevin Secrest, Eugene Stevens, Rosanna Villa, Charles Vrabel, and Chris Warweg made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00