

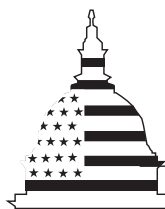
GAO

Report to the Chairman, Subcommittee
on Department Operations, Oversight,
Nutrition, and Forestry, Committee on
Agriculture, House of Representatives

August 2000

INFORMATION SECURITY

USDA Needs to Implement Its Departmentwide Information Security Plan



G A O

Accountability * Integrity * Reliability



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

Accounting and Information
Management Division

B-285277

August 10, 2000

The Honorable Robert Goodlatte
Chairman
Subcommittee on Department Operations,
Oversight, Nutrition, and Forestry
Committee on Agriculture
House of Representatives

Dear Mr. Chairman:

As you know, the Department of Agriculture (USDA) relies 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. To safeguard these systems and ensure the protection and privacy of information they contain, USDA needs to have a departmentwide information security program. At your request, we identified steps USDA is taking to help ensure departmentwide information systems security and briefed your office on the results of our work on May 17, 2000. The briefing slides are included in appendix I.

This report provides a high-level summary of information presented at that briefing and presents recommendations we are making to USDA for strengthening information security throughout the department.

Results In Brief

USDA has taken positive steps to begin improving its information security by developing its August 1999 Action Plan with recommendations to strengthen departmentwide information security and hiring a new Associate Chief Information Officer (CIO) for Cyber-Security who is working to address specific vulnerabilities and other potential threats. However, since the plan was issued in August 1999, little progress has been made to implement other recommendations in the plan for strengthening the department's information security. Moreover, USDA has not developed and documented a strategy for implementing the action plan recommendations with established priorities and the detailed steps, time frames, milestones, and total resources needed to fully carry them out.

Until and unless the department fully implements these important information security improvements, its critical assets will remain at risk to cyber attacks and other threats. Therefore, we are recommending that USDA develop a detailed strategy for implementing the action plan and demonstrate that information security at USDA is a departmental priority by (1) directing that sufficient resources be available to fund the department's information security improvement strategy and implementing plan, (2) holding the CIO and Associate CIO for Cyber-Security accountable for carrying out the strategy and plan, and (3) requiring quarterly reports describing the results of these efforts. We are also recommending that USDA report its information security weaknesses and lack of departmentwide information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act.

In its comments, USDA agreed with our recommendations for ensuring that information security is strengthened at the department and offered some clarifications, which we incorporated as appropriate.

Background

Automated systems are essential to USDA's operations and the delivery of its mission-critical programs, especially as it moves towards electronic government (e-government). USDA has many critical assets, including

- billions of dollars in federal payroll, thrift savings, program, and other accounts at the National Finance Center (NFC) and other agencies;
- sign-up and participant information and other information critical to the delivery of billions of dollars in USDA programs;
- market-sensitive data on commodities/agricultural economy; and
- personal information on employees and customers, including social security numbers and health, business, and financial data.

Under federal law and guidance, agencies are required to take necessary steps to ensure the protection of mission-critical systems and data. The Computer Security Act of 1987 requires the establishment of a security plan for systems containing sensitive information commensurate with the risk and magnitude of potential harm. Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires federal agencies to establish information security programs, including completing risk assessments to identify threats and vulnerabilities and steps to mitigate them.

Under the Federal Managers' Financial Integrity Act (31 U.S.C. 3512 (1982)), federal department and agency managers are required to evaluate whether internal control systems have weaknesses that can lead to fraud, waste, and abuse in government operations. The act is a key mechanism that the Congress has put into place to ensure that management controls, including those over automation efforts, are effective, and to hold managers accountable for correcting identified deficiencies. Federal managers are required to annually review their internal controls and report to the President and the Congress any material weaknesses identified in these controls, along with the status of corrective actions.

As technology has enhanced the ability to share information instantaneously among computers and networks, federal agencies, including USDA, have become more vulnerable to unlawful and destructive penetration and disruptions. These kinds of cyber threats prompted the May 1998 issuance of Presidential Decision Directive 63, requiring, among other things, that agencies develop plans to protect their information systems and cyber infrastructure.

Additionally, plans for expanding USDA's use of the Internet as well as allowing the public more access to services through electronic on-line transactions pose even greater security and privacy concerns for USDA's many information systems and networks. Specifically, the Freedom to E-File Act (P.L. 106-222) was enacted on June 21, 2000; it requires USDA to expand its use of electronic filing across a range of services and have on-line systems in place within 2 years.

In 1998, we issued an executive guide¹ on information security management for helping federal agencies better manage their information security resources. The guide, which describes five key principles and corresponding best practices, presents a management framework that agencies can use to establish more effective information security programs.

USDA and its 29 component agencies' fiscal year 2000 program budget is \$105.4 billion, including \$1.2 billion for information technology. The Office of the Chief Information Officer (OCIO) is responsible for establishing, implementing, and overseeing a departmentwide information security

¹*Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

program, while the component agencies are responsible for the day-to-day management of information security for their mission- support systems.

During 1999, USDA's Office of Inspector General (OIG) and we found significant information security weaknesses at the department's two major data centers, which placed critical assets at significant risk. For example, the OIG's general controls review at USDA's National Information Technology Center reported network security vulnerabilities and weaknesses, such as poor network monitoring and intrusion detection and inappropriately controlled access authority.² In July 1999, we reported on further security weaknesses at USDA's NFC that included inadequate computer security planning and systems information that was vulnerable to unauthorized access.³

USDA Has Developed a Plan to Strengthen Departmentwide Information Security

As a result of the OIG's and our reports on information security problems at USDA, in July 1999 the Secretary of Agriculture asked for a plan within 30 days that described fundamental ways to improve information security and provided recommendations for addressing security problems in a comprehensive fashion across the department. In its comments on a draft of this report, USDA stated that another reason the Secretary asked for a plan was his long-standing and keen interest in federal information security. For example, USDA stated that the Secretary co-authored the Computer Security Act of 1987.

In developing its plan, USDA's OCIO assessed departmentwide information security by (1) conducting a workshop with security experts from key USDA agencies and a USDA contractor, (2) visiting other federal agencies, including the Internal Revenue Service, the Department of Commerce, and the Department of Energy, to examine actions they were taking to improve information security, and (3) comparing USDA's current security practices with the "best practices" identified in our May 1998 executive guide as well as with practices followed by other federal departments.

²*U.S. Department of Agriculture Office of Inspector General Audit Report/Fiscal Year 1998 National Information Technology Center General Controls Review* (#88099-1, Dec. 1999).

³*Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-99-227, July 1999).

In August 1999, USDA's OCIO issued *An Action Plan to Strengthen USDA Information Security*, which emphasized protecting USDA's critical assets as a top priority for the department. The plan identified weaknesses at USDA that included the lack of

- OCIO resources necessary to provide technical assistance, enforce and monitor policy implementation, and ensure accountability;
- a comprehensive USDA risk assessment that assigns value to the department's assets and prioritizes vulnerabilities; and
- a departmentwide information security architecture.

USDA's plan also reported that the department devotes significantly fewer resources to information security than might be expected for an organization with the criticality of assets that USDA must protect. According to the plan, for example, USDA projected that it would devote about 1 percent (\$12.5 million) of its total information technology budget (\$1.2 billion) to information security in fiscal year 2000, and projected its information security budget would increase to only slightly more than 1 percent of the department's total information technology budget in fiscal year 2001.

On August 13, 1999, USDA's OCIO briefed the Secretary on the plan for improving information security. The plan's recommendations, which were based on the five key information security principles and practices in our 1998 executive guide, were to

- designate an Associate CIO for Cyber-Security and establish security program management;
- develop practical risk assessment procedures to manage risks;
- establish appropriate policies and controls linked to business risks and develop and implement an information security architecture;
- promote security awareness through systematic training; and
- establish procedures to monitor and evaluate policy and controls.

During the briefing, the CIO also discussed general steps to jump-start work on these recommendations and requested an additional \$8 million to implement most of them by March 2000. However, a strategy was not provided for implementing the plan's recommendations that had established priorities with detailed steps, time frames, milestones, and total resources needed to fully carry out the plan across the department and correct all security weaknesses. For example, while the CIO listed several action items, such as initiating a security compliance management

program, developing departmentwide security awareness training, and designing and implementing a cyber-security architecture, the CIO did not identify priorities and detailed steps, milestones, and resources needed to carry out these activities. USDA noted in its comments on a draft of this report that by the time the OCIO security plan was issued in August 1999, USDA's budget request for fiscal year 2000 had already been formulated and did not include a request for the plan's implementation.

Little Progress Made Implementing Recommended Information Security Improvements

From August 1999 through April 2000, USDA began taking action on the first key recommendation from the action plan for improving information security by hiring a senior manager for cybersecurity in February 2000. In addition, the OCIO assigned four staff members to work on the cyber-security team and has advertised three additional positions.

Beyond this, however, little else has been done to implement the other recommendations in the plan. For example, at the time of our review, OCIO had not yet obtained all of the basic information necessary to begin to determine its business risks, such as establishing a comprehensive list of sensitive systems, as required by the Computer Security Act of 1987. This is a fundamental step for establishing an information security program to protect critical business assets and mitigate risks. Until this fundamental step is complete and all business risks are adequately assessed, USDA cannot effectively implement other recommendations for improvement, such as establishing appropriate policies and controls linked to business risks, developing an information security architecture, and setting forth procedures for monitoring and evaluating policy and control effectiveness.

According to USDA's Deputy CIO, more progress implementing the recommended improvements has not been made because of delays in hiring the senior executive to fill the department's new cyber-security position. The new Associate CIO for Cyber-Security did not start work until February 17, 2000. In addition, the Deputy CIO told us that the Secretary's office did not approve the action plan or the CIO's request to seek additional appropriations in fiscal year 2000 beyond the \$500,000 already appropriated for information security during that fiscal year. We were told that USDA decided that seeking additional funds from the Congress in fiscal year 2000 was not possible at the time due to other existing priorities, such as the Year 2000 issue and the farm crisis.

The Deputy CIO told us that the OCIO did not attempt to fund needed security improvements in fiscal year 2000 to jump-start the

departmentwide information security program by reassessing the department's other information technology priorities and resources and seeking approval to use a portion of the other available fiscal year 2000 information technology resources for this purpose. These other funds included (1) the component agencies' fiscal year 2000 information technology budgets, which amounted to about \$1.2 billion, (2) the OCIO's own \$6 million budget in fiscal year 2000 appropriations, or (3) the \$61 million in information technology working capital funds allocated to the OCIO. Instead, OCIO requested an additional \$6.6 million to fund additional work on the plan in its congressional fiscal year 2001 budget request and pointed out that the component agencies would be funding their security risk assessments. OCIO has not yet taken steps to ensure that the component agencies set aside sufficient funds in their fiscal year 2001 budgets for this purpose.

Since February 2000, USDA's new Associate CIO for Cyber-Security has been working with the \$500,000 budget appropriated for information security in fiscal year 2000 and four assigned staff, primarily concentrating on

- setting up a structure for the new cybersecurity office in OCIO;
- briefing agency CIOs and security officers across the department to obtain support for needed security improvements; and
- addressing specific vulnerabilities identified in USDA OIG's and our reports.

The Associate CIO for Cyber-Security has also been responding to identified cyber intrusions, which have continued to occur at the department. According to USDA's fiscal year 2000 budget request, the department recorded 27 security incidents of intrusions during 1999. According to the Associate CIO, USDA has continued to experience a significant number of intrusions in fiscal year 2000.

As previously discussed, key information security requirements and guidelines require federal agencies to establish effective information security management programs. Failure to do so may threaten an agency's ability to carry out its missions and properly safeguard its critical assets and can constitute a material internal control weakness under the Federal Managers' Financial Integrity Act.

Conclusions

USDA has taken positive steps to begin improving its information security by developing its August 1999 action plan with recommendations for strengthening information security and hiring a new Associate CIO for Cyber-Security who is working to address specific vulnerabilities identified in our and USDA OIG's reports and other potential threats. Beyond this, however, little progress has been made for implementing other recommendations in the plan designed to strengthen departmentwide information security because USDA lacks a strategy for doing so and because sufficient resources have not been made available. Until and unless USDA fully implements these important information security improvement efforts, the department's critical assets will remain at risk for cyber attacks and other threats, and USDA will not be in a position to provide a secure environment for expanding e-government.

Recommendations

In order to ensure that information security is strengthened at the department, we recommend that the Secretary of Agriculture do the following:

- The Secretary should direct that the CIO and Associate CIO for Cyber-Security develop and document a strategy for implementing the action plan for improving USDA information security. At a minimum, the implementing strategy should establish and set forth priorities for implementing the plan and for addressing the highest risks and threats to the department's assets; time frames and milestones for completing all necessary actions; and staff and funding resources required for fiscal years 2001, 2002, and beyond.
- The Secretary should demonstrate that information security at USDA is a departmental priority by (1) directing that sufficient resources be available to fund the department's information security improvement strategy and implementing plan; (2) holding the CIO and Associate CIO accountable for carrying out the strategy and plan; and (3) requiring OCIO to provide the Secretary of Agriculture with quarterly reports describing the results of USDA's efforts to establish and implement an effective departmentwide information security program.

We also recommend that the Secretary of Agriculture report the department's information security weaknesses and lack of a departmentwide information security management program as a material internal control weakness under the Federal Managers' Financial Integrity

Act. This internal control weakness should remain outstanding until USDA fully meets the federal regulations for information security.

Agency Comments and Our Evaluation

USDA's CIO provided written comments on July 14, 2000, on a draft of this report. USDA's comments are summarized below and reproduced in appendix II.

USDA agreed with our recommendations for ensuring that information security is strengthened at the department. Specifically, USDA agreed that information systems that support its mission objectives are at risk and that dramatic changes are needed to improve cybersecurity. USDA also stated that its OCIO is committed to improving security for the department's valuable information assets and that the department intends on carrying out its security action plan. USDA stated that the President's fiscal year 2001 budget requested a \$6.6 million increase in funding for cybersecurity, and the department intends to request another substantial increase for cybersecurity in its fiscal year 2002 budget submission. According to its comments, these increases will be used to complete the development of a USDA risk management program, expand the cyber-security office, revise security policy, conduct on-site security reviews, define a security architecture, and perform other security-related activities.

USDA also raised several additional matters, none of which affect our conclusions and recommendations. These matters and our responses are discussed in appendix II.

Objective, Scope, and Methodology

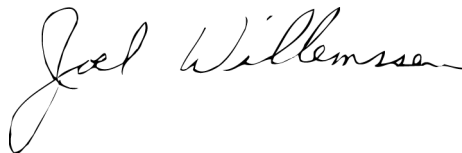
As requested, our objective was to provide information on steps being taken by USDA to help ensure departmentwide information system security. To identify these steps, we obtained and reviewed USDA internal documents including the department's budget submissions, security improvement plans, and contractor studies. Using our and other guidance as evaluation criteria, we identified and assessed plans and steps being taken by the department to improve and strengthen security. We also discussed USDA's information security weaknesses and steps completed and underway to address these weaknesses with numerous USDA officials, including the CIO, Deputy CIO, and Associate CIO for Cyber-Security and we obtained written comments on a draft of this report from USDA's CIO.

We performed our work from February 2000 through April 2000 at USDA headquarters in Washington, D.C., in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from its date. At that time, we will send copies of this report to Representative Eva Clayton, Ranking Minority Member, Subcommittee on Department Operations, Oversight, Nutrition, and Forestry, House Committee on Agriculture; Senator Richard Lugar, Chairman, and Senator Tom Harkin, Ranking Minority Member, Senate Committee on Agriculture, Nutrition, and Forestry; Representative Larry Combest, Chairman, and Representative Charles Stenholm, Ranking Minority Member, House Committee on Agriculture; and Representative Steven Horn, Chairman, and Representative Jim Turner, Ranking Minority Member, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform. We will also send copies to the Honorable Daniel R. Glickman, Secretary of Agriculture; the Honorable Jacob J. Lew, Director, Office of Management and Budget; and other interested parties. Copies will be made available to others upon request.

If you have any questions on matters discussed in this report, please call me at (202) 512-6408 or Stephen A. Schwartz, Senior Assistant Director, at (202) 512-6213. We can also be reached by e-mail at willemsenj.aimd@gao.gov and schwartzs.aimd@gao.gov, respectively. Key contributors to this assignment were Christina Bower, Troy Hottovy, Keith Rhodes, and Mark Shaw.

Sincerely yours,



Joel C. Willemsen
Director, Civil Agencies Information Systems

Briefing on USDA Information Security

GAO

Accounting and Information
Management Division



USDA Information Security

Committee on Agriculture
Subcommittee on Department Operations,
Oversight, Nutrition, and Forestry

May 17, 2000



Purpose

- Brief Requester on Information Security at USDA
- Outline of Briefing
 - Background
 - Objective, Scope, and Methodology
 - USDA Develops Plan to Improve Information Security
 - Little Progress Made Implementing Recommended Improvements
 - Summary of Observations
 - Suggested Actions



Background

- Automated systems are essential to USDA's operations and delivery of its mission critical programs, especially as it moves towards electronic government (e-government)
- USDA has many critical assets to protect, including
 - billions of dollars in Federal payroll, thrift savings, program, and other accounts at the National Finance Center for USDA and other agencies,
 - sign up and participation information, and other information critical to the delivery of billions of dollars in USDA programs,
 - market sensitive data on commodities/agricultural economy, and
 - personal information on employees and customers, including social security numbers, and health, business, and financial data.



Background (Cont'd)

- Key information security requirements/guidelines for federal agencies
 - Computer Security Act of 1987 requires the establishment of a security plan for systems containing sensitive information commensurate with the risk and magnitude of potential harm.
 - OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources requires federal agencies to establish information security programs, including completing risk assessments to identify threats and vulnerabilities and steps to mitigate them.



Background (Cont'd)

- Ever-increasing cyber threats across government prompted May 1998 issuance of Presidential Decision Directive (PDD) 63, requiring, among other things, that agencies develop plans to protect information systems and cyber infrastructure.
- Plans for expanding USDA's use of the Internet as well as allowing the public more access to services through electronic online transactions pose even greater security and privacy concerns for USDA's many information systems and networks.
 - "Freedom to E-File Act" sent from the Congress to the President for signature on June 8, 2000 requires USDA to expand its use of electronic filing across a range of services and have online systems in place no later than 2 years.



Background (Cont'd)

- In 1998 GAO issued an executive guide* on information security management that describes five key principles and corresponding best practices to help agencies establish an effective information security management framework

Key Principles

(1) Assess risk and determine needs

(2) Establish central key management focal point

(3) Implement appropriate policies and related controls

(4) Promote awareness

(5) Monitor and evaluate policy and control effectiveness

Practices include

developing risk assessment procedures and managing risk on a continuing basis

designating central group, with access to executives, to carry out key activities

linking policies to business risks and supporting them through central security group

continually educating users/others on risks and related policies

monitoring factors affecting risk and using risk assessment results to direct future efforts

*Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998)

GAO Background (Cont'd)

- USDA's FY 2000 program budget is \$105.4 billion.
- USDA's overall FY2000 Information Technology budget is \$1.2 billion.
- USDA's Office of Chief Information Officer (OCIO) is responsible for establishing, implementing, and overseeing a departmentwide information security program.
- USDA component agencies/offices are responsible for managing information security for their mission support systems on a day-to-day basis.

GAO Background (Cont'd)

- During 1999, USDA's OIG and GAO found significant information security weaknesses at USDA's two major data centers that placed its critical assets at significant risk.
 - USDA's OIG fiscal year 1998 general controls review at USDA's National Information Technology Center (NITC) reported network security vulnerabilities and weaknesses*
 - a lack of network monitoring and intrusion detection program
 - access authority not appropriately limited
 - In July 1999, GAO reported information security weaknesses at USDA's National Finance Center (NFC)**
 - information in NFC systems vulnerable to unauthorized access
 - computer security planning/management program not adequate

*U.S Department of Agriculture Office of Inspector General Audit Report/Fiscal Year 1998 National Information Technology Center General Controls Review (#88099-1, December 1999)

**USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-99-227, July 1999)



Objective, Scope, and Methodology

Objective

- Provide information on steps being taken by USDA to help ensure departmentwide information systems security

Scope and Methodology

- Obtained and reviewed USDA internal documents including the department's budget submissions, security improvement plans, and contractor studies.
- Using GAO and other guidance as evaluation criteria, reviewed USDA's plans to improve security and discussed USDA's information security weaknesses and steps completed and underway to address these weaknesses with numerous USDA officials, including the CIO, Deputy CIO, and Associate CIO for Cyber-security.
- Performed work at USDA headquarters offices in Washington D.C. from February 2000 through April 2000 in accordance with generally accepted government auditing standards.

GAO USDA Develops Plan to Improve Information Security

- In response to the Secretary's July 1999 call for a plan within 30 days to address the department's security weaknesses, OCIO issued "An Action Plan to Strengthen USDA Information Security" in August 1999.
- OCIO's plan emphasized protecting USDA's critical assets as a top priority for the department and identified key weaknesses, such as
 - OCIO lacked resources necessary to provide technical assistance, enforce and monitor policy implementation, and ensure accountability;
[OCIO had a part-time computer security manager and 3 full-time staff devoted to information security.]
 - USDA lacked a comprehensive risk assessment that assigns value to the department's information assets and prioritizes vulnerabilities; and
 - USDA lacked a department-wide information security architecture.

GAO USDA Develops Plan to Improve Information Security (Cont'd)

- OCIO's plan also reported that USDA, as a department, devotes significantly less resources to information security than might be expected for an organization with the criticality of assets it must protect.
 - USDA projected it would devote about 1 percent (\$12.5 million) of its total IT budget (\$1.2 billion) to information security, and projected this would increase to slightly more than 1 percent in FY 2001.

GAO USDA Develops Plan to Improve Information Security (Cont'd)

- On August 13, 1999, OCIO briefed the Secretary on its plan for improving information security
 - made recommendations, which were based on GAO's five key principles and practices, to
 - designate an Associate CIO for Cyber-Security and establish security program management
 - develop practical risk assessment procedures to manage risks
 - establish appropriate policies/controls linked to business risks and develop and implement information security architecture
 - promote security awareness through systematic training
 - establish procedures to monitor and evaluate policy/controls
 - discussed general steps and \$8 million in additional funding needed to jump start work on these recommendations and have most of them implemented by March 2000
- OCIO's briefing did not include a strategy for implementing the plan's recommendations with detailed steps, time frames, milestones, and total resources needed to fully carry out the plan across the department and correct all security weaknesses.

GAO Little Progress Made Implementing Recommended Improvements

- Progress made between August 1999 and April 2000
 - USDA established senior level information security position at department.
 - OCIO hired new Associate CIO for Cyber-Security on February 17, 2000, assigned 4 existing staff to the Cyber-Security team, and advertised positions for 3 additional staff.
- Beyond this, however, little has been done on other recommendations in the plan. Specifically, OCIO has not yet
 - completed obtaining all of the basic information necessary to begin to assess and mitigate its business risks, such as establishing a comprehensive list of “sensitive” systems, as required by the Computer Security Act of 1987;
 - revised and established appropriate policies and controls linked to business risks and developed an information security architecture;
 - established a security awareness training program; and
 - developed procedures for monitoring and evaluating the effectiveness of security policies and controls.

GAO Little Progress Made Implementing Recommended Improvements (Cont'd)

- According to USDA's Deputy CIO, more progress has not been made implementing the plan because
 - delays were encountered hiring a new senior executive to fill the department's new Cyber-Security position, and
 - the Secretary's office did not approve the plan, nor OCIO's request to seek additional appropriations in FY2000 beyond the \$500,000 already appropriated for information security.
 - USDA decided that seeking additional funds from the Congress in FY2000 was not possible at the time due to other existing priorities, such as the Year 2000 issue and the Farm Crisis

GAO Little Progress Made Implementing Recommended Improvements (Cont'd)

- OCIO did not attempt to fund additional activities to implement information security recommendations during FY2000 by reassessing priorities and seeking approval to use a portion of
 - the Department's overall \$1.2 billion IT budget,
 - OCIO's budget of \$6 million in FY2000 appropriations, or
 - the \$61 million in IT working capital funds allocated to OCIO in FY2000.
- Instead, for its FY 2001 budget, USDA's OCIO
 - requested an additional \$6.6 million to fund work on these recommendations during FY2001, and
 - stated that USDA's component agencies would fund security risk assessments.
 - However, OCIO has not taken steps to ensure that USDA component agencies set aside sufficient funds in their FY2001 budget for this purpose.

GAO Little Progress Made Implementing Recommended Improvements (Cont'd)

- Working with \$500,000 for FY2000 (less than 1/20 of 1 percent of USDA's total IT budget) and 4 assigned staff, USDA's Associate CIO for Cyber Security has, since being hired in February 2000, primarily concentrated on
 - setting up a structure for the new Cyber-Security office in OCIO,
 - briefing agency CIOs and security officers across the department to obtain support for needed security improvements,
 - addressing specific vulnerabilities identified in GAO/OIG reports, and
 - responding to cyber-intrusions as they occur
 - USDA reported in its FY 2000 budget that during 1999 it recorded 27 security incidents of intrusions
 - USDA continues to experience a significant number of intrusions

GAO Summary of Observations

- USDA has taken positive steps to begin improving its information security by developing its August 1999 Action Plan with recommendations for strengthening information security.
 - As a first step, OCIO hired a new Associate CIO for Cyber-Security who is working to address specific vulnerabilities identified in GAO/OIG reports and other potential threats.
- Beyond this, however, little progress has been made implementing other recommendations in the plan related to
 - establishing departmentwide security program management,
 - assessing and mitigating USDA's business risks,
 - establishing appropriate policies and controls linked to these risks and developing an information security architecture,
 - building a security awareness training program, and
 - developing procedures for monitoring and evaluating the effectiveness of security policies and controls.

GAO Summary of Observations (Cont'd)

- OCIO has not developed and documented a strategy for implementing its information security improvement plan with established priorities and the detailed steps, time frames, milestones, and total resources needed to fully carry it out
- Until and unless USDA fully implements these important information security improvement efforts,
 - the department's critical assets will remain at risk to cyber attacks and other threats
 - USDA will not be in a position to provide a secure environment for expanding e-government

GAO Suggested Actions

To ensure that information security is strengthened at the department, the Secretary of Agriculture should


- Direct that the CIO and Associate CIO for Cyber-Security develop and document a strategy for implementing the action plan for improving USDA information security. At a minimum, the implementing strategy should establish and set forth
 - priorities for implementing the plan and for addressing the highest risks/threats to the department’s assets,
 - time frames and milestones for completing all necessary actions, and
 - staff and funding resources required for FY2001, FY2002 and beyond.
- Demonstrate that information security at USDA is a departmental priority by directing that sufficient resources are available to fund the department’s information security improvement strategy and implementing plan.

GAO Suggested Actions (Cont'd)

- Hold the CIO and Associate CIO for Cyber-Security accountable for carrying out the plan and require OCIO to provide you quarterly reports describing the results of USDA's efforts to implement departmentwide information security improvements.

Comments From the Department of Agriculture

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



**United States
Department of
Agriculture**

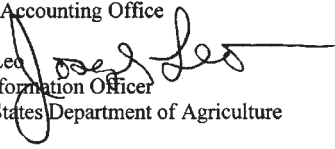
**Office of the Chief
Information Officer**

1400 Independence
Avenue SW

Washington, DC
20250

JUL 14 2000

TO: Jeffrey C. Steinhoff
Assistant Comptroller General
General Accounting Office

From: Joseph Lee 
Chief Information Officer
United States Department of Agriculture

SUBJECT: GAO Audit AIMD-000217

USDA welcomes the opportunity to comment on the subject audit report. We concur with recommendations contained within. Attached are a number of comments that we believe will improve the audit report and more accurately reflect the current status of our effort to improve information technology security within the Department.

We are concerned with the overall tone of the audit report. In particular, we feel the report should better reflect USDA Secretary Glickman's proactive attitude toward cyber security. Secretary Glickman co-authored the Computer Security Act of 1987 and has maintained a keen interest in the security of USDA's information assets throughout his tenure here. The audit report is silent on these facts. We believe an acknowledgement of his concerns and attention to cyber security at USDA would be a more fair portrayal than that which is suggested in the draft report.

If you need additional information regarding this matter, please contact Mr. William D. Hadesty, Associate Chief Information Officer for Cyber Security at 202-720-5865.

CC:
Lynda Couvillion, OBPA
Benjamin Young, OGC

AN EQUAL OPPORTUNITY EMPLOYER

See comment 1.

**Appendix II
Comments From the Department of
Agriculture**

GAO Audit No. AIMD-00-217

USDA Comments:

Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan

SUMMARY OF GAO COMMENTS

GAO notes that USDA relies heavily on automated systems and networks to deliver billions of dollars in programs to its customers and that a departmentwide information security program is necessary to ensure the safety and privacy of these systems. GAO acknowledges that USDA has developed a comprehensive cyber security action plan and has taken positive steps to begin improving its information security, but has made little progress in implementing the plan since it was issued in August, 1999. According to GAO, "Until and unless the department fully implements these important information security improvements, its critical assets will remain at risk to cyber attacks and other threats."

GAO recommends that USDA develop a detailed strategy for implementing its action plan, direct sufficient resources to fund the security improvement strategy, hold the CIO and Associate CIO for Cyber Security accountable for carrying out the strategy, and provide quarterly reports to the Secretary describing the result of these efforts. GAO further recommends that USDA report the department's information security weaknesses as a material internal control weakness under the Federal Managers' Financial Integrity Act.

DEPARTMENTAL RESPONSE

USDA agrees that information systems that support its mission objectives are at risk and that dramatic changes are needed to improve cyber security throughout the department. Both within and outside of the federal government, new information technology advances, combined with changes in the way service is delivered, have combined to introduce new cyber security threats. USDA's Office of the Chief Information Officer (OCIO) is committed to improving security for the department's valuable information assets and has taken positive steps in this regard. However, developing a comprehensive, integrated strategy for the vast and complex business needs of the Department requires time and resources.

Until well into calendar year 2000, OCIO was primarily focused on the Y2K anomaly. Most of our staff and attention was directed to ensuring that as we moved into the year 2000, our systems and those of our partners, would continue to deliver the products and services they were designed to provide. Y2K was our overriding priority and we are proud of our success in that endeavor.

Appendix II
Comments From the Department of
Agriculture

Nevertheless, during this same period of time, OCIO responded to the Secretary's direction to assess the Department's overall cyber security program and develop plans for improvement. Our August 1999, Action Plan to Strengthen USDA Information Security provides a comprehensive strategy for building a sound cyber security program. OCIO based this plan on the best practices of leading organization, as well as guidance provided by oversight agencies. In fact, the plan relies heavily on GAO's own executive guide to information security management.

Our action plan addresses a number of critical security disciplines and management strategies. We have established priorities for these:

- Establishing an Associate CIO for Cyber Security and establishing a central management focal point to carry out key activities.
- Addressing immediate security risks and solving security problems, particularly network intrusions, as they arise.
- Developing practical risk assessment procedures that link security to business requirements and manage this risk on a continuing basis.
- Designing and implementing a department-wide information security architecture that aligns security measures with identified risks and vulnerabilities.
- Implementing a security awareness and training program to ensure USDA employees have the knowledge and skills they need to safeguard information assets.
- Implementing a software control and licensing program
- Implementing an information survivability program that will address intrusion detection, data protection, system recovery, and legal investigation.
- Implementing a system certification program designed to evaluate system security controls and ensure that sensitive systems are continually managed with security as a top priority.

See comment 2.

Unfortunately, by the time the OCIO security action plan was issued in August 1999, USDA's budget request for fiscal year 2000 had already been formulated and did not include a request for the plan's implementation. With the \$500,000 increase OCIO did receive for cyber security in fiscal year 2000, the action plan priority items are being addressed. For example, in fiscal year 2000 OCIO hired an Associate Chief Information Officer for Cyber Security and has begun staffing its Cyber Security Program. Since his arrival, the Associate CIO for Cyber Security has formed a work group to address risk assessment, is analyzing encryption requirements and tools, has formed a Cyber Security Emergency Response Team, and is overseeing a USDA contract effort that will engage expertise to assist the Department and its agencies in establishing a comprehensive information security program for Internet/Intranet/Extranet services and standardized security solutions.

See comment 3.

The President's fiscal year 2001 budget requested a \$6.6 million increase in funding for cyber security. The Department intends to request another substantial increase for cyber security in its FY 2002 budget submission. If granted, these increases will allow OCIO to address the full spectrum of security disciplines necessary to fulfill its security action plan.

**Appendix II
Comments From the Department of
Agriculture**

See comment 3.

The FY 2001 increase will provide the resources to complete the development of a USDA risk management program, the cornerstone of any cyber security program. In addition, OCIO will expand its Cyber Security Office, thereby bringing into USDA the requisite skills and expertise necessary to provide timely and appropriate advice and support. Existing policies will be completely reviewed and changed where necessary, and new policies and procedures will be implemented. Cyber Security Program staff members will also conduct a number of on-site reviews, to both identify security weaknesses and to provide training and hands-on assistance. The OCIO Cyber Security Program project plan also calls for a major effort in FY 2001 to define requirements for a security architecture and begin its design and implementation.

However, the initial congressional mark-up suggests substantially less will be appropriated for FY 2001 than we have requested. If so, some of our planned activities must be curtailed or deferred until additional resources are made available.

For fiscal year 2002, our proposed budget would allow the Cyber Security Office to address the balance of issues necessary to fulfill the OCIO security action plan. New initiatives planned for FY 2002 include the development and implementation of a Security Awareness and Training Program, addressing software control and licensing, establishing an Information Survivability Program that will address intrusion detection, emergency response, disaster recovery and business continuity, and a Sensitive System Certification Program.

See comment 4.

An initial project plan (attachment I) including milestones, deliverables, and time frames for these and other security program activities accompanies this report, along with a summarization of our budget requests for the current and next two years (attachment II).

Furthermore, we offer additional comments regarding the draft report. They are:

See comment 1.
Now on p. 4.

1. In the paragraph entitled "USDA HAS DEVELOPED A PLAN TO STRENGTHEN DEPARTMENTWIDE INFORMATION SECURITY", (page 6), the report states that USDA's Secretary asked for an information security improvement plan as a result of OIG and GAO reports. We feel this statement alone minimizes Secretary Glickman's long-standing and keen interest in federal information security. He is particularly attuned to the issues of computer security, having co-authored the Computer Security Act of 1987.

Since receiving the August 1999 Information Security Action Plan, Secretary Glickman has championed its implementation, ensuring it remains a top USDA priority. He insisted that OCIO hire the best computer security manager available and he has supported OCIO's budget requests for substantial increases in cyber security.

**Appendix II
Comments From the Department of
Agriculture**

See comment 1.

The report is silent on Secretary Glickman's proactive position in regards to information technology security at USDA. We request that the report more accurately reflect his interest and involvement.

See comment 5.
Now on p. 6.

2. In the paragraph entitled "LITTLE PROGRESS MADE IMPLEMENTING RECOMMENDED INFORMATION SECURITY IMPROVEMENTS", (page 8), focus is placed on the fiscal year 2000 budget resources that have so far been devoted to cyber security at USDA. The narrative indicates that part of USDA's \$1.2 billion in information technology budgets could have and should have been redirected to the Department's Cyber Security Program (page 10). This position suggests a degree of budget flexibility that simply does not exist. Much debate and consideration is given to all agency and departmental requests. Priorities are established and compromises are made, when necessary. Moreover, appropriations are specific to USDA agency and Departmental activities and programs. Once these appropriations have been granted to the various agencies, the CIO's authority is very limited, even for technology issues that require some reallocation of resources.

In addition, this section of the report identifies \$61 million in working capital funds and \$6 million in OCIO office budget and suggests they too could have been directed toward OCIO's Cyber Security Program. Working capital funds are directed to OCIO's fee-for-service activities in Kansas City, Ft. Collins, Co., and Washington DC headquarters operations. They support telecommunications services and application development and maintenance and therefore are not available for reallocation. The CIO's office budget is almost entirely devoted to personnel salaries and expenses. Within the CIO office little is available for program expansion. We suggest that the narrative be changed to more accurately reflect the budget limitation within the CIO.

See comment 2.

As stated previously, our information security action plan was developed after the FY 2000 budget was submitted. Since that time, OCIO has devoted much effort to developing implementation strategies and corresponding budget requests. In less than a year after it was issued, we believe we have demonstrated our commitment to its fulfillment and would recommend that your report more accurately reflect our progress to date.

See comment 6.
Now on p. 6.

3. The report points to the fact that business risks have yet to be completely determined across USDA, nor have assessments been made to identify vulnerabilities (page 9). While OCIO recognizes its responsibility to oversee and encourage these and other security activities, accountability for system security ultimately must be borne by system owners, managers and users. Within the Department security framework, the business community determines the specific security requirements. Also, the business community must pay for necessary or required security controls. We believe the report should more accurately address this issue of accountability and distinguish between OCIO's policy and oversight role and agency security control and operations responsibilities.

**Appendix II
Comments From the Department of
Agriculture**

USDA is committed to meeting its information system security responsibilities. We believe our plan and our strategy to implement security is a sound and reasonable approach. Our actions to date provide evidence that our intentions are good and that our proposed action plans for the future will lead to a significantly improved cyber security program. We request that you consider adjusting your report to reflect the issues we have identified.

GAO Comments

1. USDA noted a concern over the tone of the draft report, stating that the draft should better reflect USDA Secretary Glickman's proactive attitude toward cyber security. Specifically, USDA stated that Secretary Glickman co-authored the Computer Security Act of 1987 and has maintained a keen interest in the security of USDA's information assets throughout his tenure. We added language to the report to reflect this.
2. We added language to the report noting that by the time the OCIO security plan was issued in August 1999, USDA's budget request for fiscal year 2000 had already been formulated and did not include a request for the plan's implementation.
3. Discussed in "Agency Comments and Our Evaluation" section of this report.
4. These attachments have not been reprinted in the report.
5. USDA noted that the draft report indicates that part of USDA's \$1.2 billion in information technology budgets and \$61 million in working capital funds could have and should have been redirected to the department's cybersecurity program.

This is not an accurate characterization of what the draft report stated. Specifically, the draft report states that we were told by the OCIO that USDA did not attempt to fund needed security improvements in fiscal year 2000 to jump-start the departmentwide information security program by (1) reassessing the department's other information technology priorities and resources and (2) seeking approval to use a portion of the other available fiscal year 2000 information technology resources for this purpose.

6. USDA commented that the draft report points to the fact that business risks have yet to be completely determined across USDA, and assessments have not been made to identify vulnerabilities. While USDA did not dispute this, it noted that the report should more accurately distinguish between OCIO's policy and oversight role and the agency security control and operations responsibilities. We believe the background section of the draft report accurately describes these responsibilities.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:

(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

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

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

<p>Bulk Rate Postage & Fees Paid GAO Permit No. GI00</p>

