United States Department of Agriculture
Office of Inspector General

Audit of the Office of the Chief Information Officer's FYs 2010 and 2011 Funding Received for Security Enhancements

Audit Report 88401-0001-12

August 2012

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

DATE: August 2, 2012

AUDIT
NUMBER: 88401-0001-12

TO: Cheryl L. Cook
Acting, Chief Information Officer
Office of the Chief Information Officer

ATTN: Denice Lotson
Acting Agency Audit Liaison

FROM: Gil H. Harden
Assistant Inspector General for Audit

Gil H. Harden

SUBJECT: Audit of the Office of the Chief Information Officer's FYs 2010 and 2011
Funding Received for Security Enhancements

This report presents the results of the subject review. Your written response to the official draft is included at the end of this report. Excerpts of your June 21, 2012, response and the Office of the Inspector General's (OIG) position are incorporated into the applicable sections of the report.

We accept management decision for Recommendation 1. Based on your response, we were unable to reach management decision on Recommendations 2, 3, and 4. Management decision for these recommendations can be reached once you have provided the additional information outlined in the OIG Position section under each recommendation.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned, and timeframes for implementing the recommendations for which management decisions have not been reached. Please note that the regulation requires management decision to be reached on all recommendations within 6 months from report issuance, and final action to be taken within 1 year of each management decision to prevent being listed in the Department's annual Performance and Accountability Report. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions.

Table of Contents

Office of the Chief Information Officer's FYs 2010 and 2011 Funding Received for Security Enhancements

Executive Summary

In fiscal year (FY) 2010, Congress provided the Office of the Chief Information Officer (OCIO) a $44 million increase to its baseline appropriations from approximately $18 million to $62 million for security enhancements within the Department of Agriculture (USDA). In FY 2011, OCIO received $22 million in additional security enhancement funding for a total appropriation of $40 million. These funds were intended to help OCIO improve USDA's information technology (IT) security posture.[1] To accomplish this, OCIO selected 16 projects and, as of April 2, 2012, had expended $63.4 million on these projects. We initiated this audit to determine how OCIO utilized funding in FYs 2010 and 2011, primarily focusing on the increase for security enhancements in OCIO's annual appropriation request.

Over the last few years, OCIO has taken action towards improving security efforts at the Department, such as establishing the Agriculture Security Operations Center (ASOC) as an enterprise operational presence for OCIO's security activities. Prior to this, the only security organization at the Department-level was primarily focused on policy and compliance tracking. ASOC now has Federal employees with the requisite skills that provide enterprise services in security engineering, monitoring and analysis, incident handling, and security integration. Within ASOC, the Department has deployed security management tools to monitor and protect network traffic.

While we acknowledge that OCIO has made progress in addressing USDA's security posture, there is further need for improvement. Since 2009, we have noted that OCIO should prioritize its efforts to mitigate IT security weaknesses and accomplish a manageable number of the highest priority projects before proceeding to the next set of priorities.[2] We continue to find that OCIO's efforts should have been strategically planned, prioritized, and managed in order to be more effective. First, we found that several of OCIO's projects did not meet the purposes outlined in the Congressional request for funding or address the Department's most critical IT security concerns.[3] For example, OCIO funded an intern program for a total of $2 million which, while funded as a security enhancement project, only resulted in one intern being hired full-time for ASOC. In other instances, we found that OCIO exceeded proposed budgets for projects, or did not allot sufficient funding to key security areas. Second, we found that some projects were not completely implemented. For example, we found that OCIO had only assigned two individuals to analyze 13.3 terabytes of security alert data per day, resulting in the analysis of approximately

[1] Security posture describes how well an organization has minimized security risks. It consists of technical and non-technical policies, procedures, and controls that are the result of the strategy an organization undertakes to minimize risks.

[2] *U.S. Department of Agriculture, Office of the Chief Information Officer, Federal Information Security Management Act Report*, FYs 2009-2011, 50501-0015-FM, (October 2009), 50501-0002-IT, (November 2010), and 50501-0002-12 (November 2011).

[3] 2010 USDA Budget Explanatory Notes for Committee on Appropriations, Office of the Chief Information Officer, (April 2009).

10 security incidents a week.[4] The actual number of weekly incidents is unknown and could vary each week. OCIO stated that regardless of the resources available, the amount of information gathered is so massive it would require a tremendous workforce to evaluate all incidents identified by the security sensor array.[5] Lastly, other projects were not sufficiently coordinated, which included projects with duplicate objectives. For example, OCIO spent $235,000 on a project that duplicated another project's objectives, and was subsequently cancelled. This occurred because OCIO did not adequately develop oversight mechanisms and internal controls to plan projects, coordinate and communicate between projects, or determine how it would effectively utilize its resources. Because these projects were not effectively planned, coordinated, or managed, the Department's information systems are still at risk.

Recommendation Summary

OCIO should document the prioritization of projects Departmentwide, develop detailed internal control procedures for project management, and strengthen communication and coordination between OCIO management, project managers, account managers, and contractors.

Agency Response

In its written response dated June 21, 2012, OCIO concurred with the four recommendations in this report. Excerpts from the response and OIG's position have been incorporated into the relevant sections of the report. The written response is included in its entirety at the end of the report.

OIG Position

We accept OCIO's management decision for Recommendation 1. For Recommendations 2, 3, and 4, OCIO needs to specify actions to be taken and provide an estimated completion date for implementation.

[4] A terabyte is defined as a unit of storage capacity equal to one trillion bytes. A byte is about one character (e.g., a letter or a number).

[5] The ASOC security sensor array is a comprehensive and cohesive integrated security solution comprised of a suite of security tools, which have been deployed at multiple locations across the country within the USDA's network and is the foundation for enterprise wide security monitoring, detection, and protection.

Background and Objectives

Background

The Clinger-Cohen Act of 1996 required the establishment of a Chief Information Officer (CIO) for each major Federal agency. The Act requires USDA to maximize the value of IT acquisitions to improve the efficiency and effectiveness of its programs. To meet the intent of the law and to provide a Departmental focus for information resources management issues, USDA established OCIO.[6] The CIO serves as the primary advisor to the Secretary on IT issues. The OCIO website states its "primary responsibility is to supervise and coordinate within USDA the design, acquisition, maintenance, use, and disposal of IT by USDA agencies, as well as monitoring the performance of USDA's IT programs and activities."[7]

One of OCIO's primary responsibilities is to oversee the Department's IT systems and security efforts.[8] Specifically, this includes:

- Periodic risk assessments that consider internal and external threats;
- Development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the Department's information;
- Training that covers security responsibilities for personnel;
- Periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- Processes for identifying and remediating significant security deficiencies;
- Procedures for detecting, reporting, and responding to security incidents; and
- Annual program reviews by Department officials.

To evaluate IT security needs throughout the Department, OCIO created a 36-month plan and in May 2009 organized a team, referred to as the Tiger Team, which identified the Department's top security issues. The team consisted of 5 of USDA's 33 agencies and offices.[9] The Tiger Team identified almost 100 issues and a series of 37 solutions for those security issues, which were intended to be the basis for implemented projects.

In April 2009, OCIO requested a $44 million increase to its baseline of $18 million for security enhancements within the Department, which it received for FY 2010.[10] In FY 2011, OCIO received $22 million in additional funding, which was $22 million less than it anticipated. In addition, OCIO received an extra $27 million in FY 2012 above the FY 2009 baseline of

[6] Secretary's Memorandum 1030-30 (August 8, 1996).

[7] http://www.ocio.usda.gov/index.html.

[8] Public Law 107-347, *e-Government Act,* Title III FISMA.

[9] The five agencies consisted of OCIO, the Food and Nutrition Service, the Animal and Plant Health Inspection Service, the Office of the Chief Financial Officer, and the Forest Service—which constitutes a small portion of USDA's total 33 agencies and offices.

[10] Public Law 111-81, Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriation Bill, 2010 (June 23, 2009).

$18 million. These increased funds were intended to improve the Department's IT security by conducting network security assessments, procuring and deploying security tools, and establishing the ASOC to monitor and protect USDA's systems. As of April 2, 2012, OCIO had expended $63.4 million on security enhancements. OCIO selected 16 projects to enhance the Department's IT security. In FY 2010, OCIO chose to initiate all 16 projects simultaneously, expecting a continuation of funding in future years. However, in April 2011, Congress decreased OCIO's appropriation as part of the continuing resolution.[11] This caused projects to be severely scaled back and project timelines to be extended further into the future.

Objectives

The objective of this audit was to determine how OCIO utilized funding in FYs 2010 and 2011, primarily focusing on the increase for security enhancements requested by OCIO and the internal controls implemented to ensure the funds were expended in a manner to mitigate the risk of waste and mismanagement.

[11] Public Law 112-10, *Department of Defense and Full Year Continuing Appropriations Act 2011* (April 15, 2011).

Section 1: Effectively Plan, Prioritize, and Manage Projects

Finding 1: OCIO Needs to Effectively Plan, Prioritize, and Manage its Projects

While OCIO has made progress in addressing the Department's security needs, OCIO's efforts would have been more effective if strategically planned, prioritized, and managed. Specifically, we found that some of OCIO's projects did not meet the purposes outlined in the Congressional request for funding or were not targeted to improve the most critical IT security risks.[12] Additionally, some of these projects were not completely implemented, and were not sufficiently coordinated. This occurred because OCIO did not adequately plan projects and determine how it would utilize both internal and external resources. Additionally, OCIO did not establish the internal control procedures for project management necessary to track and monitor expenditures and project progress. Because these projects were not effectively managed, the Department's information systems are still at risk, even after expending $63.4 million of funding increases received in FY 2010 and 2011.[13]

According to OCIO, in 2009, USDA networks were under constant attack and were targeted by an abundance of malicious activity, and USDA had no visibility into its own networks. The only means for the Department to become aware of these compromises was if the Department of Homeland Security, law enforcement, or other intelligence agencies informed OCIO of a problem, which happened frequently. Since that time, OCIO has established ASOC. Prior to this, the only security organization at the Department-level was primarily focused on policy and compliance tracking. ASOC now has federal employees with the requisite skills that provide enterprise services in security engineering, monitoring and analysis, incident handling, and security integration. Additionally, in FY 2011, ASOC stated that it responded to three times as many incidents compared to FY 2010, indicating that USDA is evolving to a more mature and proactive stance regarding security monitoring and incident handling. Within ASOC, the Department has deployed security management tools to monitor and protect network traffic. Due to this increase of insight into USDA's network, ASOC has been able to detect a number of incidents and block malicious activity as it occurs.

The Department has also implemented the Tivoli Endpoint Manager, an inventory management system, on over 140,000 endpoint devices, such as desktops, laptops, and servers.[14] This has allowed the Department to gather data and report to the agencies on a number of potential vulnerabilities in real-time and determine the risk presented by emerging threats. This reporting effort has resulted in improved ability to manage the numerous USDA endpoints at risk.

While OCIO has made progress in addressing the Department's IT security weaknesses, there is room for improvement. In FY 2009, we recommended that OCIO's efforts to mitigate material

[12] 2010 USDA Budget Explanatory Notes for Committee on Appropriations, Office of the Chief Information Officer, 111st Cong., 2nd sess. (April 2009).

[13] As of April 2, 2012, OCIO had expended $63.4 million for IT security enhancements.

[14] The Tivoli Endpoint Manager project established a Departmentwide inventory management system to report the status of all USDA devices.

IT security weaknesses in the Department be prioritized, with defined goals and realistic timeframes. We also recommended that OCIO accomplish a defined set of critical objectives prior to proceeding on to the next set of priorities.[15] OCIO concurred with these recommendations. However, when we did further audit work of OCIO's efforts in FY 2011, we noted the same issues and once again recommended that USDA undertake a manageable number of its highest priority projects and show measureable progress towards the milestones for each active project.[16] As of April 2012, we have not achieved management decision on this recommendation. OCIO has not sufficiently prioritized or managed its projects intended to reduce critical IT security weaknesses. Specifically, OCIO did not always 1) expend resources to sufficiently address the most critical IT security weaknesses, 2) fully implement projects, or 3) efficiently manage resources both collaboratively between projects and within individual projects. Instead, OCIO initiated 16 projects simultaneously.

Expenditures Did Not Sufficiently Address Established, Critical IT Security Weaknesses

When requesting an increase in funding from Congress, OCIO proposed that these funds would be used to bolster three IT security areas: Network Security Assessments, Security Tools, and a Security Operations Center. For FY 2010, Congress specified that the $44 million increase in funding should be used "to improve the Department's information technology security by conducting network security assessments, procuring and deploying security tools, and establishing the Agriculture Security Operations Center to monitor and protect USDA's systems."[17] However, we found that when OCIO received its funding increase for the proposed projects, it did not use the money exclusively for the purposes outlined in its Congressional request or for projects addressing the Department's most critical IT security concerns.

We found that OCIO did not always use the allocated money as requested to complete the most critical IT security projects. For example, in FY 2010, OCIO spent $4.7 million on other projects, rather than on network security assessments, as proposed to Congress. As a result, though OCIO stated to Congress that it would complete 11 network assessments by FY 2010, we found that it only completed 8 by the end of that year.[18] While providing some benefits, the completed network security assessments, costing $2.7 million, did not meet Federal guidelines.[19] For example, OCIO's security assessment methodology did not identify examination techniques for some monitoring network and device communications, which may have left critical network vulnerabilities unaddressed. The original reason for planning and conducting these network assessments was to identify,

[15] *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2009 Federal Information Security Management Act Report*, Audit Report 50501-0015-FM (October 1, 2009).

[16] *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2011 Federal Information Security Management Act Report*, Audit Report 50501-0002-12 (November 15, 2011).

[17] Public Law 111-81, Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriation Bill, 2010 (June 23, 2009).

[18] *Report to Congress on the Status of Information Technology Security FY 2010 Program Activities through early February 2010; Subcommittee on Agriculture, Rural Development, Food and Drug Administration, and Related Agencies* (May 17, 2010).

[19] National Institute of Standards and Technology (NIST) Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment* (September 2008).

track, and mitigate security weaknesses. In addition, though required by Office of Management and Budget (OMB), none of the Department's agencies created Plans of Action and Milestones (POA&Ms) for the vulnerabilities identified by the network assessments because OCIO did not enforce compliance.[20]

OCIO expended over $6.7 million in FYs 2010 and 2011 for three projects not proposed to Congress (Exhibit A).[21] For example, a two-year internship program, which cost approximately $2 million, was initiated with these funds. This project is intended to develop and sustain a highly skilled IT security and computer technology workforce. Expenditures for FY 2010 and 2011 included over $686,000 for development and implementation of a networking website and approximately $192,500 in housing costs for two summers. While the intern program may be a beneficial step in the long-run, it did little to further the more pressing objective of improving USDA's IT security. Focusing resources on this project may have detracted from other, more pressing projects, such as conducting network security assessments, that more directly addressed Congress' and the Department's IT security priorities.

We found that the projects OCIO initiated did not always align with the priorities laid out in OCIO's own initial planning efforts. Prior to receiving increased funding, OCIO developed a 36-month plan and invited USDA agencies to provide input to develop project initiatives based on the various needs of the Department. Referred to as the Tiger Team, representatives from 5 of USDA's 33 agencies and offices developed a total of 37 solutions to IT security issues.[22] While this should have been a key step to planning and addressing assessed Departmental needs, we found that three of the Tiger Team's highest-priority initiatives—physical security, media sanitization and disposal, and network firewalls—were not addressed by the 16 selected projects.[23]

Projects Not Fully Implemented

With multiple, interconnected projects to manage, it is important that OCIO ensure that projects are implemented with realistic and manageable timeframes. Without these

[20] OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004), requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. POA&Ms identify tasks needing to be accomplished to assist agencies in assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. A POA&M details resources required to accomplish the elements of the plan, milestones for meeting the task, and scheduled completion dates for the milestones.

[21] Although we acknowledge that one of these projects, Certification and Accreditation, was initiated to remedy a previous OIG recommendation, we have included it in this report, because it was not included as a security initiative by OCIO as a basis for increasing its funding in its request to Congress.

[22] The five agencies consisted of OCIO, the Food and Nutrition Service, the Animal and Plant Health Inspection Service, the Office of the Chief Financial Officer, and the Forest Service—which constitutes a small portion of USDA's total 33 agencies and offices.

[23] The Tiger Team determined the highest priority initiatives by aggregating decision criteria such as mitigating risk, business impact, and meeting regulatory requirements. Physical security refers to the controls that help protect computer facilities and resources from espionage, sabotage, damage, and theft. Media sanitization and disposal refers to the disposal, clearing, purging, and destroying of media when no longer needed. Network firewalls allow or disallow communication to or from networks based upon rule sets determined by the agency.

measures, security enhancements may be outdated by the time projects are completed. In December 2010, the U.S. Chief Information Officer explained that to prevent implementing outdated technology and solutions, Federal IT programs must be structured to deploy working business functionality in release cycles no longer than 12 months and, ideally, less than 6 months, with initial deployment to end users no later than 18 months after the program begins.[24, 25] Additionally, to ensure that IT projects progress as planned, the Clinger-Cohen Act of 1996 requires agency management to implement a system of milestones for measuring IT project progress.[26]

However, we found that OCIO has initiated more projects than it can complete in a reasonable timeframe. Of the 16 projects OCIO undertook to further USDA IT security efforts, 7 projects were completed. Of these, 3 were pilot projects conducted to evaluate potential software options for the Department, none of which were determined to be viable. As of February 2012, 9 projects were still in progress for longer than the U.S. Chief Information Officer's recommended 12-month implementation timeframe. OCIO did not create milestones for eight projects, and critical projects have not been completed because significant resources were redirected elsewhere.

These critical projects have not been as comprehensive as they were intended to be. For example, in FY 2010, OCIO informed Congress that it would utilize $12.3 million to establish ASOC, which was to "coordinate continuous 24x7x365 security operations to defend USDA information, assets, network and systems."[27] For FYs 2010 and 2011, OCIO has expended over $18.7 million towards accomplishing this goal. OCIO expended an additional $10.6 million for the security sensor array project, to "employ state of the art monitoring, incident response, threat analysis, and forensics capabilities."[28]

However, we found that while OCIO has tools in place for monitoring daily data, security efforts are not as robust or comprehensive as they should be to support an effective 24x7x365 security operation. While the security sensor array gathers data for threat analysis and forensics capabilities, this information is not fully analyzed, and has resulted in security issues not being investigated. Though this stands as an immense and important undertaking which OCIO has invested $29.3 million towards accomplishing, ASOC has only assigned two individuals to work on data monitoring and analysis and it only operates 11 hours a day, 5 days a week. OCIO stated that the resources required to fully review, address, and resolve every event that the security sensor array identifies is unknown due to the tremendous amount of data generated. We found that because OCIO has not designated the necessary number of personnel, OCIO is only able to analyze and

[24] The U.S. Chief Information Officer position was established within the White House's OMB to provide leadership and oversight for IT spending throughout the Federal Government.

[25] *25 Point Implementation Plan to Reform Federal Information Technology Management* (December 9, 2010).

[26] Clinger-Cohen Act (January 1996).

[27] *2010 USDA Budget Explanatory Notes for Committee on Appropriations, Office of the Chief Information Officer.* 24x7x365 is defined as 24 hours a day, 7 days a week, and 365 days a year.

[28] The ASOC security sensor array is a comprehensive and cohesive integrated security solution comprised of a suite of security tools, which have been deployed at multiple locations across the country within the USDA's network and is the foundation for enterprise-wide security monitoring, detection, and protection.

process approximately 10 security incidents a week. This allows the vast majority of incidents to go unanalyzed.

Additionally, OCIO was not adequately remediating identified weaknesses. First, we found during our review that OCIO was not conducting vulnerability scans.[29] OCIO stated that it did not have the licensing available to accomplish scanning. As of January 2012, ASOC has been performing vulnerability scans as recommended by OIG and dictated by USDA policy. Second, OIG identified 77 of 333 software packages on the security sensor array that had not received recommended security patches.[30] These patches safeguard against known security threats and are a necessary step for IT security. Finally, as of February 2012, we found there were 1,309 critical and high unmitigated vulnerabilities, of which 624 were over 30 days old and POA&Ms had not been created.[31]

We also found that projects were not as far along as they should have been. For example, several projects have been partially implemented because of a sudden reduction in contractor personnel. When OCIO received a total of $40 million for FY 2011, $22 million less than what it anticipated, OCIO decided to reduce the number of contractors working on key projects from 48 to 4. As a result of this abrupt, unanticipated transition, progress on several projects was halted or delayed. For example, two contractor-run projects, with a total cost of $4.7 million, were intended to create and implement required risk management policy and procedures to ensure agency compliance with Federal and Departmental regulations. [32] However, OCIO was not efficiently monitoring the contractors' progress. Consequently, when budgetary cuts came, and the contracts were terminated, OCIO was not aware of the contractors' progress and therefore was unable to fully utilize the work performed by the contractors. This set OCIO back significantly, and OCIO was unable to meet Federal guidelines. Additionally, when OCIO released the contractor assigned to a $2.9 million project, OCIO found that it did not have access to the administrator functions—which had been maintained by the contractor. Although some functions were available, without access to the administrator accounts OCIO was unable to provide critical Department-level information.

[29] Vulnerability scanning is the process of searching the network and its devices, including servers, for known vulnerabilities. It is used to identify vulnerabilities that need to be remediated and also to verify that required patches have been applied. Patching is the process of applying software updates to remediate and prevent known vulnerabilities. Software vendors release patches periodically to fix known flaws and to upgrade the software.

[30] Vulnerability data were obtained for 3 of the 11 security sensor sites, which included the primary, backup, and monitoring sites.

[31] The vulnerability scanning software ranks vulnerabilities on a severity scale of 1-10. The scanning software considers vulnerabilities ranked 4-10 as critical or high. The Department *Plan of Action and Milestones Management Standard Operating Procedure* (June 29, 2011) requires that POA&Ms must identify the source of the vulnerability and be created within 30 days of vulnerability identification if not immediately resolved.

[32] *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 (February 2010).

Project and Resources Were Not Efficiently Managed

With fluctuating budgets on multiple, high-priority projects, it is crucial that project expenditures be carefully managed both collaboratively between projects and within individual projects. Without careful management of resources and expenditures, OCIO cannot ensure that funds are expended as originally intended for uses that would best accomplish project goals. The Government Accountability Office (GAO) states that effective stewardship of Federal funds depends upon the establishment of certain internal controls meant to ensure that those funds are used in the most efficient manner to maximize the impact of the funding received.[33] Likewise, *The USDA Management Control Manual* states that management controls are used to reasonably ensure that projects and resources are protected from waste and mismanagement.[34]

However, we found that OCIO had not managed resources efficiently for some of its key IT security projects. Specifically:

- In FYs 2010 and 2011, OCIO spent at least $1.8 million to acquire four tools for the security sensor array project—which are not currently used—and subsequently spent additional annual maintenance costs of approximately $1.2 million. In addition, OCIO determined that one of these tools, costing approximately $425,000, could not handle the amount of data that USDA's network generates. OCIO has maintained this tool at a cost of approximately $81,000 annually but has not been able to utilize it. As of December 2011, OCIO stated that it was determining the feasibility of using the tool elsewhere.
- In FY 2010, OCIO spent $235,000 to research possible solutions for a project intended to prevent data leakage outside of USDA networks.[35] The project was subsequently cancelled because its goals were redundant with another ongoing project, the security sensor array.

With proper coordination within OCIO and improved communication between project managers, these unnecessary costs could have been avoided. Careful planning and coordination of expenditures is necessary to ensure projects and project costs are optimized to accomplish IT security goals and reduce wasteful spending.

In other instances, OCIO did not appropriately track resources or expenditures. Guidance from the Office of the Chief Financial Officer states that all direct costs, such as salary and other benefits for employees working directly on projects and all goods and services must be included in the full cost of projects.[36] However, we found that 11 of 16 projects did not have Federal salaries and benefits charged to them. One project charter specifically instructed Federal employees to track their hours but not to charge them to the project, even though Federal employees were working directly on the project, as indicated by bonuses and travel expenses charged to this project. For another project,

[33] GAO, *Standards for Internal Control in the Federal Government* (November 1999).
[34] *USDA Management Control Manual*, Department Manual 1110-002 (November 29, 2002).
[35] Data leakage refers to the unauthorized transfer of information from a computer or datacenter to the outside world.
[36] Office of Chief Financial Officer, *Agriculture Financial Standards Manual* (May 2004).

> OCIO explained that full contract costs were not included in the project in order "to maximize the ASOC security dollars."
>
> Without providing supporting documentation for accounting transactions, OCIO cannot adequately oversee and manage its projects. OCIO assigned this responsibility to the control account managers (CAMs), who were required to track, summarize, and report all obligations and expenditures. We found that OCIO lacked oversight on several of its projects. For example, expenditures for two projects exceeded obligations by approximately $1.2 million. The two project CAMs could not adequately justify the expenditure overages with supporting documentation. One of these projects also incurred interest charges due to a late payment.
>
> We also found that OCIO was not taking adequate steps to document and account for its projects in order to ensure that it was providing adequate oversight. For instance, OCIO could not provide OIG with 36 contracts that would explain specific contractor work, deliverables, and costs.[37] When we asked how many project contracts there were in total, OCIO was not able to provide a comprehensive list of all project contracts.

These issues occurred because OCIO had not established internal control procedures, such as monitoring and oversight, for project management, and did not adequately plan its projects or how it would utilize resources. When we looked at OCIO's internal controls for the 16 projects, we noticed an overall lack of controls necessary to ensure timelines were met, and to ensure funds and supporting documentation were appropriately tracked. Specifically, OCIO did not:

- provide an organizational structure to facilitate project oversight and timelines;
- have an overall project plan that considered risk factors that could impact completion of the security projects—such as budget reductions;
- implement appropriate policies, procedures, techniques, and control mechanisms to ensure sufficient documentation and expense management; or
- put a system in place to identify and communicate information to decision makers, such as regular project progress updates for on-going contracted work.

We also found that OCIO was not properly coordinating between projects in order to prevent duplicate project objectives. OCIO officials, CAMs, and contractors did not effectively communicate within projects in order to accurately track and monitor project progress, costs, and status.

When we spoke to OCIO regarding the number of projects initiated, OCIO felt it could not have scaled down the number of simultaneous projects because IT systems are complex, and require many components to come together. While we acknowledge that IT projects—like many projects—are complex, initiating all plans simultaneously led to a thin distribution of resources and strained oversight capabilities. While these 16 projects may be beneficial to the Department's overall IT security efforts, it would have been more effective to implement a

[37] We use the term "contracts" to refer to both agreements made with non-Federal vendors and with other Federal agencies.

manageable number of projects, allowing for complete implementation, monitoring, and planning—rather than a thinly distributed effort across multiple fronts.

OCIO also explained that many projects were delayed due to administrative challenges, such as the migration of accounting records to a new financial system. Although we acknowledge that migrating to a new accounting system poses a significant challenge, OCIO is responsible for being able to account for money spent, and the new financial system is USDA's required system of record.

Additionally, OCIO stated that it did not receive funding until the second quarter of FY 2010, which resulted in officials needing to spend the funds in a shorter timeframe than anticipated. However, we determined that funding was actually apportioned in November 2009.[38] We also found the Tiger Team planning meeting took place in May 2009, prior to OCIO receiving the appropriation. With adequate planning, OCIO should have determined the best use of funds and how to monitor expenditures, even with a shortened timeframe.

We acknowledge that OCIO has made progress in several key areas, including system security documentation; improving its identity and access management program; and completing a deployment of a suite of network monitoring and detection tools, which should further enhance the security of its networks. While OCIO has made progress in addressing the Department's IT security needs, as stated in three previous audits, OCIO's efforts could have had more impact if projects and resources had been better planned and effectively managed.[39] Because they were not, the Department is still at significant risk, even after the additional funding. Once USDA deploys adequate resources to properly configure and completely monitor these tools, the Department's security posture should greatly improve.

Recommendation 1

Document the prioritization of projects Departmentwide to ensure the most critical projects take a higher precedence than other, non-critical projects.

Agency Response

OCIO concurs with this recommendation. On May 31, 2012, OCIO prioritized projects with the establishment of Continuous Monitoring as its highest priority project for 2013. The second highest priority project is the identification and development of program metrics and key

[38] According to OMB A-11.120.1, *Preparation, Submission, and Execution of the Budget* (August 2011), an apportionment identifies the amounts available for obligation and expenditure. It specifies and limits the obligations that may be incurred and expenditures made for specific time periods, programs, activities, projects, objects, or any combination thereof.

[39] *U.S. Department of Agriculture, Office of the Chief Information Officer, Federal Information Security Management Act Report*, FYs 2009-2011, 50501-0015-FM (October 2009), 50501-0002-IT (November 2010), and 50501-0002-12 (November 2011).

performance indicators. The third priority for OCIO in the coming year is the introduction and effective engagement of the agency security and operational personnel.

OIG Position

We concur with the agency response for this recommendation and have reached management decision.

Recommendation 2

Designate sufficient resources to adequately configure and monitor the security sensor array in order to defend USDA's information system against external and internal threats.

Agency Response

OCIO stated it will provide planned accomplishments and timelines to designate a group of security sensor array experts who will develop and provide instructions and hands-on training to agency IT personnel, and bring agency subject matter experts in to help OCIO better understand agency data and activities within 120 days of the date of this final report.

OIG Position

While OIG agrees this course of action will help to address this recommendation, in order to reach management decision, OCIO needs to finalize the plans and provide estimated completion dates for implementing these planned actions.

Recommendation 3

Develop detailed internal control procedures for project management that include the requirement to specify and document project milestones, accurately allocate and track project costs, develop project timelines, and establish project-specific roles and responsibilities.

Agency Response

OCIO implemented internal control procedures for managing initiatives by implementing a methodology for managing projects. As of FY 2010, OCIO required project managers to engage with the Portfolio and Project Management Branch of International Technology Services. OCIO will require all new projects to conform to the single artificial risk matrix model. These efforts have been supplemented with the ASOC contracted Project Management Office team to develop required project documentation that includes tailored project charters; defined roles and responsibilities, project plans, work breakdown structures, and project schedules.

OIG Position

While OIG concurs with OCIO's proposed actions, in order to reach management decision, OCIO needs to formalize this requirement in a policy and procedure and provide estimated release dates.

Recommendation 4

Strengthen communication and coordination between OCIO management, project managers (CAMs), and contractors, allowing the different parties to work collaboratively and effectively

Agency Response

OCIO has worked in collaboration with OCIO Program Management Office to manage the security project portfolio. At a minimum, all project managers communicate project status, through project team reports to the CAM; and the CAM, in turn, reports to OCIO leadership and its project management branch.

OIG Position

In order to reach management decision, OCIO needs to specify actions taken or that it plans to take and provide actual or estimated completion dates for implementation.

Scope and Methodology

Our review analyzed the funding that OCIO received in FYs 2010 and 2011, primarily focusing on the increased funding allocation for security enhancements. We compared the controls that OCIO had in place to plan, spend, and monitor this funding to GAO's Standards for Internal Control in the Federal Government.

Fieldwork for this audit was performed from March 2011 through January 2012 in Washington, D.C.; Kansas City, Missouri; and Denver and Fort Collins, Colorado.

To accomplish our audit objective, we performed the following procedures:

- Reviewed Office of Budget and Program Analysis (OBPA) and Congressional documentation regarding the increased funding allocation for the security enhancements.[40]
- Reviewed the methods and controls that OCIO put in place for implementing and monitoring the security enhancement projects as per budgetary requirements (Public Law 111-80), OMB, OBPA, and the Federal Acquisition Regulation (FAR).
- Reviewed financial transactions recorded in OCIO's accounting system associated with the FY 2010 and 2011 OCIO appropriations.[41]
- Selected a judgmental sample of contracts and transactions for analysis. The judgmental sample was based upon the number and availability of contracts within each project.
- Tested a judgmental sample of contracts using FAR guidelines.[42]
- Reviewed and analyzed financial transaction documentation support including contracts, statements of work, reimbursable agreements, and invoices.

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[40] Documents included the Appropriations Acts of 2010, 2011, and 2012; House of Representatives Explanatory Notes, and documents provided by OCIO to the House Appropriation Subcommittee staff.

[41] We relied on information from the Financial Management Modernization Initiative system. This is the USDA accounting system of record and is reviewed by OIG in *Department of Agriculture's Consolidated Financial Statements for Fiscal Years 2010 and 2009*, 50401-70-FM (November 2010) and *Department of Agriculture's Consolidated Financial Statements for Fiscal Years 2011 and 2010,* 50401-0001-11 (November 2011).

[42] FAR Part 6.1-6.3, *Fair and Open Competition*; and Part 15.406-3, *Documenting the Negotiation*.

Abbreviations

ASOC	Agriculture Security Operations Center
CAMs	Control Account Managers
CIO	Chief Information Officer
FAR	Federal Acquisition Regulation
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
NIST	National Institute of Standards and Technology
OBPA	Office of Budget and Program Analysis
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&Ms	Plans of Action and Milestones
USDA	Department of Agriculture

Exhibit A: OCIO Projects Not in Budgetary Request to Congress

Project	FY 2010 & 2011 Expenditures
IT Intern Program	$2,013,396
Re-engineered Certification and Accreditation	$2,458,360
Governance, Risk and Compliance	$2,249,998
Total	**$6,721,754**

USDA’S

OFFICE OF THE CHIEF INFORMATION OFFICER’S

RESPONSE TO AUDIT REPORT

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

June 21, 2012

TO: Gil H. Harden
Assistant Inspector General for Audit

FROM: Cheryl. L. Cook /s/
Acting, Chief Information Officer

SUBJECT: Request for Management Decision Concurrence on Recommendations 1-4
Office of Inspector General Audit # 88401-0001-12
"Audit of the Office of the Chief Information Officer's FYs 2010 and 2011 Funding Received for Security Enhancements"

The Office of the Chief Information Officer (OCIO) is requesting Management Decision concurrence on recommendation(s) 1-4 of the subject audit. OCIO concurs with all 4 recommendations. However, it is important to note that over the past year, OCIO has put in place processes and procedures as part of the ongoing maturity of the Agriculture Security Operations Center program that address the basis for the recommendations. These processes and procedures may not have been fully implemented at the outset of the audit.

Recommendation 1 – Document the prioritization of projects Department-wide to ensure the most critical projects have a higher precedence than other, non-critical projects.

OCIO concurs with this recommendation. OCIO/ Agriculture Security Operations Center (ASOC) has established rigorous procedures to focus on critical security concerns. ASOC will continue to work with OIG to ensure that the documentation of priorities is in an acceptable format. Securing our nation against cyber attacks has become one of the nation's highest priorities. As the organization charged with the responsibility for ensuring the Department's ability to support the national food supply chain, the agriculture economy, research and development, and an active loan portfolio of over $120 billion, we understand the challenges of securing this complex environment; as such, this urgent and compelling workload demands that we successfully manage multiple projects, risks, and emerging requirements on a daily basis. In response to this recommendation, on May 31, 2012, ASOC takes the establishment of Continuous Monitoring as its highest priority project for 2013. The biggest single issue facing ASOC, and USDA Enterprise Security as a whole, is the challenge of transforming security awareness through the automation of the risk and continuous assessment of the enterprise. Frequently referred to as Continuous Monitoring (CM), it is the challenge of taking the technology and processes that ASOC has built over the last two years (including BigFix™, the Security Sensor Array, Opnet™, and the ASOC monitoring, analysis, and forensics programs), weaving in the data and activities of OCIO and agency operational IT programs, and producing timely and actionable intelligence on the state of the enterprise and the prioritized issues requiring attention. Critical to determining the success of this effort will be the early agreement with OIG on how a nascent CM program will be measured and evaluated. Emerging guidance from the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technologies are all clear that there is no boilerplate approach to CM; each agency must determine what controls and processes can be adapted, and how that adaption can best be assessed. The ASOC efforts toward CM will be focused on continuous vulnerability assessment, which should be understood to be an activity set different from CM for continuous authorization, which is targeted to replace manual Certification and Accreditation activities. The planned ASOC activities are foundational for much of the Continuous Authorization model as it is currently being developed in the federal community. ASOC will complete the rollout of the Enterprise Vulnerability Scanner as a critical component of the continuous monitoring model. Within 120 days of this final report, ASOC will provide planned accomplishments and timelines regarding continuous monitoring.

A second high priority project for ASOC, identified on May 31, 2012, in conjunction with the CM activity, is the identification and development of program metrics and key performance indicators. Effective program management requires both the bottom-up (from the CM functions) and a top-down approach. The latter will be achieved through a cross-OCIO management effort that will identify and measure critical interdependencies, and the portion of those elements that can be met from ASOC data resources. We anticipate that developing useful metrics and KPI's will be an evolutionary process. ASOC recognizes the need to continuously improve them, based upon OIG and the Agency feedback, in order to shift focus in response to the evolving nature of cyber security threats. Within 120 days of this final report, ASOC will provide planned accomplishments and timelines regarding program metrics and key performance indicators.

The third priority for ASOC in the coming year (identified on May 31, 2012) is the introduction and effective engagement of the agency security and operational personnel. Incident Response is hampered when the parties engaged do not understand each other's methods, or the underlying data upon which the incident is predicated. Further, ASOC is hampered by the reduction in resources available to review and analyze the data being made available by the Security Sensor Array (SSA). By training agency personnel on ASOC tools and methods, and then extending connectivity to the SSA in a secure manner to those same agency personnel, ASOC can double or treble the number of simultaneous analysis sessions being performed. The agency personnel will also bring their subject matter expertise regarding agency data and activities to the ASOC, allowing the SSA tools to be further enhanced and tuned for more accurate monitoring. In addition, ASOC will continue leverage its investment in the SSA by developing and publishing agency-specific status reports in order to help agency CIOs and system owners improve their security posture. Within 120 days of this final report, ASOC will provide planned accomplishments and timelines regarding the introduction and effective engagement of agency security and operational personnel.

Recommendation 2 – Designate sufficient resources to adequately configure and monitor the security sensor array in order to defend USDA's information system against external and internal threats.

OCIO concurs with this recommendation. The architecture design of the security sensor array provides a means for granular control of ASOC infrastructure at the point of presence (POP); and includes the ability to work closer to infected workstations as well as detect lateral POP attack/infection. Information Security subject matter experts across the enterprise are being trained to make use of the enhanced awareness provided by the security sensor array.

With the implementation of the Security Stack Array (SSA) in April 2011, OCIO has been able to shift the USDA posture in security cyber threat operations from a reactive to proactive state. The array has greatly reduced the amount of data exfiltrated (stolen) from USDA. We have been and will continue to fine tune the tool's capabilities, reduce false positives, and train the supporting technical staff on the administration and usage of all the tool capabilities so that the tools can be used in a fully functional operational environment. Additionally, OCIO quickly recognized that the volume of potential security events that the Security Stack Array was identifying on a daily basis was presenting an enormous challenge to manage and research in a timely manner. To address this, OCIO initiated effort to develop and tune automated security rules and conditions to handle the volume of data. This effort was temporarily impacted when the budget was reduced in April 2011.

To partially meet the budget challenge, we have realigned staffing to better utilize our resources, improve general IT hygiene, and concentrate on High Value Targets (HVT) (personnel, systems and endpoints). We are also developing a cadre of SSA expertise by providing instruction and hands on training to agency IT personnel, bringing agency subject matter experts in to help OCIO better understand agency data and activities. The goal is to continue to fine-tune the SSA through implementation of security rules and conditions to proactively identify true attacks and compromises, and greatly reduce the false positives. Within 120 days of this final report, ASOC will provide planned accomplishments and timelines regarding this effort.

Recommendation 3 – Develop detailed internal control procedures for project management that include the requirement to specify and document project milestones, accurately allocate and track project costs, develop project timelines, and establish project-specific roles and responsibilities.

OCIO concurs with this recommendation. OCIO has implemented internal control procedures for managing ASOC Initiatives. The Portfolio and Project Management Branch (PPMB) of International Technology Services (ITS) was engaged at the onset of fiscal year 2010 to implement a consistent methodology for managing projects. The ITS PPMB Portfolio and Project Management Procedural Guide established management policies, procedures, and practices governing the origination, initiation, planning, implementation and closeout of the portfolio management framework and the ITS 5D Solution Life Cycle (Discover, Define, Design, Develop, and Deliver) stages of the Project Management Framework.

ASOC has established an internal management structure for project control adhering to the methodologies established by the PPMB framework and following principles based upon the PMI Project Management Body of Knowledge (PMBOK). Roles and responsibilities are defined in each project charter and identify each respective project stakeholder to their project function. Control Account Managers (CAMs), who are also OCIO program leaders, have been assigned delegated obligation authority to manage one or more control accounts, and are given the autonomy to assign the appropriate project resource levels to fulfill the expected outcomes. CAMs identify risks throughout each project's lifecycle and identify strategies to minimize the impact of risk occurrence. OCIO/ASOC also installed a team of certified Project Managers to serve as liaison to the CAMs, and each has been charged with ensuring that the internal project framework is implemented and followed. Project performance is measured against the project baseline in terms of schedule, cost, scope and quality and project status information is communicated during OCIO bi-weekly meetings where OCIO leadership is able to make key project decisions and recommendations. A change management process has been instituted to establish an orderly and effective procedure for tracking the submission, coordination, review, evaluation, and approval for release of all changes to the project's baselines. OCIO has also implemented several oversight mechanisms for detecting individual project risk. The overall project objectives have been defined in the project charters, and are also monitored via the bi-weekly CAMs meetings, and are supplemented with weekly senior executive reporting. Risks for each project are identified and addressed during the bi-weekly CAMS and/or senior executive reporting.

In addition, a project control environment has been provided by ITS support services which included cost accounting models, templates, common reporting forum (e.g., SharePoint). These efforts have been supplemented with the ASOC contracted PMO team to develop required project documentation that includes tailored project charters; defined roles and responsibilities, project plans, work breakdown structure (WBS), and project schedules. OCIO/ASOC have implemented a cost control governance model based upon the industry standard Project Managers Body of Knowledge (PMBOK), and with the assistance of OCIO/ITS, have developed and deployed one of the most sophisticated Cost Models ever attempted in FMMI. Continuous status and financial monitoring are an integral part of the ASOC activities, and have included ensuring appropriate closeout activities after the unexpected funding cut.

Because projects are at various stages of their respective life cycle, ASOC, in the interest of efficiency, has not required all projects to restart and re-develop all project artifacts into a single artificial risk matrix model. However, individual project risk was managed as part of overall governance, and, going forward, all new projects will conform to the recommended single artificial risk matrix model.

Recommendation 4 – Strengthen communication and coordination between OCIO management, project managers (CAM), and contractors, allowing the different parties to work collaboratively and effectively.

OCIO concurs with this recommendation. ASOC has worked in collaboration with the Office of Chief Information Officer (OCIO) Program Management Office (PgMO) to manage the security project portfolio. ASOC directs the management of all security initiatives and projects, determines priorities, and governs the strategic decision-making. OCIO PgMO directs the business practices that bring the world of projects into tight integration with USDA enterprise business operations. This combined leadership oversight affirms cross-agency and/or interoffice coordination of work efforts. Major components of the Project Portfolio Management include:

- Management oversight and governance
- Budget management
- Acquisition management
- Risk management
- Stakeholder management
- Standards and best practices
- Strategic goals and objectives
- Performance criteria (metrics), and
- Enterprise reporting

At a minimum, all projects communicate project status, whereby each project team reports to the CAM; and the CAM, in turn, reports to ASOC leadership and OCIO PgMO. Two typical forums for communicating status are through bi-weekly OCIO project status meetings and ASOC project roadmap status reports. Each forum provides an opportunity for knowledge sharing and coordination amongst CAMs, ASOC leadership, and OCIO PgMO.

OCIO always strives to provide multiple conduits for communication opportunities between OCIO Federal staff, contractors and assigned project managers. OCIO also meets weekly with the project leads for all contracts. Within 120 days of this final report, ASOC will provide planned accomplishments and timelines regarding this effort.

We shall continue to keep you posted of our progress on these recommendations.

If additional information is needed, please contact Denice A. Lotson, OCIO Audit Liaison, on telephone number (202) 720-9384.

Attachments

cc: Lennetta Elias, Program Analyst, OCFO (w/attachment)
Denice A. Lotson, Management Analyst (w/attachment)

Informational copies of this report have been distributed to:

Office of the Chief Information Officer
Attn: Agency Liaison Officer (3)

Government Accountability Office (1)

Office of Management and Budget (1)

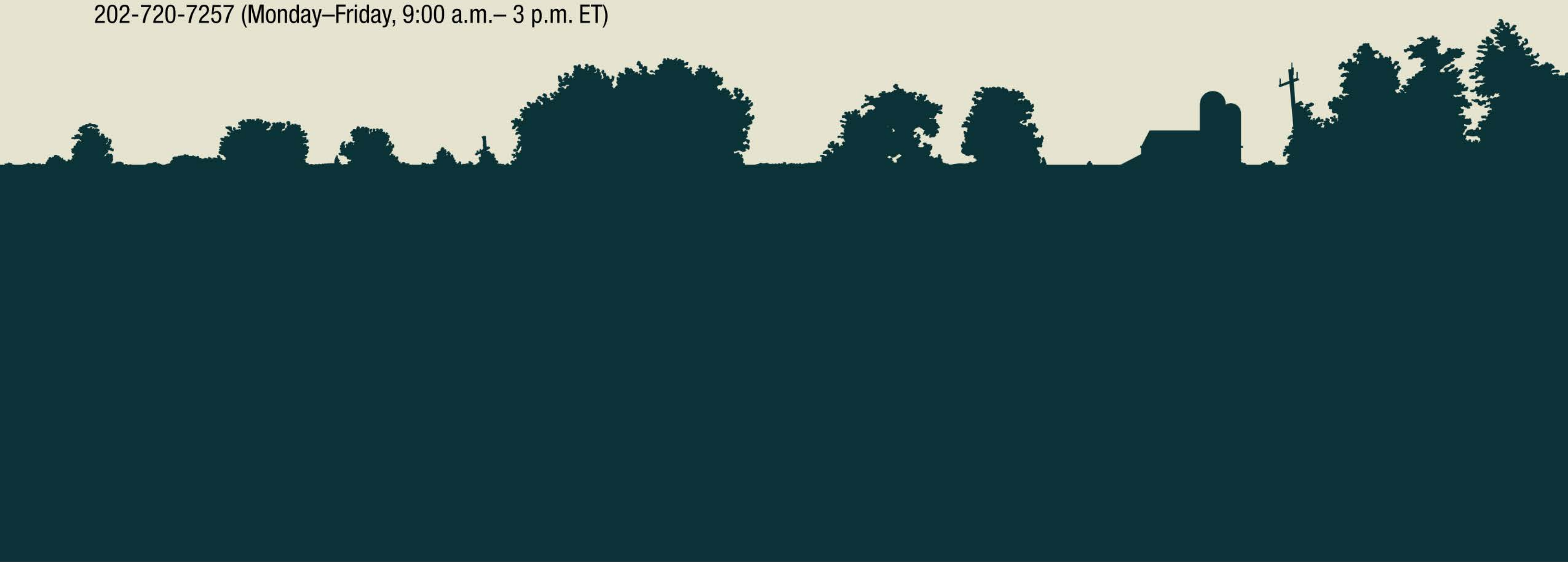
Office of the Chief Financial Officer
Attn: Director, Planning and Accountability Division (1)

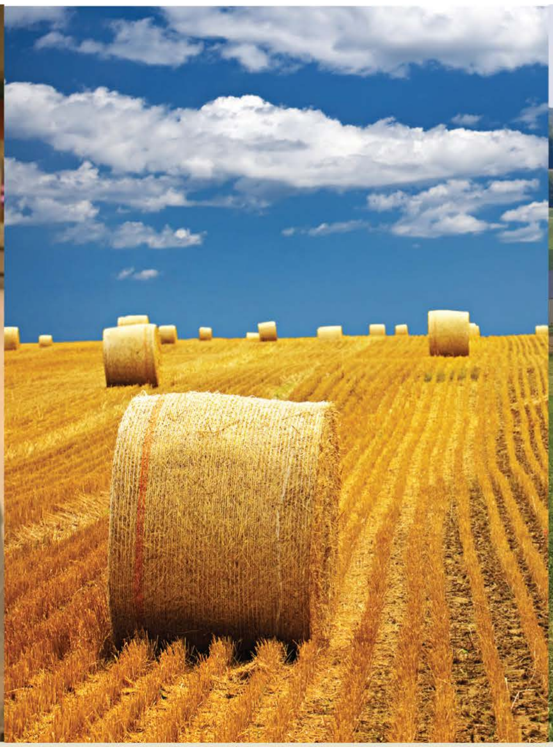
To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

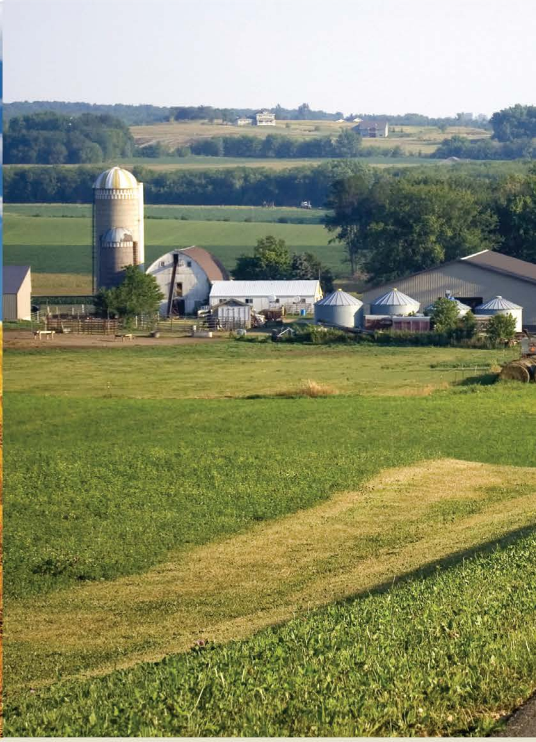
How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

Bribes or Gratuities
202-720-7257 (Monday–Friday, 9:00 a.m.– 3 p.m. ET)







The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD). USDA is an equal opportunity provider and employer.