2012 Explanatory Notes

Departmental Management

Office of the Chief Information Officer
Table of Contents

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Purpose Statement

The Clinger-Cohen Act of 1996 required the establishment of a Chief Information Officer (CIO) for all major Federal agencies. The Act requires USDA to maximize the value of information technology acquisitions to improve the efficiency and effectiveness of USDA programs. To meet the intent of the law and to provide a Departmental focus for information resources management issues, Secretary's Memorandum 1030-30, dated August 8, 1996, established the Office of the Chief Information Officer (OCIO). The CIO serves as the primary advisor to the Secretary on Information Technology (IT) issues. OCIO provides leadership for the Department's information and IT management activities in support of USDA program delivery.

OCIO is leading USDA's efforts to transform the Department's delivery of information, programs, and services by using integrated services that simplify citizens' interactions with their government. OCIO is designing the Department's Enterprise Architecture to efficiently support USDA's move toward consolidation and standardization. OCIO is strengthening USDA's Computer Security Program to mitigate threats to USDA's information and IT assets and to support the Department's Homeland Security efforts. OCIO continues to facilitate the USDA IT capital planning and investment control review process by providing guidance and support to the Department's Executive IT Investment Review Board, which approves all major technology investments to ensure that they efficiently and effectively support program delivery. More information about these investments and their Exhibit 300 capital planning documents can be found at: http://www.ocio.usda.gov/cpic/usda_cpic_material.html.

OCIO provides automated data processing (ADP) and wide-area network telecommunications services funded through the USDA Working Capital Fund and appropriations to all USDA agencies through the National Information Technology Center and the Telecommunications Services and Operations organization, with locations in Ft. Collins, Colorado; Kansas City, Missouri; and Washington, D.C. Direct ADP services are provided to the Office of the Secretary, Office of the General Counsel, Office of Communications, and Departmental Management.

OCIO also has direct management responsibility for the IT component of the Service Center Modernization Initiative through the International Technology Services. This includes the consolidated IT activities for the Farm Service Agency, the Natural Resources Conservation Service, and Rural Development mission area.

The OCIO Headquarters is located in Washington, D.C. As of September 30, 2010, there were 978 full-time permanent employees funded by appropriated, reimbursed, and Working Capital Funds.

Open Audits (During FY 2011):

Government Accountability Office Reports:

GAO-06-831 8/2006
Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation

GAO-08-525 6/2008
Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains

GAO-10-2 10/2009
Information Technology: Agencies Need to Improve the Implementation and Use of Earned Value Techniques to Help Manage Major System Acquisitions

GAO-10-202 3/2010
Federal Information Security Initiatives, FDCC/TIC/Einstein

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

GAO-10-42SU 11/2010
INFORMATION SECURITY: Federal Agencies Have Taken Steps to Secure Wireless Networks but Further Actions Can Mitigate Risk

GAO-10-701 7/2010
INFORMATION TECHNOLOGY: OMB's Dashboard Has Increased Transparency and Oversight, but Data Accuracy Improvement Needed

Office of Inspector General Reports:

50501-15-FM 11/2009
Fiscal Year 2009 Federal Information Security Management Act Report

50501-02-IT 11/2010
Fiscal Year 2010 Federal Information Security Management Act Report

Closed Audits (During FY 2010):

Government Accountability Office Reports:

GAO-8-925 7/2008
Information Technology: Agencies Need to Establish Comprehensive Policies to Address Changes to Projects' Cost, Schedule, and Performance Goals

GAO-10-237 3/2010
Information Security Concerted Effort Needed to Reduce and Secure Internet Connections at Federal Agencies

GAO-10-513 5/2010
INFORMATION SECURITY: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing

GAO-10-808 9/2010
Financial Management Systems: Migration of Agency Core Financial Systems to External Providers Varies as Government-wide Modernization Priorities Evolve

Office of Inspector General Reports:

88501-14-FM 9/2010
Statement on Auditing Standards No. 70 – National Information Technology Center General Controls Review

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Available Funds and Staff Years

2010 Actual and Estimated 2011 and 2012

Item	2010 Actual Amount	2010 Actual Staff Years	2011 Estimated Amount	2011 Estimated Staff Years	2012 Estimated Amount	2012 Estimated Staff Years
Salaries and Expenses.....	$61,161,667	79	$61,579,000	119	$63,579,000	119
Lapsing Balances.....	417,333	--	--	--	--	--
Total, Salaries and Expenses...	61,579,000	79	61,579,000	119 a/	63,579,000	119
Obligations under Other USDA appropriations:						
Reimbursements:						
Innovation & Operations Architecture.....	774,837	--	775,000	--	775,000	--
CSAM.....	400,000	--	400,000	--	400,000	--
CPIC.....	350,000	--	350,000	--	350,000	--
Geospatial IS.....	8,330,001	--	8,330,000	--	8,330,000	--
VTC.....	221,827	--	222,000	--	222,000	--
WCF Management Fee b/..	583,365	8	413,000	2	413,000	2
Project Management	120,000	--	120,000	--	120,000	--
NTIA Spectrum.....	1,595,861	--	1,600,000	--	1,600,000	--
Other Activities.....	217,720	--	218,000	--	218,000	--
Subtotal, Reimbursements.....	12,593,611	8	12,428,000	2	12,428,000	2
Working Capital Fund (WCF) c/						
Information Technology.....	400,251,904	855	387,143,000	933	389,555,000	943
NITC (Non-USDA).....	12,190,625	17	14,600,000	25	14,600,000	25
Capital Equipment.....	9,400,000	--	12,000,000	--	3,000,000	--
Subtotal, WCF.....	421,842,529	872	413,743,000	958	407,155,000	968
Total, OCIO.....	496,015,140	959	487,750,000	1,079	483,162,000	1,089

a/ This increase is for ASOC only. In FY 2010, ASOC activities were focused on procuring security tools and contractual services. In FY 2011, OCIO's staffing levels reflect an effort to Federally convert ASOC contractors to permanent positions.

b/ Management fee includes the salaries and benefits for two staff years, and 25 percent of the salaries and benefits for six Senior Executives.

c/ This section only includes WCF activities managed by OCIO. Please refer to the WCF Explanatory Notes for more details about the WCF.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Permanent Positions by Grade and Staff Year Summary

2010 Actual and Estimated 2011 and 2012 a/

	2010			2011			2012		
Grade	Wash DC	Field	Total	Wash DC	Field	Total	Wash DC	Field b/	Total
Senior Executive Service	6	--	6	6	--	6	6	--	6
GS-15	14	1	15	18	1	19	18	1	19
GS-14	22	3	25	44	8	52	44	8	52
GS-13	13	0	13	22	4	26	22	4	26
GS-12	7	1	8	12	1	13	12	1	13
GS-11	1	--	1	2	1	3	2	1	3
GS-10	1	--	1	--	--	--	--	--	--
GS-9	1	--	1	--	--	--	--	--	--
GS-8	1	1	2	--	--	--	--	--	--
GS-4	19	--	19	--	--	--	--	--	--
GS-3	7	--	7	--	--	--	--	--	--
GS-2	2	--	2	--	--	--	--	--	--
Total Permanent Positions	94	6	100	104	15	119	104	15	119
Unfilled Positions end-of-year	-21 c/	--	-21	--	--	--	--	--	--
Total, Permanent Full-Time Employment, end-of-year	73	6	79	104	15	119	104	15	119
Staff Year Estimate	73	6	79	104	15	119	104	15	119

a/ Positions shown are appropriated and reimbursement only. For WCF financed positions, refer to the WCF Explanatory Notes for more details

b/ Field employees are located in Kansas City, MO. Staffs work on all Security Incident Processing and Validation.

c/ Positions shown are reserved for the annual IT Summer Intern Program.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

SIZE, COMPOSITION AND COST OF MOTOR VEHICLE FLEET

The 2012 Budget Estimates propose no additional purchases or leases of vehicles.

OCIO-ITS is the in-house provider of information technology service and support for over 40,000 USDA Service Center Agency (SCA) employees and their network computers, IT equipment, and the shared infrastructure of the Common Computing Environment (CCE) that agency networks and applications run on. Our customers are FSA, NRCS, and RD and their respective partner organizations.

The current OCIO-ITS fleet consists of GSA leased vehicles and one agency owned vehicle. They are used by IT specialists and support teams to assist in keeping the computing environment operating to ensure that computers, applications, networks, and communication technologies do what they are suppose to do, allowing the agencies to support the efforts of the farmers, property owners, and rural communities. ITS uses its fleet to support best industry practices to organize IT resources and personnel efficiently and deploy them where and when they are needed. ITS fleet service is needed to allow its employees to travel to other SCA locations and to maintain a unified organization dedicated to supporting both the shared and diverse IT requirements of the SCAs and their partner organizations.

OCIO's current fleet is based on mission and geographic needs. As of December 2010, ITS has 223 leased GSA vehicles and one Agency owned vehicle and NITC has one leased GSA vehicle. Vehicles will continue to be leased from GSA. ITS continues to lease vehicles from GSA to provide IT support to the Service Center Agencies (SCA) within USDA. The SCAs consist of Farm Service Agency, Rural Development and the Natural Resources Conservation Service. ITS provides service to 40,000 people at 3,400 field, state, and headquarters offices located across all 50 U.S. States. ITS uses its fleet to support best industry practices to organize IT resources and personnel efficiently and deploy IT equipment where and when it is needed. ITS also use the fleet to address issues with malfunctioning IT equipment at these locations.

Changes to the motor vehicle fleet. No changes are proposed to the fleet for FY 2012.

Replacement of passenger motor vehicles. The GSA-leased vehicles are replaced based on the GSA regulations.

Impediments to managing the motor vehicle fleet. There are none at this time.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

Size, composition and cost of agency motor vehicle fleet as of September 30, 2010, are as follows:

Size, Composition, and Annual Cost
(in thousands of dollars)

	Number of Vehicles by Type								
Fiscal Year	Sedans and Station Wagons	Light Trucks, SUVs and Vans		Medium Duty Vehicles	Ambulances	Buses	Heavy Duty Vehicles	Total Number of Vehicles	Annual Operating Cost ($ in thous)
		4X2	4X4						
*FY 2009	120	90	10	0	0	0	0	220	$500
Change from 2009	-24	**+20	+9	0	0	0	0	+5	+ $495
FY 2010	96	110	19	0	0	0	0	225	***$995
Change from 2010	0	0	0	0	0	0	0	0	$0
FY 2011	96	110	19	0	0	0	0	225	$995
Change from 2011	0	0	0	0	0	0	0	0	0
FY 2012	96	110	19	0	0	0	0	225	$995

*ITS expanded its' fleet services in FY 2009 to support the SCAs.
** ITS requested and leased bigger vehicles to transport large IT and telecommunications equipments to multiple sites and locations.
***Please note that during FY 2009 vehicles were received from GSA at different times. Not all vehicles were used (billed) for the whole year. FY 2010 was first year that whole fleet was billed for full 12 months.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Appropriation Language

For the necessary expenses of the Office of the Chief Information Officer, $63,579,000.

Lead-off Tabular Statement

Annualized Continuing Resolution, 2011	$61,579,000
Budget Estimate, 2012	63,579,000
Change in Appropriation	+ 2,000,000

Summary of Increases and Decreases
(On basis of appropriation)

Item of Change	2011 Estimated	Program Changes	2012 Estimated
Office of the Chief Information Officer	$61,579,000	+$2,000,000	$63,579,000

Project Statement
(On basis of appropriation)

	2010 Actual		2011 Estimated		Increase or	2012 Estimated	
	Amount	Staff Years	Amount	Staff Years	Decrease	Amount	Staff Years
Chief Information Officer	$61,161,667	79	$61,579,000	119	+$2,000,000	$63,579,000	119
Unobligated Balance	+417,333	--	--	--	--	--	--
Total available or estimate	61,579,000	79	61,579,000	119	+2,000,000	63,579,000	119

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Justification of Increases and Decreases

(1) An increase of $2,000,000 for the Office of the Chief Information Officer consisting of:

a) An increase of $3,000,000 to expand the use of Enterprise Data Centers (EDD) (0 available in FY 2011). Funding is necessary to accelerate the migration of agency infrastructure and application to the USDA EDCs. Currently, there are ninety-seven data center/computer rooms in USDA. At the end of the consolidation, USDA will be operating on thirty-eight. This increase in funding will partially enable the EDC to upgrade existing facilities, implement technology refreshment, and provide resources to facilitate agency infrastructure and application migration activities. Through data center consolidations performed to date, USDA is achieving data center hosting efficiencies and economies of scale that will grow through further consolidation. The USDA Data Center Consolidation (DCC) plan will lead to significant reductions in data center build-outs through the use of server virtualization, cloud computing technologies and consolidation of data centers/data rooms. DCC will streamline IT operations, reduce costs and improve data security while reducing the associated energy costs and physical space allocations. This strategy aligns with the OMB DCC effort, the 25 Point Implementation Plan and industry best practices for consolidating IT hosting into larger, more robust data centers. This funding will be invested in the expansion of shared computing platform capacity and to support migration of Agency business applications where agency budgets are insufficient to absorb the costs.

USDA's OCIO, is committed to the Federal DCC Initiative and is poised to forge ahead with a plan to achieving significant reductions in data center build through the use of server virtualization and Cloud Computing technologies.

b) A decrease of $1,000,000 from Cyber Security activities to fund the EDC ($47,967,000 available for FY 2011).

The reduction in funding reflects the Agriculture Security Operation Center's shift away from the capital investment in security infrastructure to an ongoing program of analysis, incident response, and continuous monitoring. Funds were redirected from Cyber Security to the EDC.

Geographic Breakdown of Obligations and Staff Years
2010 Actual and Estimated 2011 and 2012

	2010		2011		2012	
	Amount	Staff Years	Amount	Staff Years	Amount	Staff Years
District of Columbia	$59,681,233	73	$58,600,000	104	$60,600,000	104
Kansas City, MO	1,063,101	6	2,979,000	15	2,979,000	15
Subtotal, Available or Estimate...	61,161,667	79	61,579,000	119	63,579,000	119
Unobligated balance	417,333	--	--	--	--	--
Total, Available or Estimate	61,579,000	79	61,579,000	119	63,579,000	119

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects

2010 Actual Estimated 2011 and 2012

		2010	2011	2012
Personnel Compensation:				
Washington, D.C.		$7,761,861	$8,928,000	$8,979,000
Kansas City, MO....		668,436	1,720,000	1,725,000
11	Total personnel compensation	8,430,297	10,648,000	10,704,000
12	Personnel benefits	1,912,165	2,684,000	2,703,000
13	Payments to prior employees	125,420	--	--
	Total personnel comp. & benefits	10,467,882	13,322,000	13,407,000
Other Objects:				
21	Travel	301,574	310,000	310,000
22	Transportation of things	2,180	3,000	3,000
23.3	Communications, utilities, and misc. charges	925,750	1,000,000	1,000,000
24.0	Printing and Reproduction	60,370	61,000	61,000
25.2	Training	99,197	100,000	100,000
25.2	Other services	16,640,462	14,860,000	16,785,000
25.3	Purchases of goods and services from Government Accounts	29,536,315	28,413,000	28,413,000
26	Supplies and materials	1,956,853	2,000,000	2,000,000
31	Equipment	1,171,046	1,500,000	1,500,000
43	Interest and Dividends	8	0	0
	Total other objects	50,693,785	48,257,000	50,172,000
Total direct obligations		61,161,667	61,579,000	63,579,000
Position Data:				
Average Salary, ES positions		$160,182	$177,182	$177,761
Average Salary, GS positions		$89,033	$100,904	$100,904
Average Grade, GS positions		13.1	13.5	13.5

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

STATUS OF PROGRAM

The Clinger-Cohen Act of 1996 required the establishment of a Chief Information Officer (CIO) for all major Federal agencies. The Act required USDA to maximize the value of information technology acquisitions to improve the efficiency and effectiveness of USDA programs. To meet the intent of the law and to provide a Departmental focus for information resources management issues, Secretary's Memorandum 1030-30, dated August 8, 1996, established the Office of the Chief Information Officer (OCIO). The CIO serves as the primary advisor to the Secretary on Information Technology (IT) issues. OCIO provides leadership for the Department's information and IT management activities in support of USDA program delivery.

Current Activities:

Expanding Electronic Government:

USDA Initiatives: Progress made in recent years allows USDA to continue its Department-wide approach to delivering shared services. USDA's shared services are described in the USDA IT Strategic Plan. A copy of the plan is available at http://www.ocio.usda.gov/n_USDA_IT_Strategic_Plan.pdf. Participation in these services is strong, with USDA agencies actively involved in the Enterprise-wide shared services (USDA's eAuthentication Service, AgLearn, and the common infrastructure provided through USDA's Enterprise Shared Services, Enterprise Correspondence Management Modules, the Enterprise Architecture Repository (EAR), and capital planning investment tools). For example, there are over 127,865 active AgLearn accounts across USDA, and in FY 2010 users completed 508,789 courses. USDA eAuthentication Service protects 381 Web-based applications that require single factor (userid/password) authentication and provides the option to authenticate using the USDA LincPass card. In FY 2010, OCIO began implementing an enterprise Web content and document management service using Site Studio technology. All USDA agencies will also migrate to version 6.1 of the IBM Websphere Portal, which is capable of seamlessly integrating with a Departmental social networking solution.

USDA Participation in E-Government Initiatives: USDA participates in 31 E-Government Initiatives and Lines of Business (LoB). USDA is also an active participant in the development of a Government-wide infrastructure to support Homeland Security Presidential Directive 12 (HSPD-12) and is also making significant progress implementing continuity of operations communications capabilities to meet the requirements of the National Communications System Directive 3-10 (NCSD 3-10). USDA will provide an estimated $11,125,353 to support 8 E-Government Initiatives and 5 LoBs in FY 2011. By participating in the E-Government Initiatives and LoBs, USDA has improved its business processes and program delivery to its customers, employees, and partners. Through these efforts, USDA has been able to work with other Federal agencies to streamline common areas of business delivery (e.g. rulemaking, payroll, and grants management) and learn from best practices throughout the Government. The Department will continue to implement these Initiatives and LoBs to achieve further benefits for its customers.

Presidential E-Government Initiatives and Lines of Business

Presidential E-Government Initiatives and Lines of Business		
1. Budget Formulation and Execution LoB	12. E-Rulemaking	22. Human Resources Management LoB
2. Business Gateway	13. E-Training	23. Information Systems Security (ISS) LoB
3. Disaster Assistance Improvement Plan	14. Federal Asset Sales	24. Integrated Acquisitions Environment (IAE)
4. Disaster Management	15. Federal Health Architecture LoB	25. Integrated Acquisitions Environment (IAE) – Loans and Grants
5. E-Authentication	16. Financial Management LoB	26. International Trade Process Streamlining (ITPS)
6. E-Clearance	17. Geospatial LoB	27. IT Infrastructure Optimization LoB
7. E-Government Travel	18. Geospatial One-Stop	28. Recreation One-Stop
8. E-Loans	19. GovBenefits.gov	29. Recruitment One-Stop
9. Enterprise Human Resources Integration (EHRI)	20. Grants.gov	30. SAFECOM
10. E-Payroll	21. Grants Management LoB	31. USA Services
11. E-Records Management		

Enterprise Architecture: The USDA Enterprise Architecture (EA) Program is a collaborative effort between OCIO, USDA agencies, and supporting EA communities through membership, and active participation. USDA business requirements are driving towards cross-agency solutions that are standards based and interoperable. Interoperability objectives increase the need for change and standardization across technology architecture domains. OCIO has partnered with The Gartner Consulting Group to develop a technology architecture guidebook with USDA Department-wide technology standards. The technology standards have been defined in a form that leverages illustrations "Patterns" to clearly communicate how technologies should be developed to deliver capabilities to USDA users and systems; emphasize the intended target state to enable tactical decision making; allow varying degrees of cross-Agency standardization; address lifecycle of technology standards from emerging to retirement; and is easy to maintain and adjust over time as business needs and technology capabilities change. Based on the Federal Enterprise Architecture Reference Models, USDA developed a current architecture, target architecture, and transition plan. USDA's Department-wide EA effort provides a "corporate" view of an EA, and builds on the architectures already under development within USDA's agencies. At the center of the USDA EA knowledge base is the Enterprise Architecture Repository (EAR) -- a Web-based knowledge repository solution that provides executives, managers, staff, and authorized contractors a place to design, capture, view, and collaborate on the information that defines the USDA enterprise architecture. This system can be aligned with other knowledge repositories based on common key data points. It also enables the creation of value-added reports, the sharing of key information, the development and storage of models, and other important functions.

Primary users of the USDA EA include strategic planners, enterprise architects, business process owners, program managers, project managers, vendors, budget officers, investment decision-makers, acquisition personnel, developers, and security personnel.

The FY 2011 EA activities include:

- Development of the USDA technology standards (Bricks and Patterns);
- Participation in Open Government and Data.Gov Initiatives;
- Continue to update the EA Program Plan based on Value Measurement Survey results and independent third party assessment results of USDA EA program;
- Continue development of executive and management reports and dashboards;

- Continue the enhancement of data quality through the development and implementation of data entry templates;
- Update and initiation of EA Guiding Principles;
- Creation and incorporation of EA Governance into IT Governance; and
- Initiation of a Security Architecture Blueprint.

Capital Planning and Investment Control (CPIC): OCIO is responsible for ensuring that the Department's IT investments deliver products that result in an effective and efficient set of business benefits to agencies. The outcome of this work is oriented around the assurance of a positive return on the investment in IT for taxpayers. To accomplish this goal, USDA established the CPIC Program in 1997 for selecting, managing, and evaluating the results for all major IT investments. The Department's Enterprise IT Governance process will serve as the USDA senior authoritative body charged with the oversight of all investments categorized as "major," according to OMB protocol. Capital planning requirements for investments that are not considered in the "major" category are managed by the OCIO Capital Planning Division, under the guidance of the Information and Technology Management unit, with consideration to Government "best practices," as well as OMB Federal Acquisition Regulation and USDA official guidance.

CPIC is used to evaluate investments with the end goal of selection based on a high probability of long-term success. Investments are assessed based on their ability to:

- Effectively meet mission needs;
- Provide a favorable profile by evaluating alternatives using cost/benefit/return calculations;
- Meet security mandates, as well as commonly accepted standards;
- Manage the use of telecommunications technologies and resources;
- Conform to Federal EA standards applied within the Department;
- Manage the risks of the investment lifecycle; and
- Comply with Federal mandates (GAO, OMB, etc.) to include appropriate guidance.

The CPIC Program uses a core set of information that permits evaluations across different investments as well as focusing agency attention on factors that bear on their investments and their management of IT resources. This, combined with the supplemental data provided through the use of standard project management techniques within the agencies allows for the OCIO to aid in organizational strategic planning aimed at the long-term effective use of IT to maximize the return to the U.S. citizen.

The key focus in FY 2011 is the Enterprise IT Governance process. This is critically important to maturing the overall management of IT across USDA. OCIO places significant focus on the use of EA, the quality of business cases, supporting project management documentation, and the use of earned value management (EVM) discipline to manage investments.

IT Acquisition Approval Review (AAR) Process: The IT acquisition approval process is an OCIO control activity that involves a technical review of USDA IT acquisitions for $25,000 and above for conformity with USDA, Federal Enterprise Architecture, USDA telecommunications standards and practices, IT security considerations, and IT investment supporting documentation. The CIO is the final approval authority on all acquisition approval requests. The OCIO works with agencies to ensure that approved IT acquisition requests provide the necessary information, as part of the Enterprise IT Governance process for managing the USDA IT portfolio of major and non-major investments.

Cyber Security: OCIO continues to implement its aggressive strategy to improve USDA's information security via: 1) training; 2) establishing standardized computer security policies, processes and controls within the Department; and 3) identifying and pursuing funding for various initiatives designed to improve Department security. The OCIO Cyber Policy and Oversight (CPO) and Agriculture Security Operations Center (ASOC) continued to focus our activities on the transformation and improvement of our Security-related services. CPO continued to align with security best practices, Federal laws and oversight requirements. For example, USDA participated in two Office of Management and Budget (OMB) Information Systems Security Lines of Business (LoB) such as the 1) Federal Information Security

Management Act (FISMA) Reporting Portal and 2) Security Awareness Training. USDA will continue leveraging these partnerships to improve our security operations and service offerings. USDA will also expand current security operations and compliance processes in the transition to Continuous Monitoring, to provide real-time monitoring and data feeds regarding IT systems, hardware, inventories, and other security-related statuses.

The OCIO continues aggressive implementation of its 36-month information security "get healthy" plan (developed in FY 2010), in coordination with the Department of Homeland Security (DHS) and other security leaders in the public and private sector. OCIO also launched the "Getting to FISMA Green" program consisting of 10 initiatives to improve FISMA compliance across the Department. In FY 2010, OCIO successfully implemented three major security initiatives: 1) network base lining; 2) procuring and deploying additional security tools; and 3) establishing the Agriculture Security Operations Center. In addition to continuing with initiatives begun in FY 2010, in FY 2011 the OCIO will address several additional initiatives of the "get healthy" plan including the: 1) Governance; Compliance and Risk Management Program – implementing Continuous Monitoring strategies and activities including Plan of Actions and Milestones program improvements; 2) Incident Response and secure systems configurations; and 3) Contingency Planning/Continuity of Operations program improvements.

Systems Certification and Accreditation: In FY 2010, USDA's aggressive strategy for Certifying and Accrediting (C&A) USDA's information systems included the implementation of its Center of Excellence (COE) for the C&A program. The mission of the USDA's COE is to provide agencies with operational support and tools to improve the USDA C&A process, including the conduct of concurrency reviews, development and management of Plans of Action and Milestones (POA&Ms), administration of the USDA's Federal Information Security Management Act (FISMA) activities, use of the Cyber Security Assessment and Management (CSAM) tool, and dissemination of security information to ensure that USDA is in full conformance with all National Institute of Standards and Technology (NIST), FISMA, Office of Management and Budget (OMB) and USDA security polices and requirements. The COE will evaluate the risks, costs, mitigation strategies, and consequences of lapses in security, and will guide USDA to economically viable investments in security projects and tools. The COE will accomplish its mission through an integrated and cooperative approach with all USDA entities who have responsibility for protecting USDA's information assets.

OCIO continues its use of the CSAM, the Department of Justice's LoB for the FISMA reporting tool, to support its C&A process and in conjunction with OCFO, has implemented a process to minimize duplication of testing controls while simultaneously improving the quality and effectiveness of testing. In FY 2011, USDA will transition to CSAM version 3 and incorporate NIST SP 800-53 Rev. 3 security controls into it Risk Management Framework activities.

Information Survivability: One essential goal of USDA's computer security program is to develop recovery strategies to minimize disruptions in the event of a catastrophic interruption. To achieve this objective, OCIO is leading the development and deployment of disaster recovery and business resumption plans for all USDA IT Systems. These plans, as well as the other plans required for a viable Continuity of Operations Program (COOP) are maintained in CSAM. OCIO is currently working to improve the policy, guidance, templates, and training on information survivability.

The OCIO participated in and provided guidance and leadership in the COOP Eagle Horizon 2010 exercise which crossed multiple Government agencies/departments including all preparatory work done before the exercise. OCIO acted as a trusted agent in the development of the briefing book guidance to the Secretary and senior staff, gave presentations to senior OCIO staff before the exercise, gave a presentation on Cyber Security to all Critical Action Team (CAT) members at the Employee Relocation Facility (ERF) before the exercise, prepared alternate locations to receive key OCIO personnel , identified and updated vital records, prepared detailed briefing books for OCIO leadership to use during the exercise, and created a detailed after action plan identifying areas to improve upon. The OCIO also led the effort to find other potential ERF locations for USDA.

Agriculture Security Operations Center

As part of the USDA's information security "get healthy" plan, in FY 2010, OCIO established the ASOC. The ASOC is operational and has taken responsibility for the ongoing enterprise security operations functions of USDA.

- Security Monitoring and Analysis: The ASOC's Monitoring and Analysis Division (MAD) will provide operational support and continuous monitoring and analysis of the USDA backbone and USDA agency networks from a central enterprise perspective. MAD will monitor, collect and analyze key data to identify patterns that indicate exploitation of vulnerabilities, intrusions, and malicious activities. MAD will provide near-real-time analytical support of incident handling activities using tools, sensors, and security-collection and analysis systems. Priorities have been established to provide continuous 24/7 monitoring, detection, and alerting capabilities which in turn will enhance the overall assessment capability of USDA to cyber-security threats.

  Additionally, ASOC will actively participate as the Department's representative in the National Cyber Security Center and Department of Homeland Security initiatives and collaborate, as necessary, with the United States Computer Emergency Readiness Team (US-CERT); Joint Task Force-Global Network Operations; National Cyber Investigative Joint Task Force; Intelligence Community-Incident Response Center; National Security Agency Threat Operations Center, and Defense Cyber Crime Center.

Secure Communications: USDA has removed the Department of Defense Secret Internet Protocol Router Network (SIPRNET) and transferred all users to the DHS Homeland Security Data Network (HSDN). USDA is actively procuring and installing secure communications in support of the National Communications System Directive (NCSD) 3-10, *Minimum Requirements for Continuity Communications Capabilities*, at the Headquarters Facility, the Alternate Operating Facility, and the Devolution Facility. This will allow USDA to perform its National Essential Functions before, during, and in the aftermath of an emergency.

Enhanced Incident Handling Program: USDA is focusing on improving the USDA Incident Handling program. This program includes the implementation of USDA Incident Handling Best Practices and Guides, integrated Department and Agency Incident Response Plans (Per OMB and FISMA Requirements), and modernization of the USDA Incident Handling policies and standards. These efforts target improvements to the Department's situational awareness through collaboration and communication within the USDA, US-CERT, and other Government Agencies.

Intrusion Detection: USDA is currently deploying a comprehensive and cohesive integrated security solution called the Security Stack and Console (SSC) that will provide a foundation for enterprise wide security monitoring, detection, and protection in USDA. Detection and response time for incidents will be shortened to hours. The SSC is designed and built to perform a mix of critical security functions in near-real-time, including intrusion detection and prevention, network data loss prevention, network behavior analysis, secure socket layer encryption/decryption, malware detection and prevention, and network packet analysis. The SSC's deployment plan consists of a phased rollout of twelve sites that follow detailed, well-defined procedural steps for installation, configuration, and implementation. As of the end of December, 2010, deployment has been completed at seven of the sites.

Contracting Agreements: USDA has used its collective buying power to establish a number of enterprise agreements for IT hardware, software and services that support the USDA enterprise. OCIO has led these efforts by identifying products and services that many USDA agencies had already purchased, consolidated funding and worked with procurement to negotiate a lower price for items that were already being used throughout USDA. These new contracts including consolidated email have and will continue to result in hundreds of thousands of dollars per year in savings across the USDA.

Enterprise Data Centers: USDA released its Enterprise Data Centers and Critical Systems memo on January 4, 2008, requiring critical IT to be hosted in the Department's Enterprise Data Centers. These

critical information technology solutions include mission critical systems, mixed-financial systems, disaster support systems, incident response systems, and information systems that handle privacy, sensitive and personally identifiable information (PII). This effort is ongoing moving from the planning stage to full implementation.

The National Information Technology Center (NITC) is working with the following agencies on some key Enterprise Data Center migration initiatives:

- Foreign Agricultural Service (FAS)
- Food Safety and Inspection Service (FSIS)
- Agricultural Marketing Service (AMS)
- Food and Nutrition Service (FNS)
- Risk Management Agency (RMA)
- Grain Inspection, Packers and Stockyards Administration (GIPSA)
- National Agricultural Statistics Service (NASS)
- Animal and Plant Health Inspection Service (APHIS)
- Forest Service (FS)
- Economic Research Service (ERS)
- Office of Inspector General (OIG)
- National Institute of Food and Agriculture (NIFA)
- Office of the General Counsel (OGC)

Platform as a Service: Platform as a Service (PaaS), formally known as Software as a Service and Enterprise Shared Services, is a suite of tools, standards, and business applications that facilitate USDA's Department-wide effort to deliver citizen-centric, online information and services. These services utilize Government and industry standards and best practices. USDA developed these shared services with the goal of maximizing efficiency, reducing cost, and improving customer service. Beginning in FY 2011, these services were unbundled and will be a combination of fee-for-service and Core charges for the customers. The move toward 100 percent fee-for-service model will be implemented as soon as possible. As of FY 2010, there were 144 agency applications in production, with an additional 21 applications planned throughout FY 2011.

E-Authentication: The Identity and Access Management program is composed of eAuthentication and the HSPD-12 Personal Identity Verification Service. E-Authentication is a public-private partnership that enables citizens, businesses, and Government employees to access online Government services using credentials issued by trusted third-parties, both within and outside the Government. Once an agency's system has been enabled to accept eAuthentication credentials, it is able to grant access to end users who have an identity credential from one or more of the E-Authentication Federation's Credential Service Providers (CSPs). USDA's eAuthentication Service was the first General Services Administration approved authentication and authorization service, Government-wide CSP, which enables USDA to provide Level 2 credentials to employees, customers, and partners. A Level 2 credential provides a higher degree of confidence to ensure that the customer accessing an application on the USDA Web is an authentic and authorized customer.

Identity, Credential, and Access Management (ICAM) in USDA: HSPD-12 ushered in a new era of identity assurance, making it more important than ever that Federal Departments manage identity, credentials, and access to its resources. USDA is already a leader in this area, developing systems and processes to get HSPD-12 PIV (LincPass) cards issued to its staff, over 90,000 to date. USDA continues to lead the way for credential utilization beyond simple assertion of authorization. On November 10, 2009, OMB issued the Federal Identity, Credential, and Access Management (FICAM) roadmap and implementation guidance. The FICAM document establishes a common framework and implementation guide to plan and execute ICAM programs within the Federal Government. Most importantly, the FICAM document issued a *Call to Action* for Federal Departments to take ownership of ICAM concepts necessary to achieve overall success of the Federal cyber security, physical security, and electronic Government (eGov) visions. Recognizing the ongoing need for ICAM, USDA has developed permanent, cross-

functional ICAM teams for its 29 agencies, offices, and institutes. These teams are deeply involved in re-engineering business processes that leverage the PIV card for HR functions, remote access, telework initiatives, and emergency response. USDA has also successfully completed the initial phase of its Enterprise Entitlement Management Service (EEMS), which when fully implemented, will leverage the LincPass for identity federation with other Federal Departments, enable automated role entitlements to reduce costs and improve security controls, and serve as a platform for future enterprise projects that rely on knowing both who their users are and their various relationships to the organization.

Enterprise VPN for Remote Access: In the past, USDA had a variety of virtual private network (VPN) solutions for granting remote access by users to USDA networks. Each solution had different access methods and limitations, resource needs, and capabilities. Helpdesks had to manage an increasing number of procedures for supporting these solutions, and most systems were already at capacity for the number of simultaneous users. The near-miss H1N1 pandemic pointed out the infeasibility of using these disparate systems for meaningful pandemic response. The solution was to design and implement the Enterprise VPN. Managed at the highest enterprise level, and with significantly larger capacity, the Enterprise VPN was already a material improvement in enabling remote access. Most importantly, however, the Enterprise VPN uses the HSPD-12 LincPass for access control, resulting in no additional costs for yet another pool of identities, and increasing USDA's return on investment for its PIV card implementation.

eAuthentication/LincPass Single Sign-on: USDA's eAuthentication service provides authenticated Level 2 access for both internal users (employees, contractors, affiliates, et al) and external users (USDA customers) to a steadily growing list of Web-based applications (381 as of October 2010). It is used by approximately 104,000 employees on a daily basis to access administrative and mission critical applications such as HR systems, GovTrip, and financial systems. In September 2010, the eAuthentication system handled approximately 7.4 million login validation events. Previously, each of those meant the employee entered an eAuthentication ID and password to gain access. Now, thanks to the successful integration of eAuthentication and the HSPD-12 system, USDA employees can use their LincPass to log in to eAuthentication-protected Web applications. This not only reduces the number of credentials that employees have to remember, but it saves a few seconds with each login event. This may not be much per individual, but multiplied by the number of login events, the eAuthentication-LincPass single sign-on project will save approximately 140 person hours per week across USDA in the first few months alone.

Key eAuthentication FY 2011 Activities include:

- Continue agency Web application integrations;
- Continue 99.99 percent system availability and reliability;
- Continue ensuring security incidents are handled in an expedient manner;
- Complete processing changes to accommodate the National Finance Center's Person Model Implementation;
- Implement Sharepoint;
- Eliminate the use and storage of Social Security numbers, where possible; and
- Customize login and help pages for mobile access

Digital Signatures Using the LincPass: Because USDA's LincPass (HSPD-12 PIV card) is tied to a known identity in a centralized and trusted system (meaning it's based on accepted standards of assurance), it provides reasonable assurance of the cardholder's identity. USDA developed and implemented procedures for using the card to digitally sign documents (e.g., Word documents and PDFs), files (e.g., spreadsheets), and emails. Digital signatures are a type of electronic signature that is non-repudiable, offering reasonable assurance that it was the person signing, and the file/record/ transaction is unchanged from when it was signed. Using digital signatures is helping USDA move from a paper-based workflow to an electronic workflow, resulting in simplifying, streamlining, and speeding up of processes, and improved security and assurance for each step in the process. Expanded digital signature use in USDA is expected to address a variety of NIST audit and accountability controls, as well as protection of communications.

Enterprise-Class Video Teleconferencing: USDA analyzed the costs and benefits for using video-teleconferencing (VTC) in USDA to reduce travel expenses, increase collaboration, and reduce USDA's carbon footprint. To that end, USDA designed, architected, and implemented a centralized, enterprise-class VTC infrastructure. The additional benefits are significant:

- Reduced or eliminated redundant architecture and equipment purchases.
- Standardized connectivity and equipment improved ease of use (and therefore utilization) and reduced helpdesk support and maintenance costs.
- Security, access control, and monitoring are done from a central location, and invisible to the end user.
- Consolidated equipment purchases have achieved significant cost savings.

Enterprise Geospatial Management Office: The USDA Enterprise Geospatial Management Office (EGMO) ensures the agriculture spatial data assets and lifecycle are effectively managed and optimized, and Geographic Information Systems (GIS) services have the capacity to address current and future policy and public administration business requirements. Through enterprise-level collaborative strategic planning, geospatial portfolio investment, innovation projects, and governance with USDA agencies, the EGMO provides coordinated leadership to extend best practices and generate cost savings and avoidance.

To achieve these outcomes, and provide a sustainable structure for geographic solutions value-creation, accountability, transparency, and stakeholder participation, three core performance goals are established in FY2011:

- Develop and disseminate a USDA Department Geospatial Strategy to establish direction, building continuity, align resources, and communicate performance measures supporting the USDA mission.
- Create and publish a Geospatial Data Asset Management Policy to include guidance regarding data and services, metadata, and Enterprise Data Center migration.
- Launch tactical partnership between EGMO and Ft.Collins OCIO Application Development teams for GIS development, testing, research, invention, etc., to support place-based policy, planning, and programming through rapid deployment spatial analytic capabilities, competencies, and agency capacity building

Selected Examples of Recent Progress:

Operational Security Assessments: The Agriculture Security Operations Center conducts operational security assessments of USDA agencies and staff offices to evaluate an organization's detection and defense methods against a combination of guidelines, many published by NIST, the DoD and Intelligence Community, and industry best practices and standards. This security assessment goes beyond a checklist mentality to assess networks in terms of operational security effectiveness and efficiency. The assessment provides agencies with real, actionable intelligence to assist in defending their mission critical information and assets from current and future cyber-attacks. ASOC completed or initiated 11 agency assessments by the end of FY 2010, and is on track to complete 11 agency assessments in FY 2011. The 11 agency assessments in FY 2010 represent USDA networks carrying 80 percent or more of the Department's total network traffic.

Incident Handling Program: In FY 2010, the ASOC responded to 75 percent more incidents in the first four months as compared to the same timeframe in FY 2009. Previous to 2010 this was handled by Cyber Policy and Oversight. This higher incident rate is an indication that USDA is evolving to a more mature and proactive stance regarding security monitoring and incident handling.

Throughout 2010, the ASOC reached out to multiple Federal and DOD agencies to evaluate their best practices and lessons learned. Based on this information and internal program analysis, USDA made significant revisions to existing Computer Incident Response Team (CIRT) procedures. These changes reflect actual operational processes and improved the quality of services and communications throughout the incident lifecycle. This continuous process ensures the CIRT Incident Handling procedures are repeatable and sustainable.

The ASOC implemented changes to the operational model, program support and case management system to support the Incident Handling Program. Collectively, these efforts led to significant decreases of incident resolution times, more accurate reporting, and improved incident management. In 2nd Qtr FY 2010, ASOC implemented the first series of changes to the Incident Handling and Escalation procedures. These changes were in conjunction with ASOC's transition to the custom Remedy ticketing system. This led to a 9.9 percent decrease in the average incident age compared to 2009. In the last QTR FY 2010, ASOC completed the second series of improvements that included realignment of program priorities and technical execution, a new contractor support team, and implementation of incident validation processes and quality standards for reporting. These improvements have led to a further decline in the average age of an incident by 8.9 percent compared to 2009.

End-Point Security: ASOC provided oversight in the implementation of the USDA enterprise end-point security tool to over 130,000 laptops, desktops and servers. The end-point security tool is currently supporting real-time continuous asset tracking and provides inventory and health status data. This tool also provides USDA with greater visibility towards compliance with the Federal Desktop Core Configuration (FDCC). ASOC is also in the process of implementing Security Management Sensors and Consoles. The sensor tool when fully implemented will better protect the USDA network and provide situational data into a common operating picture to further standardize the overall USDA security posture. The security tools taken as a whole will enable quicker and more comprehensive response to security threats and vulnerabilities.

Security Awareness and Training: USDA has an aggressive security awareness program that uses the ISS LoB for security awareness training as its foundation. This program is supplemented with "live" town-hall security awareness training sessions, expanded Agency outreach, and an active communications strategy that notifies individuals of the requirement to take the training. This year, USDA also hosted the Cyber Security Summit and Cyber security Speaker's Series to increase awareness of Cyber security best practices and the Federal Government strategic direction for Cyber security. For FY 2010, over 99 percent of Agriculture personnel received security awareness and specialized security training.

Updated Incident Handling Procedures: Cyber Security has updated its Security Computer Incident Response Team (CIRT) Standard Operating Procedure (SOP) several times this fiscal year in response to incidents and changes to the incident handling process. The USDA CIRT SOP was modified in the third quarter of FY 2008 to include checklists; additional/revised PII information on forms and checklists; updated workflow diagrams and decision trees; and additional phishing and SPAM guidance.

Contracting Agreements: The USDA is in the process of consolidating the more than 21 different agency email systems into a single consolidated system. This solution will provide all USDA with a single address book, the ability to schedule meeting across agencies, ediscovery tools, access to collaboration tools such as SharePoint, Video conferencing and archiving.

Communications and Security: The OCIO has begun to deploy an emergency notification system called MIR3 Department wide. This solution will provide the ability to notify users through multiple devices including email, cell phone, home phone and text devices. Standardizing on a single platform will save the USDA thousands of dollars and improve overall communications and security.

E-Authentication: Following represents progress with this initiative:

- As of 2010, 381 agency Web applications have integrated with eAuthorization with 99 more integration efforts in various process stages.
- More than 102,000 employees and approximately 424,000 customers owned an eAuthentication credential in a typical month in FY 2010.
- In an average month in FY 2010, USDA eAuthentication Service customers used their credentials for nearly 3,800,000 authentications of personal identity and over 84,000,000 Web site authorizations for access to protected content.

Enterprise Entitlement Management System: To improve access controls, USDA is implementing an Enterprise Identity, Credential and Access Management (ICAM) program. As part of that effort, the Enterprise Entitlement Management System (EEMS) provides a set of integrated tools to manage the identity, entitlements, and roles for all of USDA computer users, including an Identity Management system, an Enterprise directory, provisioning and workflow engines, and an auditing and reporting application. USDA must implement a strong access control environment to address its control issues surrounding access to its mission critical systems and data, protect confidential personal and business information from unauthorized access, and meet FISMA and OMB Circular A-123 requirements.

EEMS is divided into the following sub-projects:

- Core Infrastructure Deployment – deployment of the base infrastructure;
- Business Process Modernization – development of use cases to reflect best practices and compliance needs based on A-123 and FISMA;
- Business Integration – coordination with the Agencies and Staff Offices to deploy business processes and EEMS tools;
- Application Integrations – coordination and development of application connectors, such as AgLearn and HSPD-12, to EEMS; and
- Operations and Maintenance – operating and maintaining the completed infrastructure and integrations.

ICAM and EEMS reduce the business risk exposure of USDA networks and data, and represent an enterprise-wide vision for securing our technical infrastructure and business applications, as well as protecting the rights of individuals. EEMS leverages USDA existing C&A commercial software investment to provide the critical entitlement management layer and will deliver long term benefits to the USDA, including 1) improving the speed, and efficiency, and accuracy of identity management; 2) increased security posture; 3) cost savings reduction of unneeded manual processes; 4) increased application stability and administration; 5) compliance management (A-123 & FISMA); and 6) auditing and reporting. During Fiscal Year 2010, USDA completed deploying several CA tools, including an Enterprise Directory, Identity Manager and data synchronization tool. USDA successfully integrated the new Enterprise remote access application with EEMS and established roles for the agency pilots. Two applications (AgLearn and eAuth) completed role engineering analyses to improve their role models for integration with EEMS. A pilot was started to begin addressing privileged access controls. USDA with its' agencies has developed a variety of use cases to identify standard processes for access management throughout the Department. The USDA program team began collaborating with the Agencies to deploy ICAM teams. These teams will be used to communicate what the Department has started and the impact to the Agencies.

E-Training and AgLearn/other EGov Initiatives: Refer to the EGovernment Status of Program found on pages 8g-28 and 8g-29.

Systems Certification and Accreditation: USDA continued its efforts toward improving its C&A process. In FY 2010, OCIO improved the quality of the C&A documentation submitted to identify and correct root causes of non-compliance. Reviewers worked with agencies individually to improve agency C&A documentation and mitigate weaknesses. Plans of Action and Milestones (POA&M) were established to address non-critical deficiencies noted in concurrency reviews. In addition to the C&A COE, OCIO leveraged C&A Tiger Teams to work with Agencies across the Department to improve C&A artifacts and controls testing, provide training, and streamline the C&A process by reducing inefficiencies in the current process.

Information Survivability: In FY 2010, OCIO continued its efforts to improve information survivability by providing a centralized storage capability for disaster recovery plans.

Information Technology Governance: OCIO is engaged in an ongoing effort to establish, maintain and support an integrated IT governance and decision-making environment. This integrated IT Governance process, when completely implemented, will provide a dynamic means of capturing, retaining, and presenting IT investment information so that the CIO has the necessary tools to carry out legislated mandates. For the security aspects of this area, in FY 2010, OCIO established it's Governance, Risk, and Compliance (GRC) program for Cybersecurity, creating GRC strategic plans, metrics, and templates for C&A tracking to build the framework and deployment strategy for the GRC program. Ultimately, the governance process is intended to ensure that all IT investments support the Departmental and agency mission, particularly in terms of the services provided to citizens, and contribute to the USDA's enterprise-wide IT infrastructure.

Enterprise Architecture (EA): In FY 2010, OCIO accomplished the following major EA objectives. USDA supported several external EA communities of practice; specifically, the Chief Architects Forum, the Architecture and Infrastructure Committee, the Data Architecture Subgroup, the Enterprise Process Improvement Committee, and the Data.gov Point of Contact Working Group. USDA also responded to the OMB Open Government Directive and Data.gov Initiative establishing USDA points of contact, working groups, support processes, and submissions. Additionally, EA executive and management dashboards were developed to provide at-a-glance segment architecture views, along with cyber security synchronization and investment information views.

USDA continued full segment architecture build-out for the Geospatial and Human Resources Management LoBs. USDA initiated the build of seven domains for IT Technical Architecture, addressing Security and Information Management with the other five to be completed by the end of FY 2010. We also performed an internal assessment of the USDA EA Program in compliance with the Enterprise Architectural Assessment Framework, Version 3.1. USDA supported an Independent Verification and Validation review of the USDA EA Program and leveraged feedback from it and the 2010 USDA EA Value Measurement Survey to update the EA Program Plan. USDA also continued development of common EA elements, particularly those supporting Enterprise-wide projects.

Capital Planning and Investment Control (CPIC): The USDA IT Investment Portfolio for FY 2010 included 280 investments funded at $2.5 billion; the OCIO conducted investment reviews to evaluate the FY 2011 business cases on all major and non-major investments. The OCIO worked with USDA agencies to improve the quality of documentation for IT investments which provided the Department with supporting details critical for the successful management of the IT portfolio.

The USDA OCIO reviewed all USDA FY 2011 IT investment documentation and assessed them relative to IT management "best practices." The OCIO staff worked closely with agencies in ongoing discussions and technical support to ensure excellence of documentation provided to OMB. The OCIO created detailed financial plans for better understanding of the investments and for creating opportunities for consolidation. To support OCIO and agency reviews, the OCIO provided near-real-time reporting and a feedback mechanism with access to the FY 2011 budget document reviews. OCIO finalized the migration to a cheaper, better CPIC tool that makes it easier for agencies and OCIO staff to manage the IT portfolio. To support the USDA EVM process, the USDA OCIO certified that the 13 investments that are in the acquisition or mixed phases are ANSI-748 EVM compliant (including MIDAS, the Modernize and Innovate the Delivery of Agricultural Systems project, and the Financial Management Modernization Initiative) and all are within 10 percent of their cost and schedule goals. The USDA OCIO submits monthly EVM Reports to OMB. In addition, the OCIO has finalized a USDA EVM directive.

IT Acquisition Approval Process: In FY 2010, OCIO reviewed for prior approval more than 209 IT acquisition requests (AAR) valued at more than $1.26 billion. In addition, OCIO successfully automated the tracking, scoring, and electronic signing of the requests via the IT Acquisition Approval process, integrating SharePoint with the Department's Enterprise Content Management platform. Of all the FY 2010 AARs, OCIO processed 114 requests, valued at $362 million in the newly integrated system. OCIO also issued a Draft AAR Guidance document, February, 2010.

In FY 2009, OCIO reviewed for prior approval more than 220 IT acquisition requests (AAR) valued at more than $1.3 billion. In addition, OCIO successfully automated the IT Acquisition Approval process using the Department's Enterprise Content Management platform. Of all the FY 2009 AARs, OCIO processed 93 valued at $818 million in the newly automated system. OCIO also issued version 2 of the AAR Preparation and Submission Guidance document.

Workforce Planning and Development: In September 2009, OCIO updated its progress in accomplishing objectives of the Government-wide Human Capital Management Report and provided projections for its IT Workforce through FY 2013. Through training and development, organizational intervention, and talent recruitment, USDA continues to close the current competency gaps in IT and works toward improving electronic Government. During FY 2010, USDA's CIO co-chaired the IT Workforce Committee of The Chief Information Officer's Council; and helped lead a significant effort in preparing for the FY 2011 Information Technology Workforce Capability Assessment (ITWCA). Prior to implementing the Web-based workforce survey, the ITWCA working group reviewed and revised the survey content to ensure that the:

- Specialized Job Activities covered all key IT program areas of responsibility;
- IT Skills Inventory reflected the most current IT professional requirements; and
- IT Certifications Inventory included all up-to-date certification areas and examples of their application.

In FY 2010, OCIO was selected to pilot the OMB Multi Sector Workforce Initiative for USDA. OCIO chose the Applications Operations Branch (AOB) in the International Technology Services (ITS) organization as the pilot organization. AOB resources consisted of 25 Federal employees and 110 contractor employees. The organization conducted an extensive evaluation of specific factors including, analysis of inherently Government functions, retention rates, volume requirements, workflows, cost comparisons, etc. The results of the pilot, which are being executed, recommended 50+ contract positions be federalized.

Enterprise Geospatial Management Office: EGMO was established in FY 2010 to offer executive leaders geographic-based analytic skills, application tools and data asset management at the Department level of USDA. Through a collaborative approach with agency GIS centers of excellence, EGMO developed a USDA capability assessment, best practices network, technology architecture for data and services, and geospatial governance in FY 2010. Insights derived from these contributions helped drive innovation and increase the maturity of solutions for diverse stakeholder and public problems.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Statement of Goals and Objectives

The OCIO has three strategic goals and seven objectives that contribute to all of the Department Strategic goals and objectives

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcome
OCIO supports all USDA strategic goals	Goal 1: Provide customers and employees with access to the information they need.	Objective 1.1: Enhance service delivery by: 1) Improving citizen's knowledge and access to USDA services, 2) Collaborating with public and private partners, and 3) Achieving internal efficiency through Department-wide solutions. Objective 1.2: Provide high quality, secure, and reliable telecommunications services to USDA agencies and customers, enabling them to obtain timely and accurate data.	Presidential E-Gov Initiatives Innovations and Emerging Technology; Identity, Credential, and Access Management; remote Mobility Departmental e-Gov Initiatives Enterprise Architecture Telecommunications	Key Outcome 1.1: Customers and employees have access to the information they need, when they need it and where they need it.
	Goal 2: Ensure the privacy of customer data and protection and safety of USDA information.	Objective 2.1: Strengthen the security of USDA information assets. Improve the management and mitigation of risk to USDA information assets. Objective 2.2: Promote awareness and understanding of USDA Cyber Security Program by enhancing communications and information security awareness within all levels of USDA and implement mechanisms to enhance information sharing and interoperability among all agencies within USDA. Objective 2.3: Centrally manage and monitor all USDA network and security systems across the diverse USDA IT environment and intelligently and proactively mitigate security breaches and vulnerabilities.	Systems Certification and Accreditation Cyber Security Enterprise Architecture Security Operations Center Innovations and Emerging Technology; Identity, Credential, and Access Management Privacy	Key Outcome 2.1: USDA programs are delivered in a safe, secure IT environment that protects the confidential data of customers and program recipients. Protect Sensitive and Personally Identifiable Information (PII)

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcome
OCIO supports all USDA strategic goals	Goal 3: Strengthen the management and use of USDA IT resources.	Objective 3.1: Focus IT spending on high priority modernization initiatives. Objective 3.2: Leverage security spending to ensure consumer trust is established and emerging IT services, systems, and related infrastructures.	Capital Planning and Management Asset Management and Risk Assessment Innovations and Emerging Technology; Identity, Credential, and Access Management Security Operations Center	Key Outcome 3.1: USDA acquires, manages and uses IT resources in cost efficient ways; and achieves economies of scale. Key Outcome 3.2: USDA demonstrates effective, efficient and proactive security practices and risk management strategies that demonstrate the trustworthiness of its IT resources, enabling private and public partners to expand their use of USDA IT services with confidence and reliance.

Selected Accomplishments Expected for the FY 2012 Proposed Resource Level:

- The majority of USDA agencies on-line services will be integrated with USDA's enterprise eAuthentication Service, the goal will be to ensure all are integrated.
- The majority of the USDA agencies will have integrated their email services with USDA's enterprise messaging service.
- USDA agencies will continue integrating applicable agency systems with USDA's enterprise ICAM Program Service.
- USDA will hold a mobile workforce conference and identify opportunities for enhanced information sharing.
- Continue ongoing Certification and Accreditation (C&A) process for all new and continuing systems in its inventory.
- Continue Governance, Compliance and Risk Management program to improve the identification, management, and mitigation of risks to USDA information systems and digital assets.
- Cross-walk the Federal Information Security Management Act list of systems to the Enterprise Architecture Repository.
- Continue implementation of initiatives to improve FISMA compliance and mitigate the IT Material Weakness.
- OCIO will continue to offer a variety of training on Earned Value Management (EVM) and other project management issues.
- Staff will monitor agency updates to Capital Planning Investment Repository (CIMR) (USDA's name for the proprietary software, WorkLenz) to ensure that actual performance data is being tracked for all IT investments that meet USDA's EVM threshold. CIMR is the capital planning and EVM monitoring tool that USDA's agencies use to record IT investment data. In addition, it formulates investment files for the electronic submission to OMB.

- Staff will also monitor agency EVM process maturity. OCIO will continue to monitor IT investments on OMB's "watch list" to ensure the quality of the business case documentation is strengthened.
- Complete comprehensive security assessments of the network and infrastructure General Support Systems across USDA.
- Provide continuous, 24x7x365 IT security monitoring, security trend analyses and incident response through the Agriculture Security Operations Center (ASOC).
- Identify standard security tools and techniques for the ASOC; and create a corresponding multi-year, multi-vendor blanket purchase agreement for the USDA agencies use that both consolidates the technical approach and provides economies of scale in bulk purchasing.
- Provide real-time asset tracking and inventory data through enterprise deployment of BigFix™ software.
- Provide USDA CIO and senior managers with an effective monitoring and reporting tool that integrates real-time situational data and standardizes it into a common operating picture the overall USDA security posture.
- OCIO will provide bi-weekly and monthly security reports showing each component agency's progress on security patching, vulnerability scanning, FDCC compliance, and energy management.
- OCIO will provide monthly automated data feeds for OMB's Cyberscope reporting initiative, based on ASOC's investment in security automation tools.
- OCIO will capture USDA data and incident trends. Based on common data platforms and analysis tools for security events
- Rather than investing in computer rooms scheduled to be decommissioned as a result of the USDA Data Center Consolidation Initiative, USDA will be is focusing capital investment into its EDCs and implementing new green technologies and industry best practice to drive down the PUE ratio at these sites.
- Rather than investing in computer rooms scheduled to be decommissioned as a result of the USDA Data Center Consolidation Initiative, USDA will be is focusing capital investment into its EDCs and implementing new green technologies and industry best practice to drive down the PUE ratio at these sites.
- Expansion of shared private-cloud computing and storage platforms. Implementation of Platform as a Services (PaaS) windows/Linux has been successful and plans for Solaris and AIX are underway with implementation expected during FY 2011.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Key Performance Outcomes and Measures

Goal 1. Provide customers and employees with access to the information they need.

Key Outcome: Customers and employees have access to the information they need – when they need it, where they need it.

Key Performance Measure:
- Increase return on investment for eGovernment and Lines of Business common solutions.

Goal 2. Ensure the privacy of customer data and protection and safety of USDA information.

Key Outcome: USDA programs are delivered in a safe, secure IT environment that protects the confidential data of customers and program recipients.

Key Performance Measures:
- Percent of USDA IT systems that are certified, accredited or otherwise authorized as being properly secured.
- Percent of identified population that completed annual security awareness refresher training.
- Number of program security reviews completed.
- Percentage of systems tested using 800-53 rev. 3 security controls
- Number of security incidents closed within 30 days.
- Number of General Support Systems inventoried, base-lined, and assessed.
- Number of ASOC incident first phone calls that are answered live by an incident handler.
- Number of agencies/components participating in USDA's enterprise Identity, Credential, and Access Management (ICAM) Program service.
- Percentage of agency systems integrated compacted with agency systems planned to be integrated

Goal 3. Strengthen the management and use of USDA IT resources.

Key Outcome: USDA acquires, manages and uses IT resources in cost efficient ways; and achieves economies of scale.

Key Performance Measures:
- Number of investments in USDA IT portfolio.
- Through the use of Earned Value Management, maintain 100 percent of USDA IT projects that are within 10 percent of cost/schedule/performance objectives.
- Number of ASOC-conducted penetration tests to validate the system security controls of the USDA General Support Systems undergoing certification and accreditation in FY 2011 (in accordance with NIST special publication 800-53).
- Number of system security controls for the USDA General Support Systems undergoing certification and accreditation in FY 2011 that are tested in accordance with NIST special publication 800-53, rev.3.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Key Performance Targets:

Performance Measure	2007 Actual	2008 Actual	2009 Actual	2010 Actual	2011 Target	2012 Target
Performance Measure #1						
Increase return on investment (ROI) for eGovernment and Lines of Business (LOB) common solutions at portfolio level for all E-Gov activities.						
a. Units	5%	5%	5%	5%	5%	5%
b. Dollars	$7,155	$7,741	$8,328	$8,016	$8,071	$8,071
Performance Measure #2						
Percent of USDA IT systems that are certified, accredited or otherwise authorized as being properly secured.						
a. Units	100%	100%	100%	100%	100%	100%
Percent of identified population that completed annual security awareness refresher training.						
a. Units	90%	100%	100%	100%	100%	100%
Number of program security reviews completed.						
a. Units	8	8	8	8	24	24
Number of agencies/components participating in USDA's enterprise Identity, Credential, and Access Management (ICAM) Program.						
a. Units	N/A	N/A	N/A	N/A	20	29
Number of ASOC incident first phone calls that are answered live by an incident handler.				Est.		
a. Units	N.A.	N.A.	N.A.	Baseline	80%	80%
Number of security incidents closed within 30 days.				Est.		
a. Units	N.A.	N.A.	N.A.	Baseline	90%	90%
Number of General Support Systems inventoried, and assessed.				Est.		
a. Units	N.A.	N.A.	N.A.	Baseline	99%	99%
b. Dollars	$3,987	$3,700	$3,981	$48,060	$47,967	$46,967
Performance Measure #3						
Through the use of Earned Value Management (EVM), maintain 100% of USDA IT projects that are within 10% of cost/schedule/ performance objectives.						
a. Units	100%	100%	100%	100%	100%	100%
Reduce number of non-EDC computer facilities.						
a. Units	97	97	97	97	97	38
b. Dollars	$5,103	$4,676	$5,030	$5,086	$5,541	$8,541

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER
Full Cost by Department Strategic Goal

	Dollars in thousands		
	FY 2010	FY 2011	FY 2012
Strategic Goal 1: Provide customers and employees with access to the information they need.			
Information and Technology Management			
Administrative Costs (Direct)	$8,016	$8,071	$8,071
FTEs	21	22	22
Performance Measure:			
Increase ROI for e-Government and LoB common solutions at portfolio level for all E-Gov activities.	5%	5%	5%
Strategic Goal 2: Ensure the privacy of customer data and protection and safety of USDA information.			
Cyber Security Program Office			
Administrative Cost (Direct)	37,861	35,940	34,940
ASOC			
Administrative Costs (Direct)	10,199	12,027	12,027
Total Costs	48,060	47,967	46,967
FTEs	36	69	69
Performance Measure:			
Percent of USDA IT Systems that are certified, accredited, or otherwise authorized as being properly secured	100%	100%	100%
Percent of identified population that completed annual security awareness refresher training	100%	100%	100%
Number of program security reviews completed	8	24	24
Number of security incidents closed within 30 days	Est. Baseline	90%	90%
Number of General Support Systems inventoried, baselines, and assessed	Est. Baseline	99%	99%
Number of ASOC incidence first phone calls that are answered live by an incident handler	Est. Baseline	80%	80%
Number of agencies/components participating in USDA's enterprise ICAM program	Est. Baseline	20	29
Strategic Goal 3: Strengthen the management and use of USDA IT resources.			
Program Management Office			
Administrative Costs (Direct)	5,086	5,541	5,541
EDC			
Administrative Costs (Direct)	--	--	3,000
Total Costs	5,086	5,541	8,541
FTEs	22	28	28
Performance Measure:			
Through the use of EVM, increase the percentage of a USDA IT projects that are within 10% of cost/schedule/performance objectives	100%	100%	100%
Reduce number of non-EDC computer facilities	97	97	38
Total Cost all Program	$61,162	$61,579	$63,579
FTEs (direct appropriation)	79	119	119