2013 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, 2011, there were 998 full-time permanent employees funded by appropriated, reimbursed, and Working Capital Funds.

OIG Reports - Completed

88501-1-11	2/2011	Statement on Standards for Attestation Engagements #16, Report on Controls at the National Information Technology Center

OIG Reports – In Progress

50501-15-FM	11/2009	Fiscal Year 2009 Federal Information Security Management Act Report - This audit contained 14 recommendations. OCFO has granted final action on 6. Remediation action on remaining recommendations is ongoing.
50501-02-IT	11/2010	Fiscal Year 2010 Federal Information Security Management Act Report - This audit contained 19 recommendations. OCFO has granted final action on 5. Remediation action on remaining recommendations is ongoing.
50501-2-12	11/2011	Fiscal Year 2011 Federal Information Security Management Act Report - OCIO's Request for Management Decision is in draft and in clearance through OCIO management. OCIO has initiated remediation actions for all 10 of the recommendations.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

50501-01-IT	8/2011	USDA's Management and Security over Wireless Handheld Devices - The audit resulted in 5 recommendations for corrective action by OIG. Remediation actions are underway.

GAO Reports - Completed

GAO-06-831	8/2006	Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation
GAO-11-638		Green Information Technology: Agencies Have Taken Steps to Implement Requirements, But Additional Guidance on Measuring Performance Needed
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-10-701	7/2010	Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Data Accuracy Improvement Needed

GAO Reports – In Process

GAO-08-525	6/2008	Information Security – Federal Agency Efforts to Encrypt Sensitive Information are Under Way, but Work Remains - 1/24/11 – USDA updated GAO on the status of the Statement of Action in July 2010. GAO followed-up with requests for additional documentation on recommendations 1 through 3. Additional information was provided by NITC in August 2010. GAO has not requested any further information from USDA on this audit.
GAO-10-202	3/2010	Federal Information Security Initiatives, FDCC/TIC/Einstein
GAO-11-43	11/2010	Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks but Further Actions Can Mitigate Risk - There were 5 recommendations from this audit. Completion of actions on Recommendations 1 and 2 are pending publication of USDA policies on Wireless Security and Security over Wireless Devices when Traveling Internationally. USDA originally estimated these policies would be completed by 9/30/11 (revised to 12/3011). However, due to resource limitations in the IT Security area, finalization of these policies has not been completed. Recommendations 3 and 4 addressed specific wireless network issues in Lakewood, CO and Washington, DC, respectively. These issues were addressed via CIO guidance memo issued 1/30/11. No additional information or status has been requested by GAO.
GAO-11-605	6/2011	Social Media – Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate - Facebook and Twitter PIAs have been reviewed and posted to USDA.gov. The You Tube PIA is being worked on by Office of Communication
GAO-11-565	7/2011	Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Statement of Available Funds and Staff Years

(Dollars in thousands)

Item	2010 Actual		2011 Actual		2012 Estimated		2013 Estimated	
	Amount	Staff Years	Amount	Staff Years	Amount	Staff Years	Amount	Staff Years
Salaries and Expenses:								
Discretionary Appropriations....	$61,579	79	$40,000	97	$44,031	112	$44,031	112
Rescission.....	-	-	-80	-	-	-	-	-
Total Available.....	61,579	79	39,920	97	44,031	112	44,031	112
Lapsing Balances.....	-417	-	-83	-	-	-	-	-
Obligations.....	61,162	79	39,837	97	44,031	112	44,031	112
Obligations under Other USDA appropriations:								
Reimbursements:								
Innovation & Emerging Architecture.....	775	-	630	-	630	-	630	-
CSAM.....	400	-	-	-	-	-	-	-
CPIC.....	350	-	130	-	130	-	130	-
Geospatial IS.....	8,330	-	8,330	-	8,330	-	8,330	-
VTC.....	222	-	-	-	-	-	-	-
Project Management.....	120	-	95	-	95	-	95	-
NTIA Spectrum.....	1,596	-	1,756	-	1,756	-	1,756	-
Decision Lens.....	198	-	275	-	275	-	275	-
Contract Management.....	-	-	1,315	-	1,315	-	1,315	-
CPO.....	-	-	159	-	159	-	159	-
LincPass.....	-	-	231	-	231	-	231	-
Other Activities.....	224	-	361	-	361	-	361	-
Total, Agriculture Appropriations..	12,215	-	13,282	-	13,282	-	13,282	-
Working Capital Fund (WCF) a/								
Information Technology.....	400,252	855	398,728	882	406,831	948	420,539	953
NITC (Non-USDA).....	12,191	17	15,477	35	19,341	43	18,080	46
WCF Management Fee.....	379	8	-	8	-	8	-	8
Capital Equipment.....	9,400	-	11,360	-	-	-	-	-
Total, WCF.....	422,222	880	425,565	925	426,172	999	438,619	1,007
Total, OCIO.....	495,599	959	478,684	1,022	483,485	1,111	495,932	1,119

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

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Permanent Positions by Grade and Staff Year Summary a/

Item	2010 Actual			2011 Actual			2012 Estimate			2013 Estimate		
	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field b/	Total
ES	6	-	6	6	-	6	6	-	6	6	-	6
GS-15	14	1	15	15	2	17	15	2	17	15	2	17
GS-14	22	3	25	38	4	42	38	4	42	38	4	42
GS-13	13	-	13	18	5	23	18	5	23	18	5	23
GS-12	7	1	8	7	3	10	7	3	10	7	3	10
GS-11	1	-	1	4	-	4	4	-	4	4	-	4
GS-10	1	-	1	1	-	1	1	-	1	1	-	1
GS-9	1	-	1	3	-	3	3	-	3	3	-	3
GS-8	1	1	2	3	-	3	3	-	3	3	-	3
GS-7	-	-	-	2	-	2	2	-	2	2	-	2
GS-4	19	-	19	1	-	1	1	-	1	1	-	1
GS-3	7	-	7	-	-	-	-	-	-	-	-	-
GS-2	2	-	2	-	-	-	-	-	-	-	-	-
Total Perm. Positions	94	6	100	98	14	112	98	14	112	98	14	112
Unfilled, EOY c/	21	-	21	15	-	15	-	-	-	-	-	-
Total, Perm. Full-Time Employment, EOY	73	6	79	83	14	97	98	14	112	98	14	112
Staff Year Est	73	6	79	83	14	97	98	14	112	98	14	112

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

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 2013 Budget Estimates propose no additional purchases or leases of vehicles.

OCIO-International Technology Services (ITS) is the in-house provider of information technology service and support for over 40,000 USDA Service Center Agency (SCA) employees at 3,400 field, State, and headquarters offices located across all 50 U.S. States. All ITS support offices are co-located with SCA's field offices. The SCAs consist of Farm Service Agency (FSA), Rural Development (RD) and the Natural Resources Conservation Service (NRCS). 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 and ensure that computers, applications, networks, and communication technologies are fully functional. The agencies can then focus on supporting 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 to deploy them where and when they are needed. ITS fleet service allows its employees to travel to other SCA locations and maintain a unified organization dedicated to supporting both the shared and diverse IT requirements of the SCAs and their partner organizations. ITS also use the fleet to address issues with malfunctioning IT equipment at these locations.

OCIO's current fleet is based on mission and geographic needs. As of September 30, 2011, ITS has 224 leased GSA vehicles and one agency owned vehicle and NITC has two leased GSA vehicles. It continues to lease vehicles from GSA to provide IT support to the SCAs within USDA.

Changes to the motor vehicle fleet. No changes are proposed to the fleet for 2013.

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, 2011, are as follows:

Size, Composition, and Annual Cost
(Dollars in thousands)

	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 000)
		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	20	-19	1	0	0	0	0	+2	+$3
FY 2011	116	91	20	0	0	0	0	227	$995
Change from 2011	0	0	0	0	0	0	0	0	0
FY 2012	116	91	20	0	0	0	0	227	$998
Change from 2012	0	0	0	0	0	0	0	0	0
FY 2013	116	91	20	0	0	0	0	227	$998

*ITS expanded fleet services in 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 2009 was the first year that OCIO leased vehicles. Vehicles were received from GSA at various times during the fiscal year; therefore, the total cost of leasing vehicles in 2009 was not realized. In 2010 we added five additional vehicles and paid leasing costs for the 220 vehicles for the entire year.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

The estimates include appropriations language for this item as follows (new language underscored; deleted matter enclosed in brackets):

Salaries and Expenses:
For the necessary expenses of the Office of the Chief Information Officer, $44,031,000.

Lead-off Tabular Statement

Appropriations Act, 2012	$44,031,000
Budget Estimate, 2013	44,031,000
Change in 2012 Appropriation	0

Summary of Increases and Decreases
(Dollars in thousands)

	2010 Actual	2011 Change	2012 Change	2013 Change	2013 Estimate
Discretionary Appropriations:					
Office of the Chief Information Officer	$61,579	-$21,659	-$4,111	0	$44,031

Project Statement
(On basis of appropriations)
(Dollars in thousands)

Program	2010 Actual Amount	2010 Actual Staff Years	2011 Actual Amount	2011 Actual Staff Years	2012 Estimate Amount	2012 Estimate Staff Years	Change Amount	Change Staff Years	2013 Estimate Amount	2013 Estimate Staff Years
Discretionary Appropriations:										
Office of the Chief Information Officer	$61,579	79	$39,920	97	$44,031	112	-	-	$44,031	112
Rescission and Transfer (Net)	-	-	80	-	-	-	-	-	-	-
Total Appropriation	61,579	79	40,000	97	44,031	112	-	-	44,031	112
Rescission	-	-	-80	-	-	-	-	-	-	-
Total Available	61,579	79	39,920	97	44,031	112	-	-	44,031	112
Lapsing Balances	-417	-	-83	-	-	-	-	-	-	-
Total Obligations	61,162	79	39,837	97	44,031	112	-	-	44,031	112

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Project Statement
(On basis of obligations)
(Dollars in thousands)

Program	2010 Actual Amount	Staff Years	2011 Actual Amount	Staff Years	2012 Estimate Amount	Staff Years	Change Amount	Staff Years	2013 Estimate Amount	Staff Years
Discretionary Obligations:										
Office of the Chief Information Officer	$61,162	79	$39,837	97	$44,031	112	-	-	$44,031	112
Total Obligations	61,162	79	39,837	97	44,031	112	-	-	44,031	112
Lapsing Balances	417	-	83	-	-	-	-	-	-	-
Total Available	61,579	79	39,920	97	44,031	112	-	-	44,031	112
Rescission	-	-	80	-	-	-	-	-	-	-
Total Appropriation	61,579	79	40,000	97	44,031	112	-	-	44,031	112

Justification of Increases and Decreases

Base funds will allow the Office of the Chief Information Officer to continue to provide guidance, leadership and coordination for the Department's information management, technology investment and cyber security activities in support of USDA program delivery.

(1) No increase for the Office of the Chief Information Officer ($44,031,000 and 112 staff years available in 2012).

(a) An increase of $53,000 to fund increased pay costs.
The proposed funding level is needed to cover pay and benefit cost increases for existing staff. This will ensure adequate resources available to continue to allow the office to carry out its full range of responsibilities and support program delivery.

(b) A decrease of $53,000 will be absorbed in the base operating budget.
The reduction in funding reflects the redirection of funds from contracts to pay and benefits for existing staff.

Geographic Breakdown of Obligations and Staff Years
(Dollars in thousands)

State/Territory	2010 Actual Amount	Staff Years	2011 Actual Amount	Staff Years	2012 Estimate Amount	Staff Years	2013 Estimate Amount	Staff Years
District of Columbia	$60,099	73	$38,124	83	$42,305	98	$42,305	98
Kansas City, MO	1,063	6	1,713	14	1,726	14	1,726	14
Obligations	61,162	79	39,837	97	44,031	112	44,031	112
Lapsing Balances	417	-	83	-	-	-	-	-
Total, Available	61,579	79	39,920	97	44,031	112	44,031	112

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects
(Dollars in thousands)

		2010 Actual	2011 Actual	2012 Estimate	2013 Estimate
Personnel Compensation:					
Washington D.C.		$7,762	$9,547	$9,680	$10,001
Kansas City, MO.		669	1,348	1,400	1,425
11	Total personnel compensation	8,431	10,895	11,080	11,426
12	Personal benefits	1,912	2,736	3,102	3,203
13.0	Benefits for former personnel	125	-	-	-
	Total, personnel comp. and benefits	10,468	13,631	14,182	14,629
Other Objects:					
21.0	Travel and transportation of persons	302	217	210	210
22.0	Transportation of things	2	2	3	3
23.3	Communications, utilities, and misc. charges	926	731	750	750
24.0	Printing and reproduction	60	63	61	61
25.2	Other services from non-Federal sources	16,739	18,966	13,695	13,248
25.3	Other purchases of goods and services from Federal sources	29,537	6,011	14,880	14,880
26.0	Supplies and materials	1,957	83	100	100
31.0	Equipment	1,171	133	150	150
	Total, Other Objects	50,694	26,206	29,849	29,402
99.9	Total, New Obligations	61,162	39,837	44,031	44,031
Position Data:					
Average Salary (dollars), ES Position		$160,182	$165,913	$166,000	$170,000
Average Salary (dollars), GS Position		$89,033	$107,646	$94,900	$97,780
Average Grade, GS Position		13.1	13.7	13.3	13.4

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, Enterprise Shared Services, Enterprise Correspondence Management Modules, the Enterprise Architecture Repository (EAR), and capital planning investment tools). For example, there are more than 125,000 active AgLearn accounts across USDA, and in 2011 these users completed 519,783 online courses and attended 1,002 "Webinar" training events. USDA eAuthentication Service protects 462 Web-based applications that require single factor (userid/password) authentication and provide the option to authenticate using the USDA LincPass card.

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 $607,000 to support 8 E-Government Initiatives and 5 LoBs in 2012. 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.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

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's purpose is to define the "corporate" or enterprise-wide view and standards for IT infrastructure that are business driven and interoperable across agencies; including hardware, software, information management, and security. USDA's Program employs a collaborative approach between the OCIO, USDA agencies to develop USDA standards. USDA standards also consider the Federal Enterprise Architecture Reference Models which are drafted by Chief Enterprise Architecture Communities within the federal government. USDA developed an enterprise-wide view of an EA that represents the current architecture, target architecture, and transition plan, and builds on the architectures already under development within USDA's agencies. Interoperability objectives increase the need for standardization across technology architecture domains. OCIO has developed a technology architecture guidebook with USDA Department-wide technology standards. The technology standards 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; allows varying degrees of cross-agency standardization; addresses lifecycle of technology standards from emerging to retirement; and is easy to maintain and adjust over time as business needs and technology capabilities change. 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 EA. 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 2012 EA activities include:

- Refinement of the USDA technology standards (Bricks and Patterns);
- Participation in Open Government and Data.Gov Initiatives—increasing the publication of USDA data on Data.gov web site;
- Update the EA Transition Plan;
- Continue development of executive and management reports, and dashboards;
- Update and initiation of EA Guiding Principles;
- Creation and incorporation of EA Governance into IT Governance; and
- Development of a Security Architecture Blueprint.

Capital Planning and Investment Control (CPIC): CPIC is the primary process for making investment decisions, assessing investment process effectiveness, and refining investment related policies and procedures. CPIC is mandated by the Clinger-Cohen Act, which requires agencies to use a disciplined process to acquire, use, maintain and dispose of IT. CPIC accomplishes these requirements through three phases: Select Phase, Control Phase, and Evaluate Phase. The OCIO coordinates the Department's CPIC, budgeting, and performance management processes for IT. 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, while providing a positive return on the IT investments for taxpayers. The Department's Enterprise IT Governance process will serve as the USDA senior authoritative body charged with the oversight of major IT investments 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.

Two key areas of focus for 2012 are to institutionalize the Enterprise IT Governance Process and to prioritize IT investments using a comprehensive and flexible decision making process that aids decision makers in constructing actionable and repeatable resource allocations. 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. Additionally, OCIO will focus on aligning IT investments by LOBs; align with EA, IT security, and the USDA budget process. Three senior management oversight committees will be established, the Executive Committee, IT Investment Review Board, and Investment Acquisition Board, to provide executive oversight of the Department's major IT modernization investments.

IT Acquisition Approval Review (AAR) Process: The IT acquisition approval process is an OCIO control activity where the CIO approves all USDA IT acquisitions valued at $25,000 and above. OCIO technical reviews are conducted on each acquisition approval request to ensure conformity with USDA EA, USDA telecommunications standards and practices, IT security considerations, and CPIC requirements. The OCIO works with agencies to ensure that approved IT acquisition requests provide the necessary information, as part of the Enterprise IT Governance Process.

Information Management: Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. USDA's current Information management environments are comprised of legacy information resident in line of business applications: Enterprise

Content Management (ECM), Electronic Records Management (ERM), Business Process Management (BPM), Email Management (EMM), Information Organization and Access (IOA), Knowledge Management (KM), Web Content Management (WCM), Document Management (DM) and Enterprise 2.0 (E2.0) technology solutions and best practices. The CIO is responsible for managing this information throughout the information lifecycle regardless of source or format (data, paper documents, electronic documents, audio, video, etc.) and for delivery through multiple channels that may include cell phones and web interfaces.

In 2011, OCIO has made many strides in improving IM across the Department, including developing mandatory records management training for the workforce, developing Section 508 Training for the workforce, and partnering with USDA agencies to improve accessibility to EIT for persons with disabilities. In addition, in 2011 OCIO processed over 90 information collections that allowed USDA agencies to collect information critical to continuing business operations and execute the mission. OCIO also processed over 50 Departmental directives, Departmental notices, and other policies.

Privacy Act and Freedom of Information Act (FOIA): The CIO is the Department's Chief FOIA Officer and Senior Official for Privacy matters. The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974) established a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. In 2011, the USDA Privacy office conducted over 70 Privacy Threat Assessments (PTAs) and Privacy Impact Assessments (PIAs), and reviewed and processed over 50 System of Records Notices (SORNs) for USDA systems. OCIO oversaw the USDA Data Integrity Board (DIB) process and made recommendations to the DIB for computer matching requirements.

FOIA is a law ensuring public access to U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government - not the public - to substantiate why information may not be released. Upon written request, agencies of the United States government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in the FOIA. This right of access is ultimately enforceable in federal court. The OCIO processed over 295 FOIA requests for the Office of the Secretary in 2011. To gain efficiencies in the FOIA process, OCIO implemented a Department-wide FOIA management system and provided training to FOIA Officers, FOIA analysts, and other key personnel involved in the FOIA process. Additionally, the OCIO participated in regular Chief FOIA Officer meetings with the Department of Justice.

Strategic Planning, Policy, and Governance: In 2011, the OCIO drafted the IT Strategic Plan for 2012-2016, which outlines the strategic direction for the Department in utilizing IT products and services to achieve the business objectives and successfully execute the mission. OCIO also developed policy for capital planning and enterprise architecture. OCIO developed an enterprise governance process, and supporting documents to describe the roles and responsibilities of key decisions makers in the governance process.

Cyber Security: OCIO continues to implement its aggressive strategy to improve USDA's information security via: 1) training; and 2) establishing standardized computer security policies, processes and controls within the Department. 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.
The OCIO continues to align with security best practices, Federal laws and oversight requirements. The USDA participates in the OMB Information Systems Security LoB: 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.
To improve FISMA compliance throughout the USDA, OCIO continues to improve the Center of Excellence operations, which were chartered in 2010 work to ensure that all systems traverse the USDA/National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) security processes, achieve Authorization to Operate for all systems, provide for timely mitigation of all identified weaknesses, and report weekly on the status

of all Plans of Actions and Milestones (POA&Ms). An ongoing initiative to complete the acceptance process for all newly developed USDA policies are underway, synchronizing with newly issued Federal guidance.
Implementation of a plan to begin the transition/implementation of a RMF compliant Continuous Monitoring process, as defined by FISMA, independently assessing 1/3 of the controls each year, identify yearly, key controls to more rapidly assess annually, the controls identified as weaknesses through testing, and more rapidly remediate identified issues.
The Annual Information Security Awareness Training classes were revised, reducing the class length by 40 percent, and are now available online. The classes include pre-testing and local classroom diversity training. OCIO monitors and reports on the results monthly to the agencies, quarterly and annually to FISMA. The OCIO continues to aggressively implement initiatives to improve FISMA compliance and mitigate the identified IT material weakness.
To provide more complete oversight, concurrency reviews of all systems are now performed after the development of a system, and then again after tests are completed. Strict guidelines have been implemented to ensure all USDA systems comply through implementation of a new Performance Work Statement, mandatory training of all personnel engaged in security assessments, and remediation of all identified issues.
USDA will also expand current security operations and compliance processes in the transition to *Continuous Monitoring*, which will provide real-time monitoring and data feeds regarding IT systems, hardware, inventories, and other security-related statuses. These efforts are expected to reduce the on-going costs of security operations.

OCIO continues its use of the Cyber Security Assessment and Management (CSAM), the Department of Justice's LoB for the FISMA reporting tool, to support its Certification & Accreditation (C&A) process. In conjunction with OCFO, OCIO has implemented a process to minimize duplication of testing controls while simultaneously improving the quality and effectiveness of testing. In 2012 new initiatives include:

- Moving CSAM to the Cloud environment at NITC
- Modernizing CSAM through major upgrade to Version 3.0
- Implementing common controls (program, policy and data center inheritable controls) in CSAM

In 2012 the Center of Excellence (COE) will continue implementation of the USDA 6 step RMF Process addressing OIG audit recommendations and strengthening the USDA enterprise security posture. New initiatives include:

- Conducting training sessions to continue to improve the quality of USDA C&A packages and the overall C&A process
- Continue to expand the outreach the COE Liaisons to assist 100% of all agencies in achieving FISMA compliance for 17 agencies and 15 offices supporting over 650 systems streamlined into 258 FISMA reportable systems.

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. 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. The OCIO also led the effort to find other potential ERF locations for USDA.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Agriculture Security Operations Center (ASOC): In 2010 OCIO established the ASOC. The ASOC is now operational and has taken responsibility for the ongoing enterprise security operations functions of USDA.

ASOC provides operational support and continuous monitoring and analysis of the USDA backbone and USDA agency networks from a central enterprise perspective. ASOC monitors, collects and analyzes key data to identify patterns that indicate exploitation of vulnerabilities, intrusions, and malicious activities. ASOC provides 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.
In 2012 ASOC will focus on:

1) Continue to fine tune the security stack array tools to better identify, research, analyze and resolve high risk events that become incidents in a timely manner;
2) Identify and recommend cost effective recommendations to construct staff and manage a 24/7 security operations center to provide continuous monitoring and analysis of the USDA backbone and USDA agency networks;
3) Improve technical skills to continue to detect, collect, and analyze key data patterns to provide real time analytical support and proactive responses to cyber threats and protect the business of USDA.

Additionally, ASOC actively participates as the Department's representative in the National Cyber Security Center and Department of Homeland Security initiatives and collaborates, 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.
To improve USDA workforce capabilities in the area of IT security, the OCIO has established an intern training program. This program, now in its third year, provides full-time summer employment for interns at USDA partner agencies, and limited employment throughout the academic year. Among other training, interns receive ethical hacking security training and business etiquette training. A number of candidates who have completed the program have accepted full-time employment in the federal service. The success of the program is also indicated by a doubling of the number of applicants from 2010 to 2011.

Secure Communications: 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.

In 2011 the ASOC established a presence in Kansas City for Secure Communications and worked closely with USDA's Office of Homeland Security on the build-out and staffing of a facility in Kansas City to maintain USDA operations in the event that a catastrophe prevents existing facilities from carrying out the USDA mission.

The ASOC established trust relationships and currently maintains information sharing partnerships with other governmental agencies such as the United States Computer Emergency Response Team (US-CERT), National Security Agency, Air Force Office of Special Investigations (AFOSI) and the Federal Bureau of Investigation (FBI). These relationships help identify and remediate attacks on key USDA IT assets before significant damage occurs.

In 2012, the ASOC will continue build out of the Devolution site in Kansas City. The communications infrastructure for the site as required by NCSD 3-10 is in development. The Joint Worldwide Intelligence Communications System (JWICS) and Crisis Management System (CMS) process will begin as soon as the facility has been certified by the Central Intelligence Agency. The systems are planned to be installed and operational by the end of 2012. The three systems are the primary systems for the operations of the Devolution Facility. This facility is required in the event the transfer of powers from Washington, DC is needed upon a localized emergency. The secure satellite system and the HF-ALE systems will be added in 2013.

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.

In 2012 the ASOC will improve and enhance ASOC Operational Efficiency by:

- Opening up the ASOC Remedy application to OCIO Incident Response Handlers;
- Improving agency personnel knowledge of cyber security threats;
- Establish collaborative working groups to refine incident handling best practices;
- Enhance USDA Situation Awareness for Cyber Security;
- Publish information on threats, vulnerabilities, and procedures on the ASOC Security web site;
- Integrate incident handling Best Practices; and
- Publish and disseminate incident handling technical reference guide.

Intrusion Detection: USDA has deployed a comprehensive and cohesive integrated security solution called the Security Sensor Array (SSA) that provides a foundation for enterprise wide security monitoring, detection, and protection for USDA. Detection and response time for incidents will be shortened to hours. The SSA performs 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 SSA's carefully managed deployment plan resulted in the rollout of eleven sites on-time and under budget, using detailed, well-defined procedural steps for installation, configuration, and implementation.

In 2012, OCIO will partner with select USDA agencies to deploy agency-specific enhancements to the SSA to monitor critical IT infrastructure. The ASOC will transition the Washington DC Security Sensor Array into an inline security posture in 2012. This transition will align the array into a posture to allow the active blocking of malicious activity. This architecture will also bring inline the SSL appliance. This device will allow the ASOC the ability to decrypt and inspect traffic that is inside encrypted communications tunnels. This architecture will allow the ASOC the ability to activity block malicious activity before it is allowed to enter the USDA Enterprise Computing Infrastructure.

Contracting Agreements: USDA has used its collective buying power to establish a number of enterprise-wide 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, consolidating, funding and working 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 (EDC) 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 private, sensitive, and personally identifiable information (PII). This effort is ongoing, moving from the planning stage to full implementation.

EDC's have developed a private cloud portfolio of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings that serve as the target architecture for the vast majority of applications moving from closing data centers to the Department's Enterprise Data centers. These environments are operated at average utilization rates of 55-65 percent versus the 10-20 percent average utilization rates typically found across the Department's legacy server environments. Additionally, substantial gains in uptime, security, recoverability, and reduced capital/operating costs have been realized.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Data Center Consolidation: The USDA is on track to exceed its original 2011 goal closing 20 data centers, most of which are computer rooms located in high rent office space. To date 14 data centers have been closed in 2011 and the Department is on track to close an additional 9 data centers by December 31, 2011, for a total of 23 data centers closed in Calendar Year (CY) 2011. In CY 2012, 33 additional data centers are slated to be closed.

USDA worked collaboratively with Department of State to transition end user support outside of the contiguous United States to the State Department and moved data center operations to USDA Enterprise Data Center facilities. These actions enabled the elimination of duplicative investments in information technology hardware, software and support services.

USDA focused its 2011 data center closures primarily in the District of Columbia in part to help address critical office space shortages. USDA metro DC data centers closed in 2011 will be repurposed as office space in 2012, avoiding unnecessary lease costs.

Green Initiatives: National Information Technology Center (NITC) fully supports "green" sustainability. Utilizing industry standards and best practices, NITC is implementing a plan to reduce the Department's data center related energy consumption by 50 percent over the next 5 years through virtualization of applications and consolidation of data centers. Our goal is to maximize efficiency, reduce cost and improve customer service.

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 105,000 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 21 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, the ability to derive the majority of an individual's accesses based on attributes that are entered in an HR/procurement capacity, 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 and the recent weather-related government closures pointed out the infeasibility of using these disparate systems for meaningful response and business continuity. The solution was to design and implement the Enterprise VPN. Managed at the highest enterprise level, and with significantly larger capacity, the Enterprise VPN has already realized 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. In addition, we have integrated the Enterprise VPN into the USDA's endpoint security management tool. This ensures that only secure, managed endpoints are allowed remote entry to the Department's resources. This moves the USDA security posture forward and minimizes the USDA security risk.

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 (462 as of October 2011). It is used by approximately 104,066 employees on a daily basis to access administrative and mission critical applications such as HR systems, GovTrip, and financial systems. In September 2011, the eAuthentication system handled approximately 9.1 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 2012 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;
- Continue to support eAuthentication on a 24x7 schedule;
- Continue to integrate new web applications with the eAuthentication infrastructure;
- Modernize eAuthentication to accomplish these objectives;
- Upgrade to newest release of COTS software;
- Move infrastructure to NITC EDC;
- Integrate with EEMS (e.g. Enterprise Directory);
- Migrate all integrated applications to the new infrastructure; and
- Add additional Online Identity Proofing capabilities;

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-refutable, 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. Several disparate systems already existed, so bridging capability was factored into the design to ensure current Agency investments could be leveraged moving forward. 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 are invisible to the end user.
- Consolidated equipment purchases have achieved significant cost savings.

During a time of austere budgets, the USDA's investment in video conferencing will allow us to respond to travel budget cuts without impacting the staff's ability to communicate and collaborate effectively throughout the Nation.

Enterprise Geospatial Management Office: The USDA Enterprise Geospatial Management Office (EGMO) provides Department strategic leadership, emerging technologies and innovation prototypes, Geographic Information Systems (GIS) service implementation and optimization guidance, portfolio planning and governance oversight, and ensures the agriculture spatial data asset lifecycle is effectively managed to address current and future policy and public administration business requirements. Through enterprise-level agency collaboration, the EGMO builds organization capacity and extends best practices to generate cost savings and avoidance.

To achieve these outcomes, and provide a sustainable structure for geographic solutions value-creation, accountability, transparency, and stakeholder participation, four core performance goals are established in 2012:

- Lead Department implementation of enterprise geospatial streamline optimization and strengthening initiatives through first generation policy, process design, governance, workforce development, and other structural, process, and content optimization activities
- Champion and deploy Department Geospatial Strategic Plan with publication of vision and goals, consensus building among agencies, and refinement of performance measures and metrics
- Deploy into production the Enterprise Spatial Mapping Service (ESMS) as an enterprise-level geospatial service platform providing cloud-based spatial data and geographic information systems business solutions, provisioned and consumed through a common portal framework;
- Offer branding by customer group, web map and feature services, map and data product exchange, versioning, templates, and map product and lifecycle management for the geospatial community.
- Restructure existing Department geospatial governance to ensure agency leadership representation, mission relevancy, and capability maturity for implementing contemporary strategy and conducting sustainable operations.

Selected Examples of Recent Progress:

Security Array: Completed the deployment of security management sensors to 11 locations within USDA to protect network traffic. Collectively the sensors analyze and protect our networks from vulnerabilities and report centrally to a management console at the ASOC. The sensor tools better protect the USDA network and provide situational data into a common operating picture to further standardize the overall USDA security posture.

Operational Security Assessments: ASOC 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 13 agency assessments by the end of 2011. These agency assessments represent USDA networks carrying over 80 percent or more of the Department's total network traffic.

Incident Handling Program: Throughout 2011, the ASOC Incident Handling Program (IHD) made more significant strides to improving Incident Management and Customer outreach. Through combined efforts of analyst training and better customer service and the constant re-evaluation and update of internal procedures, ASOC IHD was able to

decrease the average incident age by 35percent, while at the same time the overall number of incidents increased by 25percent, or more than 400 incidents worked.

The ASOC continued to reach 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.

End-Point Security: ASOC provided oversight in the implementation of the USDA enterprise end-point security tool to over 140,000 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).

Secure Communications: Established trust relationships and currently maintain information sharing partnerships with external governmental agencies such as the United States Computer Emergency Response Team (US-CERT), National Security Agency, Air Force Office of Special Investigations (AFOSI) and the FBI. OCIO established an Intelligence/COMSEC presence in Kansas City and continued working closely with the Office of Homeland Security and Emergency Coordination (OHSEC) on the build out and staffing of the Devolution facility in KC.
IT Intern Program: Teamed with ARS Human Resources to utilize Monster Automated Hiring Systems for the processing and ranking of approximately 1,200 applications for the Information Technology Intern Program (ITIP). The ITIP was used as a test case for this newly acquired system. The test was successful in processing and ranking the applications, efficiently executing what had previously been performed manually. Automated processes also improved the panel review process, allowing panel members to review and score top ranking applicants electronically from their offices instead of being required to meet onsite. OCIO increased leveraging of the portal by creating web pages for posting information on Departmental Management intern opportunities across the Department. It used the portal to push information out to USDA interns about Departmental Management activities and demonstrated the portal to other USDA agencies who are now interested in leveraging it for their programs.

Systems Certification and Accreditation (Now the Risk Management Framework (RMF) Process): This initiative has improved the quality of USDA RMF packages and the overall RMF process. USDA's Cyber Policy Oversight Office (CPO) established a Center of Excellence (COE) for Risk Management. The COE:

- Assisted 100 percent of all agencies in becoming FISMA compliant. This includes 17 agencies and 15 offices that supported over 650 systems streamlined into 258 FISMA reportable systems.
- Conducted 105 regular bi-weekly agency meetings in 2011 that resulted in 570 action items. The COE conducted 15 training sessions on CSAM, National Institute of Standards and Technology (NIST) 800-53 Rev3 Conversion, Concurrency Review and POA&M management.
- Conducted three ISA training classes to serve the needs of users not able to utilize the online Aglearn system.

Cyber Security Assessment and Management Tool (CSAM): CPO worked with all agencies to:

- Automate all Risk Management Framework products in CSAM.
- Re-organize CSAM to simplify the documentation of the security characteristics and security assessment information.
- Convert all security controls to comply with the latest version of NIST. This initiative involved the conversion of security controls from NIST Special Publication (SP) 800-53 Revision 2 to the required NIST SP 800-53 Revision 3 security control sets for all assessments and authorizations of USDA information systems.

- Review all information with agencies to improve accuracy of the information in CSAM for all FISMA reportable systems.
- Improve CSAM tool utilization to 100 percent for all USDA agencies and offices (up from 75 percent of re-authorizations in 2010) improving the efficiency of all other Department functions which rely on the currency and accuracy of this information.
- Finished the conversion of over 94 percent of the Department's 661 operational systems to the NIST 800-53 revision 3 control set completing the automation into CSAM.

Governance, Risk and Compliance: Developed and implemented a new concurrency review process that:

- Contained detailed checklists for all products produced during the USDA NIST 6 step RMF process.
- Made mandatory a concurrency review and remediation of all findings prior to completion of the process.
- Provided training to the agencies on the concurrency review process.
- Performed 433 concurrency reviews of systems after Security Assessments was complete on 100 percent of all FISMA reportable systems due in 2011 resulting in 13,374 items requiring remediation. Remediation of all findings was required before Authority to Operate was allowed to be issued on all 2011 systems.
- Developed and distributed a new Performance Work Statement (PWS), enforcing compliance to the USDA RMF process and requiring training of all contractors before starting work as of Q1 2012.
- Coordinated all OCIO activity to respond to request for information during OIG and GSA IT Security Audits. In 2011 four audits were conducted (GAO: Social Media in the Federal Government and Security over Wireless devices; OIG: Security and Management of Wireless Devices and FISMA.)
- In 2011, OCIO reached Management Decision on 33 IT security recommendations from the 2009 and 2010 FISMA OIG Audits. Subsequently OCIO achieved final action on eight of these recommendations in 2011.

Plans of Actions and Milestones (POA&Ms): Developed a new POA&M process that:

- Provided detailed procedures for field usage publishing the guide on the CPO's cyber security web site.
- Worked with the field on all 2011 POA&Ms improving the goals, milestones and cost information.
- Conducted management review of all POA&M items instituted on a weekly basis
- Monitored the creation, inputs and actions for adjudication of 1,155 POA&Ms in 2011.
- Resulted in a closure of 360 (3190 percent) cleanup of all 2011 POA&M Items.
- Required milestones and cost estimates that provided the ability for improved oversight and financial accountability of all USDA systems. In 2011, CPO established several POA&M remediation efforts to improve the POA&M information provided by the agencies for each and every POA&M including, but not limited to:
    - Requiring more qualitative POA&M data including milestone dates to better manage POA&M remediation planning.
    - Requiring cost estimates to provide greater insight into the financial impacts of POA&M remediation, and greater oversight capabilities for CPO to assist agencies in considering requirements, prioritization and financial impacts of POA&M remediation planning efforts.

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, the ISA class was completely reorganized reducing the class length 40 percent, including USDA specific security items and added a pre-test. For 2011, over 99 percent of Agriculture personnel received security awareness and specialized security training. For 2012 CPO has adjusted the training to accommodate employees with disabilities.

ASOC Outreach: Developed an initial outreach strategy that will convey a consistent ASOC message to internal and external stakeholders through a professionally designed newsletter. Expanded and enhanced ASOC Communications and Outreach by creating and managing active security communities on USDA Connect to advance and support OCIO and ASOC security initiatives, and created and facilitated the ASOC Intranet web site project team to improve and enhance ASOC's presence on the OCIO intranet web site.

- ASOC created and implemented a strategy targeting colleges and universities across the country, including African American, Native American, Hispanic and other minority serving universities. This strategy was in keeping with Cultural Transformation and commitment to diversity expressed by Secretary Vilsack. ASOC launched the USDA-Academy portal in Oct 2010 and refreshed the content in Sept 2011. Developed creative ad campaigns, brochures, banners, desktop banners and draft magazine. Also began outreach to local high schools that have a curriculum emphasis on IT to recruit students for summer employment at OCIO.

- Established an external communication plan with the USDA Office of Communications to respond to media inquiries regarding privacy incidents. The results of this plan will ensure USDA can respond immediately regarding incidents that have made national attention. Developed a brochure to showcase the mission and services provided by the ASOC.

- Led the design and development of the ASOC Software Update Notice (or SUN), which identifies software at risk, gives agencies direction, guidance and/or recommended actions for reducing the risk, and provides information supporting the actions, such as, ASOC incident and threat analysis, vendor software support and maintenance information, vendor security bulletins/advisories, and applicable FISMA and/or OMB policy and NIST guidance. Three SUNs were released since its inception in June 2011.

- Led the design and development of the ASOC Situational Awareness Report (or ASAR) that informs agencies on the appropriate and necessary actions to take to reduce risks posed by new or emerging threats, focusing on those threats that have had, or are more likely to have, an impact on USDA Agencies and Offices. Five ASARs were released since its inception in June 2011.

Data Center Consolidation Initiative (DCCI): Facilitate USDA agencies transition to the NITC enterprise data center; NITC is on track to close 23 data centers/computer rooms by year end. As part of the process, NITC fostered key communications with customers to drive planning, preparation, and migration of customer business applications into data center cloud service offerings in support of DCCI milestone dates. The DCCI initiative through virtualization of applications and consolidation of data centers also contributes to the "greening" of USDA by reducing energy consumption by 50 percent over the next 5 years.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Statement of Agency Goals and Objectives

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.

The OCIO has five strategic goals and twenty objectives that contribute to all of the Department Strategic goals and objectives

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
OCIO supports all USDA strategic goals.	Support all USDA Strategic priorities and initiatives by ensuring all technology investments are mission-focused and business driven.	Ensure the culture and organization focuses on the customer's mission and provides technology solutions to enable the business needs of today and tomorrow. Improve the IT service delivery and operating model to enable a cohesive and cost-effective, one-stop-shop of service offerings. Utilize portfolio management and enterprise architecture practices for driving investment decisions to address mission needs in a cost effective manner. Ensure IT investments are aligned to mission and business goals and the performance line-of-sight is clear and traceable throughout the lifecycle of an investment.	Technology Planning, Architecture and E-Government Architecture and Systems Integration Division Cyber Policy and Oversight Customer and Program Management	1: Better managed IT investment portfolio—improved data quality, and overall improved management of IT investments. 2: Improved CPIC process that measures the alignment and traceability between the Exhibits 300s and 53s and the Enterprise Architecture Transition Plan (EATP). 3: Alignment of IT investment with mission priorities and business goals. 4: SSN/TINs eliminated from USDA system.

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
OCIO supports all USDA strategic goals.	Establish a business-driven, unified architecture to create a more effective data and technical infrastructure that addresses business and technology needs.	Ensure the foundational enterprise architecture is mission-focused/business-driven and agile enough to address new business and technology needs. Leverage enterprise and cloud-based investments wherever possible to enable flexible and scalable solutions that minimize cost and risk. Enhance information sharing across USDA through improved data definitions, standards, and governance and supporting technology solutions that enable interconnectivity. Ensure that all USDA users have the same level of connectivity, service, and experience regardless of where they are or what technology they are using.	Technology Planning, Architecture and E-Government Architecture and Systems Integration Division Cyber Policy and Oversight	5: Increase in the number of projects using standardized and enterprise solutions and services. 6: Increase in the number of IT investments aligned with Enterprise Architecture. 7: High-level of customer satisfaction of services and solutions. 8: Reduced number of non-EDC computer facilities.

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
OCIO supports all USDA strategic goals.	Ensure technology resources are effectively and efficiently managed from planning to operations with informed oversight and accountability.	Optimize tax-payer dollars by ensuring IT investments meet mission needs and leverage enterprise-wide contracts and repeatable processes and solutions wherever possible. Increase oversight and accountability across the IT lifecycle through improved governance and project management to ensure IT investments deliver planned objectives in a timely manner. Enhance transparency into the status of IT investments by implementing standardized measurements that are aligned with business and technology objectives. Reduce the carbon footprint of USDA by adopting proven, energy efficient technology solutions and utilizing telework and telepresence capabilities.	Customer and Program Management Technology Planning, Architecture and E-Government Architecture and Systems Integration Division	9: Poorly performing investments (programs or projects) are turned around or terminated. 10: Improved management of major IT investments by Senior Management Oversight Committee. 11: Improved IT Governance, Program and Portfolio Management. 12: Reduced steady state spending.

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
OCIO supports all USDA strategic goals.	Create a proactive and robust security environment through actionable insight by integrating security policy and operations to continuously monitor and protect information assets.	Protect USDA business and technology assets through rigorous and adaptive monitoring, management, controls, and solutions. Push security and privacy assessments to the forefront of the technology investment cycle to proactively identify risks and threats. Streamline and align security policies and procedures to USDA's core planning and service delivery processes to promote security as an ingrained aspect of USDA's culture. Align and integrate USDA's enterprise architecture, operational risk, and security policies, objectives, and controls to improve the security posture.	Cyber Policy and Oversight Agriculture Security Operations Center	13: Modernize and streamline the security assessment process shifting the paradigm to continuous monitoring. 14: Percentage of Completed Plan of Actions & Milestones (POA&M) – measures the number of security issues identified and remediated in an effective manner.

USDA Strategic Goal	Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
OCIO supports all USDA strategic goals.	Position USDA as a Federal Government leader in the human capital and workplace environment by fostering a flexible, empowered, collaborative, and innovative workforce.	Increase Department-wide knowledge transfer and sharing of best practices by capturing and disseminating institutional knowledge in a standardized manner. Institutionalize an innovative workforce, environment and culture through fostering collaboration and rewarding creative solutions. Institute formal succession planning policies, procedures, training, and hiring so that continuity of operations and services are maintained. Rebalance and retool the USDA IT workforce by actively developing the skills of existing employees and managing the integration of new employees.	Innovations and Emerging Technologies Division AgLearn Information Security Intern Program Technology Planning, Architecture, E-Gov	15: Role Descriptions Documented – measures the number of technology positions that have detailed descriptions of roles, responsibilities, and procedures. 16: An IT Program Management Career Field with formal training program and curriculum. 17: Pipeline of trained leaders and IT Program Managers. 18: Proper balance of blended workforce.

Selected Accomplishments Expected for the 2013 Proposed Resource Level:

- An integrated Capital Planning Process with the Budget, program management, Enterprise Architecture, and Security Process managed as an overall IT Governance Process.
- The majority of USDA agencies on-line services will be integrated with USDA's enterprise eAuthentication Services.
- The majority of the USDA agencies will have integrated email services with USDA's enterprise messaging service.
- USDA agencies will continue integrating applicable agency systems with USDA's enterprise ICAM Program Service.
- Continue on-going Certification and Accreditation (C&A) process for all new and continuing systems in USDA's inventory.
- Complete comprehensive assessment of all USDA systems NIST 800-53 Revision 3 controls.
- Provide Information Security Awareness Training to 100% of USDA personnel.
- Complete remediation of weaknesses identified during comprehensive assessments of security controls at the rate of 30 percent each year.
- Continue implementation of initiatives to improve FISMA compliance and mitigate the IT Material Weakness.
- OCIO will provide Earned Value Management (EVM) training and other project management training.
- OCIO will ensure that actual performance data is being tracked for all IT investments that meet USDA's EVM threshold by monitoring agency updates to the Capital Planning Investment Repository (CIMR) to. 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.
- OCIO will monitor agency EVM process maturity.
- OCIO will monitor IT investments to improve the quality of the business cases.
- 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).
- Provide real-time asset tracking and inventory data through enterprise deployment of BigFix™ software.
- OCIO will continue to 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. OCIO will develop detailed agency profiles.
- 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 Power Utilization Efficiency (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 2012.
- Manage a USDA wide enterprise scanning tool which will allow the USDA to perform IT vulnerability scans on all assets that are connected to the USDA networks. The benefits of having this enterprise scanning application in place to gain immediate insight into the risk posture of each agency security environment by continuously discovering physical and virtual assets. An enterprise vulnerability assessment and remediation management solution will enable IT and security groups to implement an integrated and centralized approach to vulnerability management.
- OCIO will manage the Washington DC Security Sensor Array in an inline security posture in 2013. This architecture will allow the ASOC the ability to activity block malicious activity before it is allowed to enter the USDA Enterprise computing environment.
- OCIO will deploy an Enterprise Records Management Environment based on Department of Defense 5015.02-STD.
- OCIO will establish a Section 508 Center of Excellence, to deliver Enterprise Solutions to check websites, documents, and training materials for accessibility.

- OCIO will develop a USDA true testing facility for Accessibility & Section 508 compliance.
- OCIO will maximize the value of the Department's participation in E-Government and Open Government Initiatives by measuring, analyzing, an evaluating the spending levels and benefits generated by the E-Gov initiatives and lines of business.

Strategic Goal Funding Matrix
(Dollars in thousands)

Program / Program Items	2010 Actual	2011 Actual	2012 Estimate	Change	2013 Estimate
Agency Strategic Goal 1: Support all USDA Strategic priorities and initiatives by ensuring all technology investments are mission-focused and business driven.					
Office of the Chief Information Officer.....	$6,246	$4,068	$4,494	-	$4,494
Staff Years.....	20	20	22	-	22
Agency Strategic Goal 2: Establish a business-driven, unified architecture to create a more effective data and technical infrastructure that addresses business and technology needs.					
Office of the Chief Information Officer.....	6,246	4,068	4,494	-	4,494
Staff Years.....	22	22	24	-	24
Agency Strategic Goal 3: Ensure technology resources are effectively and efficiently managed from planning to operations with informed oversight and accountability.					
Office of the Chief Information Officer.....	5,267	3,430	3,790	-	3,790
Staff Years.....	8	8	9	-	9
Agency Strategic Goal 4: Create a proactive and robust security environment through actionable insight by integrating security policy and operations to continuously monitor and protect information assets.					
Office of the Chief Information Officer.....	37,443	24,388	26,963	-	26,963
Staff Years.....	21	39	47	-	47
Agency Strategic Goal 5: Position USDA as a Federal Government leader in the human capital and workplace environment by fostering a flexible, empowered, collaborative, and innovative workforce.					
Office of the Chief Information Officer.....	5,960	3,883	4,290	-	4,290
Staff Years.....	8	8	10	-	10
Total Costs, All Strategic Goals.....	61,162	39,837	44,031	-	44,031
Total FTEs, All Strategic Goals.....	79	97	112	-	112

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Key Performance Outcomes and Measures

Agency Strategic Goal 1: Support all USDA Strategic priorities and initiatives by ensuring all technology investments are mission-focused and business driven.

Key Outcome 1: Better managed IT investment portfolio—improved data quality, and overall improved management of IT investments
Key Outcome 2: Improved CPIC process that measures the alignment and traceability between the Exhibits 300s and 53s and the Enterprise Architecture Transition Plan (EATP).
Key Outcome 3: Alignment of IT investment with mission priorities and business goals.
Key Outcome 4: SSN/TINs eliminated from USDA system.

Key Performance Measure: Percent of SSN/TINs eliminated from USDA systems.

Agency Strategic Goal 2: Establish a business-driven, unified architecture to create a more effective data and technical infrastructure that addresses business and technology needs.

Key Outcome 5: Increase in the number of projects using standardized and enterprise solutions and services.
Key Outcome 6: Increase in the number of IT investments aligned with Enterprise Architecture.
Key Outcome 7: High-level of customer satisfaction with services and solutions.
Key Outcome 8: Reduced number of non-EDC computer facilities.

Key Performance Measure: Number of non-EDC computer facilities

Agency Strategic Goal 3: Ensure technology resources are effectively and efficiently managed from planning to operations with informed oversight and accountability.

Key Outcome 9: Poorly performing investments (programs or projects) are turned around or terminated.
Key Outcome 10: Improved management of major IT modernization investments by Senior Management Oversight Committee (SMOC).
Key Outcome 11: Improved IT Governance, Program and Portfolio Management.
Key Outcome 12: Reduced steady state spending.

Key Performance Measure: Percent of incidents managed through the Case Management tracking tool across the USDA Enterprise.

Agency Strategic Goal 4: Create a proactive and robust security environment through actionable insight by integrating security policy and operations to continuously monitor and protect information assets.

Key Outcome 13: Modernize and streamline the security assessment process shifting the paradigm to continuous monitoring.
Key Outcome 14: Increased Completed Plan of Actions & Milestones (POA&M) – measures the number of security issues identified and remediated in an effective manner.

Key Performance Measures:

- Measure #1: Percentage of systems tested using 800-53 rev. 3 security controls.
- Measure #2: Number of program security reviews completed.
- Measure #3: Number of General Support Systems inventoried, base lined, and assessed.
- Measure #4: Percent of ASOC incident report calls that are answered live by an incident handler.
- Measure #5: Percent of security incidents closed within 30 days.

- Measure #6: Percent of all incidents following USDA Security Incident processes and procedures to the designated authorities.

Agency Strategic Goal 5: Position USDA as a Federal Government leader in the human capital and workplace environment by fostering a flexible, empowered, collaborative, and innovative workforce.

Key Outcome 15: Role Descriptions Documented – measures the number of technology position that have detailed descriptions of roles, responsibilities, and procedures.
Key Outcome 16: IT Program Management Career Field with formal training program and curriculum.
Key Outcome 17: Pipeline of trained leaders and IT Program Managers.
Key Outcome 18: Proper balance of blended workforce.

Key Performance Measure: Percent of eligible employees approved to telework.

Key Performance Targets:

Performance Measure	2007 Actual	2008 Actual	2009 Actual	2010 Actual	2011 Actual	2012 Target	2013 Target
Performance Measure #1 Percent of SSN/TINs eliminated from USDA systems.							
a. Units	N/A	N/A	N/A	N/A	N/A	85%	85%
b. Dollars (in thousands)	$7,155	$7,741	$8,328	$6,246	$4,068	$4,494	$4,494
Performance Measure #2 The number of non-Enterprise Data Center (EDC) computer facilities.							
a. Units	97	97	97	97	74	41	33
b. Dollars (in thousands)	$5,103	$4,676	$5,030	$6,246	$4,068	$4,494	$4,494
Performance Measure #3 Percent of incidents managed through the Case Management tracking tool across the USDA Enterprise.							
a. Units	N/A	N/A	N/A	N/A	Est. baseline	10%	50%
b. Dollars (in thousands)	N/A	N/A	N/A	$5,267	$3,430	$3,790	$3,790
Performance Measure #4 Percent of systems tested using 800-53 rev. 3 security controls.							
a. Units	N/A	N/A	N/A	N/A	N/A	90%	95%
Number of program security reviews completed.							
a. Units	N/A	N/A	N/A	N/A	8	24	24
Number of General Support Systems inventoried, base lined, and assessed.							
a. Units	N/A	N/A	N/A	N/A	Est. baseline	99%	99%
Percent of ASOC incident report calls that are answered live by an incident handler.							
a. Units	N/A	N/A	N/A	N/A	Est. baseline	80%	80%

Performance Measure	2007 Actual	2008 Actual	2009 Actual	2010 Actual	2011 Actual	2012 Target	2013 Target
Percent of security incidents closed within 30 days.							
a. Units	N/A	N/A	N/A	Est. baseline	90%	90%	90%
Percent of all incidents following USDA Security Incident processes and procedures to the designated authorities.							
a. Units	N/A	N/A	N/A	N/A	90%	90%	90%
b. Dollars (in thousands)	$3,987	$3,700	$3,981	$37,443	$24,388	$26,963	$26,963
Performance Measure #5 Percent of eligible employees approved to telework.							
a. Units	N/A	N/A	N/A	N/A	67%	73%	78%
b. Dollars (in thousands)	N/A	N/A	N/A	$5,960	$3,883	$4,290	$4,290

Full Cost by Agency Strategic Goal

(Dollars in thousands)

Program / Program Items	2010 Actual	2011 Actual	2012 Estimate	2013 Estimate
Agency Strategic Goal 1: Support all USDA Strategic priorities and initiatives by ensuring all technology investments are mission-focused and business driven.				
Administrative costs (direct)	$5,177	$2,676	$3,048	$3,002
Indirect costs	1,069	1,392	1,446	1,492
Total Costs	6,246	4,068	4,494	4,494
FTEs	20	20	22	22
Performance Measure:				
Percent of SSN/TINs eliminated from USDA systems.				
Measure	N/A	N/A	100%	100%
Agency Strategic Goal 2: Establish a business-driven, unified architecture to create a more effective data and technical infrastructure that addresses business and technology needs.				
Administrative costs (direct)	$5,177	$2,676	$3,048	$3,002
Indirect costs	1,069	1,392	1,446	1,492
Total Costs	6,246	4,068	4,494	4,494
FTEs	22	22	24	24
Performance Measure:				
Number of non-Enterprise Data Center computer facilities.				
Measure	81	74	41	33
Agency Strategic Goal 3: Ensure technology resources are effectively and efficiently managed from planning to operations with informed oversight and accountability.				
Administrative costs (direct)	$4,366	$2,257	$2,570	$2,532
Indirect costs	901	1,173	1,220	1,258
Total Costs	5,267	3,430	3,790	3,790
FTEs	8	8	9	9

Performance Measure:				
Percent of incidents managed through the Case Management tracking tool across the USDA-wide enterprise.				
Measure	N/A	Est. baseline	10%	50%

Agency Strategic Goal 4: Create a proactive and robust security environment through actionable insight by integrating security policy and operations to continuously monitor and protect information assets.

Administrative costs (direct)	$31,034	$16,043	$18,273	$17,999
Indirect costs	6,409	8,345	8,690	8,964
Total Costs	37,443	24,388	26,963	26,963
FTEs	21	39	47	47
Performance Measure:				
Percentage of systems tested using 800-56 rev. 3 security controls.				
Measure	N/A	N/A	90%	95%
Performance Measure:				
Number of program security reviews completed.				
Measure	8	24	24	24
Performance Measure:				
Percent of General Support Systems inventoried, base lined, and assessed.				
Measure	N/A	Est. baseline	99%	99%
Performance Measure:				
Percent of ASOC incidence report calls that are answered live by an incident handler.				
Measure	N/A	Est. baseline	80%	80%
Performance Measure:				
Percent of security incidents closed within 30 days.				
Measure	N/A	Est. baseline	90%	90%
Performance Measure:				
Percent of all incidents following USDA Security Incident processes and procedures to the designated authorities.				
Measure	N/A	N/A	90%	90%

Agency Strategic Goal 5: Position USDA as a Federal Government leader in the human capital and workplace environment by fostering a flexible, empowered, collaborative, and innovative workforce.

Administrative costs (direct)	$4,941	$2,554	$2,909	$2,865
Indirect costs	1,019	1,329	1,381	1,425
Total Costs	5,960	3,883	4,290	4,290
FTEs	8	8	10	10
Performance Measure:				
Percent of eligible employees approved for telework.				
Measure	N/A	67%	73%	78%
Total Costs, All Strategic Goals	61,162	39,837	44,031	44,031
Total FTEs, All Strategic Goals	79	97	112	112