2014 Explanatory Notes

Departmental Management

Office of the Chief Information Officer

Contents

Purpose Statement 7-1
Statement of Available Funds and Staff Years 7-4
Permanent Positions by Grade and Staff Year Summary 7-5
Motor Vehicle Fleet Data 7-6
Salaries and Expenses
- Appropriations Language 7-8
- Lead-off Tabular Statement 7-8
- Project Statement 7-8
- Justifications 7-9
- Geographic Breakdown of Obligations and Staff Years 7-10
- Classification by Objects 7-11
- Status of Programs 7-12

Summary of Budget and Performance
- Statement of Goals and Objectives 7-25
- Full Cost by Strategic Objective 7-35

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.

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, 2012, there were 983 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. (1/23/13) Final Action received on 8 recommendations. OCIO is currently in the process of preparing documentation to request Final Action on 1 recommendation.
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. (1/23/13) Final Action received on 6 additional recommendations making the total 11. OCIO is currently in the process of preparing documentation to request Final Action on 5 more recommendations.

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. (1/23/13) Revised request for Management Decision in clearance through ACIO to CIO for signature. Remediation actions underway and OCIO is currently in the process of preparing documentation to request Final Action on 2 recommendations.
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. (1/23/13) One recommendation is closed. Remediation actions still underway and OCIO is in the process of documenting remediation actions status.
50501-0003-12	11/2012	Fiscal Year 2012 Federal Information Security Management Act Report - This audit contained 6 recommendations. ACIO stakeholders are reviewing recommendations and preparing Request for Management Decision.

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 Progress

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. 1/22/2013 – The Whole Disk Encryption (WDE) System remains fully operational. There are 18 USDA Agencies and over 82,000 devices currently using the system. Risk Management Agency (RMA) has migrated completely off the system and is using other technologies. Agriculture Marketing Service (AMS) and International Technology Services (ITS) are in the process of migrating off the MEE solution to other technologies. (1/23/13) ACIO ASOC/CISO is in process of gathering documentation to provide to GAO to substantiate completion/progress on mitigation activities.
GAO-10-202	3/2010	Federal Information Security Initiatives, FDCC/TIC/Einstein USDA responded to the Draft report in 2009. GAO had NO recommendations for USDA in the final report to Congress. Therefore, no further action is required by USDA.
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. No updates in 2012.
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. (1/23/13) GAO has not requested further information from USDA on this audit.
GAO-11-565	7/2011	Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings – USDA provided an updated inventory and data center consolidation plan to OMB addressing all findings in September 2011. Follow-on audit (GAO-12-742) of the same title recommended further actions related to inventories and plans (See GAO Report GAO-12-742, dated July 19, 2012). USDA submitted all recommended changes contained in the GAO-12-742 report to OMB on 9/27/12.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Available Funds and Staff Years (SY)
(Dollars in thousands)

Item	2011 Actual		2012 Actual		2013 Estimate		2014 Estimate	
	Amount	SY	Amount	SY	Amount	SY	Amount	SY
Salaries and Expenses:								
Discretionary Appropriation	$40,000	97	$44,031	102	$44,300	112	$44,159	116
Rescission	-80	-	-	-	-	-	-	-
Total Available	39,920	97	44,031	102	44,300	112	44,159	116
Lapsing Balances	-83	-	-34	-	-	-	-	-
Obligations	39,837	97	43,997	102	44,300	112	44,159	116
Obligations under other USDA appropriations:								
Reimbursements:								
Innovation & Emerging Architecture	630	-	400	-	420	-	420	-
CSAM	-	-	-	-	-	-	-	-
CPIC	130	-	-	-	-	-	-	-
Geospatial IS	8,330	-	8,330	-	8,745	-	8,745	-
Project Management	95	-	-	-	-	-	-	-
NTIA Spectrum	1,756	-	1,715	-	1,800	-	1,800	-
Decision Lens	275	-	-	-	-	-	-	-
Contract Management	1,315	-	1,350	-	1,415	-	1,415	-
CPO	159	-	-	-	-	-	-	-
LincPass	231	-	-	-	-	-	-	-
Other Activities	361	-	425	-	445	-	445	-
Total, Agriculture Appropriations	13,282	-	12,220	-	12,825	-	12,825	-
Working Capital Fund: a/								
Information Technology	398,728	891	379,500	827	365,129	827	397,891	874
NITC (Non-USDA)	15,477	35	10,445	38	14,313	38	15,642	38
WCF Management Fee	-	-	-	2	-	2	-	2
Capital Equipment	11,360	-	2,356	-	3,600	-	3,000	-
Total, WCF	425,565	926	392,301	867	383,042	867	416,533	914
Total, OCIO	478,684	1,023	448,518	969	440,167	979	473,517	1,030

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

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Permanent Positions by Grade and Staff Year Summary a/

Item	2011 Actual			2012 Actual			2013 Estimate			2014 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.....	15	2	17	18	2	20	18	2	20	18	2	20
GS-14.....	38	4	42	34	8	42	34	8	42	34	8	42
GS-13.....	18	5	23	13	6	19	13	6	19	14	6	20
GS-12.....	7	3	10	5	3	8	5	3	8	6	3	9
GS-11.....	4	-	4	5	-	5	5	-	5	7	-	7
GS-10.....	1	-	1	1	-	1	1	-	1	1	-	1
GS-9.....	3	-	3	-	-	-	-	-	-	-	-	-
GS-8.....	3	-	3	2	-	2	2	-	2	2	-	2
GS-7.....	2	-	2	2	-	2	2	-	2	2	-	2
GS-5.....	-	-	-	1	-	1	1	-	1	1	-	1
GS-4.....	1	-	1	5	1	6	5	1	6	5	1	6
Total Perm. Positions.....	98	14	112	92	20	112	92	20	112	96	20	116
Unfilled, EOY	15	-	15	3	-	10	-	-	-	-	-	-
Total, Perm. Full-Time Employment, EOY.....	83	14	97	89	20	102	92	20	112	96	20	116
Staff Year Est.....	83	14	97	92	20	102	92	20	112	96	20	116

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

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

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

SIZE, COMPOSITION AND COST OF MOTOR VEHICLE FLEET

The 2014 budget proposes to lease 11 additional vehicles.

OCIO-International Technology Services (ITS) is the in-house provider of information technology service and support for over 45,000 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. 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 no longer has agency owned vehicles. All vehicles are leased through GSA. Recently, OCIO added 11 additional GSA leased vehicles because the SCAs no longer allow Technical Services Division (TSD) staff to use the agency vehicles. With the recent budget situation, agencies are scaling back their fleet and reviewing ways to cut maintenance and fuel cost. As a result, some SCA locations have notified TSD Group Managers that TSD staff can no longer use their fleet. This has caused scheduling problems which ultimately impact customer service and ITS' ability to meet our Service Level Agreements.

OCIO's current fleet is based on mission and geographic needs. As of September 30, 2012, ITS' has 236 leased GSA vehicles and NITC has two leased GSA vehicles. ITS' 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 2014.

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, 2012, 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	4 X 4						
*2009	120	90	10	0	0	0	0	220	$500
Change	-24	**+20	+9	0	0	0	0	+5	+ $495
2010	96	110	19	0	0	0	0	225	***$995
Change	+20	-19	1	0	0	0	0	+2	+$3
2011	116	91	20	0	0	0	0	227	$998
Change	0	0	0	0	0	0	0	0	0
2012	116	91	20	0	0	0	0	227	$998
Change	0	0	0	0	0	0	0	0	0
2013	116	91	20	0	0	0	0	227	$998
Change	+10	+1	0	0	0	0	0	+11	+$27
2014	126	92	20	0	0	0	0	238	$1,025

*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:

Salaries and Expenses:
For necessary expenses of the Office of the Chief Information Officer, $44,159,000.

Lead-off Tabular Statement

2013 Estimate	$44,300,000
Budget Estimate, 2014	44,159,000
Change in Appropriation	-141,000

Summary of Increases and Decreases
(Dollars in thousands)

	2011 Actual	2012 Change	2013 Change	2014 Change	2014 Estimate
Discretionary Appropriations:					
Office of the Chief Information Officer	$39,920	+$4,111	+$269	-$141	$44,159

Project Statement
Adjusted Appropriations Detail and Staff Years (SY)
(Dollars in thousands)

Program	2011 Actual		2012 Actual		2013 Estimate		Inc. or Dec.		2014 Estimate	
	Amount	SY	Amount	SY	Amount	SY	Amount	SY	Amount	SY
Discretionary Appropriations:										
Office of the Chief Information Officer	$39,920	97	$44,031	102	$44,300	112	-$141 (1)	+4	$44,159	116
Rescission and Transfer (Net)	80	-	-	-	-	-	-	-	-	-
Total Appropriation	40,000	97	44,031	102	44,300	112	-141	+4	44,159	116
Rescission	-80	-	-	-	-	-	-	-	-	-
Total Available	39,920	97	44,031	102	44,300	112	-141	+4	44,159	116
Lapsing Balances	-83	-	-34	-	-	-	-	-	-	-
Total Obligations	39,837	97	43,997	102	44,300	112	-141	+4	44,159	116

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Project Statement
Obligations Detail and Staff Years (SY)
(Dollars in thousands)

Program	2011 Actual		2012 Actual		2013 Estimate		Inc. or Dec.		2014 Estimate	
	Amount	SY	Amount	SY	Amount	SY	Amount	SY	Amount	SY
Discretionary Obligations:										
Office of the Chief Information Officer	$39,837	97	$43,997	102	$44,300	112	-$141 (1)	+4	$44,159	116
Total Obligations	39,837	97	43,997	102	44,300	112	-141	+4	44,159	116
Lapsing Balances	83	-	34	-	-	-	-	-	-	-
Total Available	39,920	97	44,031	102	44,300	112	-141	+4	44,159	116
Rescission	80	-	-	-	-	-	-	-	-	-
Total Appropriation	40,000	97	44,031	102	44,300	112	-141	+4	44,159	116

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) A net decrease of $141,000 and an increase of 4 staff years for the Office of the Chief Information Officer ($44,300,000 and 112 staff years available in 2013).

(a) An increase of $128,000 for pay costs ($21,000 for annualization of the 2013 pay increase and $107,000 for the 2014 pay increase).
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) An increase of $480,000 to fund 4 additional staff years.
The proposed funding level is needed to cover pay and benefits for 4 Strategic Sourcing Coordination staff. USDA has been reviewing strategic sourcing initiatives for the last several years and has accomplished several efforts that saved the Department over $35 million. In addition, by improving the Departments email functionality USDA will see a yearly savings of $6 million. As a result of these successes, the USDA has decided to establish a formal, dedicated Strategic Sourcing Team. The team will be responsible for analyzing IT spending and commodity inventories for strategic sourcing opportunities, performing market research to determine acquisition strategies and managing vendor relationships. This additional funding will ensure adequate resources are available to continue to allow the office to carry out its full range of responsibilities and support program delivery.

(c) An increase of $348,000 to fund advisory and assistance services.
The IT redirected funds will be used to acquire advisory and assistance services to conduct a telecommunications infrastructure assessment to examine the consolidation of agency virtual private networks as well as future architecture requirements to deliver enterprise-level services; i.e. data centers,

expanding cloud services, MIDAS, and Geospatial. The network infrastructure is a critical foundational element in our information technology infrastructure.

(d) A decrease of $149,000 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 and IT.

(e) A decrease of $250,000 from Technology, Planning, Architecture and E-Gov Service Contracts program/activity to fund the IT redirection.
OCIO reduced contract costs by renegotiating and federalized positions further saving on contract dollars. The reduction in funding reflects the redirection of funds to IT advisory and assistance services.

(f) A decrease of $557,000 from Agriculture Security Operations Center program/activity to fund the IT redirection and the additional 4 staff years.
OCIO merged several contract services under one contract, reduced other contract costs by renegotiating and federalized positions further saving funding. The reduction in funding reflects the redirection of funds to the 4 additional staff years for the Strategic Sourcing Coordination and the IT advisory and assistance services.

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

State/Territory	2011 Actual		2012 Actual		2013 Estimate		2014 Estimate	
	Amount	SY	Amount	SY	Amount	SY	Amount	SY
District of Columbia.....	$38,124	73	$41,648	82	$41,928	92	$41,763	96
Kansas City, MO.....	1,713	6	2,349	20	2,372	20	2,396	20
Obligations.....	39,837	79	43,997	102	44,300	112	44,159	116
Lapsing Balances.....	83	-	34	-	-	-	-	-
Total, Available.....	39,920	79	44,031	102	44,300	112	44,159	116

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects
(Dollars in thousands)

		2011 Actual	2012 Actual	2013 Estimate	2014 Estimate
Personnel Compensation:					
Washington D.C.		$9,547	$9,796	$11,017	$11,648
Kansas City, MO		1,348	1,850	1,869	1,888
11	Total personnel compensation	10,895	11,646	12,886	13,536
12	Personal benefits	2,736	3,094	3,347	3,571
13.0	Benefits for former personnel	-	102	-	-
	Total, personnel comp. and benefits	13,631	14,842	16,233	17,107
Other Objects:					
21.0	Travel and transportation of persons	217	160	210	214
22.0	Transportation of things	2	38	45	45
23.3	Communications, utilities, and misc. charges	731	681	750	754
24.0	Printing and reproduction	63	147	151	153
25.2	Other services from non-Federal sources	18,966	13,697	11,913	10,868
25.3	Other purchases of goods and services from Federal sources	6,011	13,940	14,448	14,454
26.0	Supplies and materials	83	394	400	404
31.0	Equipment	133	98	150	160
	Total, Other Objects	26,206	29,155	28,067	27,052
99.9	Total, New Obligations	39,837	43,997	44,300	44,159
Position Data:					
Average Salary (dollars), ES Position		$160,182	$165,913	$166,000	$170,000
Average Salary (dollars), GS Position		$107,646	$108,679	$112,170	$113,782
Average Grade, GS Position		13.8	13.8	13.9	13.9

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. Participation in these services is strong, with USDA agencies actively involved in the Enterprise-wide shared services: USDA's eAuthentication Service, AgLearn, Enterprise Correspondence Management Modules, the Enterprise Architecture Repository (EAR), capital planning investment tools, and Enterprise IT Solutions. The Enterprise IT Solutions introduced new Cloud services, offered internal and external services (Infrastructure as a Service, Platform as a Service, and Managed Hosting), and utilized "green" industry best practices. For example, there are more than 125,000 active AgLearn accounts across USDA, and in 2012 these users completed about one million training events, online courses, and webinars. 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 23 E-Government Initiatives and Lines of Business (LoB). USDA is an active participant in the development of a government-wide infrastructure to support Homeland Security Presidential Directive 12 (HSPD-12). Participation includes active engagement with other Federal Agencies including GSA and the U. S. Postal Service on government-wide HSPD-12 related initiatives. Additionally USDA is making significant progress in implementing continuity of operations communications capabilities to meet the requirements of the National Communications System Directive 3-10 (NCSD 3-10).

USDA Office of the Chief Information Officer (OCIO) will provided in 2013 an estimated $9,489,426 to fund 12 of the 23 E-Government activities in which USDA participates. Of the 12 activities, seven are E-Government Initiatives and five are E-Government Lines of Business (LoB) (see table below). 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.

OCIO-Funded E-Government Presidential Initiatives and Lines of Business	
Initiatives	**Lines of Business (LoB)**
Disaster Assistance Improvement Plan	Budget Formulation and Execution LoB
Enterprise Human Resources Integration (EHRI)	Financial Management LoB
E-Rulemaking	Geospatial LoB
E-Training	Human Resources Management LoB
Benefits.gov	Grants Management LoB
Integrated Acquisitions Environment (IAE)	
Integrated Acquisitions Environment (IAE) – Loans and Grants	

Enterprise Architecture: Enterprise Architecture is a process of translating business vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future state and enable its evolution. 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 and 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. At the center of the USDA EA knowledge base is the (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 business process owners, strategic planners, enterprise architects, program managers, project managers, vendors, budget officers, investment decision-makers, acquisition personnel, developers, and security personnel.

2013 EA activities include:

- Refinement of the USDA technology standards;
- Participation in Open Government and Data.Gov Initiatives—increasing the publication of USDA data on the Data.gov website;
- Update the EA Roadmap;
- Continue development of executive and management reports, and dashboards;
- Update EA Guiding Principles;
- Integrate EA into the Enterprise IT Governance Process; and
- Development of a Security Architecture Blueprint.

Capital Planning and Investment Control (CPIC) and IT Governance: 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, IT budgeting, and performance management processes. 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.

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 2013, OCIO will continue with the many strides made in 2012 in improving IM across the Department, including promoting the 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 2012 OCIO processed over 170 information collections that allowed USDA agencies to collect information critical to continuing business operations and execute the mission. OCIO also processed over 40 Departmental directives, Departmental notices, and other policies. Additionally, OCIO developed the Department's first ever Controlled Unclassified Information implementation plan, and stood up a Department-wide Section 508 Center of Excellence.

Policy, Directives, and Strategic Planning: In 2012, the OCIO placed a new Lean Six Sigma (LSS) streamlined Departmental Directives approval process into effect, reducing the typical clearance process from 180 to a projected 32 business days. OCIO also processed over 85 Departmental Directives, Notices, and other policies. Over 30 new and revised IT directives are currently in development to address key policy gaps, audit recommendations, and OCIO management priorities. OCIO created a central repository, as an aid for IT program/project managers, of IT investment life cycle project management policies, deliverables templates, standards, and best practices.

In August 2012, the USDA Chief Information Officer convened a team to develop an Interim USDA IT Strategic Plan (2013-2014) to communicate immediate priorities, to provide continuity, and to lay a foundation for a long-term IT Strategic Plan. The development team has since expanded the scope of the plan to a 3 year long term strategic plan that aligns with the expiration date of the Department Strategic Plan in 2015. OCIO has developed the first draft of the Department's IT Strategic Plan (2013 – 2015) and it is anticipated to be vetted, approved and published by the end of March 2013.

Freedom of Information Act: In accordance with the Freedom of Information Act (FOIA) 5 U.S.C § 552, President Obama's FOIA memorandum and Attorney General Holder's FOIA guidelines, USDA must promptly disclose agency records to requesters unless withholding is permissible under one or more of the nine FOIA exemptions or three statutory exclusions. In 2012, OCIO's FOIA Service Center received 111 FOIA requests for internal review and processing. However, the FOIA Service Center processed a total number of 144 FOIA requests. The total number of FOIA requests processed included those received during the current fiscal year in addition to backlogged FOIA requests. Of the FOIA requests processed for which USDA had responsive records, more than half required FOIA Service Center staff to review 500 or more pages of responsive material. A large portion of the requests were granted in full.

In addition to reducing the backlog, OCIO's FOIA Service Center spearheaded multiple initiatives. On October 1, 2011, the FOIA Service Center implemented its first enterprise-wide tracking system in an effort to increase transparency, timeliness and the quality of FOIA responses. All USDA agency FOIA offices have some

form of access to this enterprise-wide tracking system. Agency FOIA offices at their discretion have elected to either use this tracking system throughout the agency or at specific levels.

In January 2012, OCIO's FOIA Service Center established a USDA-wide FOIA Council. The Council is composed of FOIA Officers and FOIA Specialists from each USDA FOIA office. The Council serves as a centralized forum for USDA's FOIA community to (a) streamline inter and intra agency FOIA operations; (b) strengthen USDA's FOIA regulations, policies and procedures; and (c) provide opportunities for FOIA related training for interested community members, agency directors and undersecretaries. The Council meets monthly. In addition to the FOIA Council, several subcommittees have been established to develop policies, procedures, and address specialize USDA FOIA processes. The subcommittees meet either weekly or bi-weekly.

Since its creation in early 2012, the FOIA Council has established a subcommittee to develop both a light and extended FOIA training module for use on the Department-wide system for managing training records and activity at USDA. A second subcommittee was created to review and revise the current USDA regulations. Both committees anticipate a completion date in 2013.

OCIO's FOIA Service Center also revamped the public facing USDA FOIA website. The website was streamlined and simplified. The website is user friendly and now allows the public to submit, track, and retrieve responsive records online. Since implementation in September 2012, 49 FOIA requests have been submitted online using the Public Access Link (PAL). USDA's newly revamped website can be found at http://www.dm.usda.gov/foia/index.htm.

With the deployment of the new USDA FOIA website, USDA also revamped its reading rooms based on its analysis and review of the July 2012 Government Accountability Office Report titled "Freedom of Information Act – Additional Actions Can Strengthen Agency Efforts to Improve Management" (GAO Report).

Finally, in late September 2012 OCIO awarded a contract to a legal research tool provider in an effort to assist USDA's FOIA professionals in referencing and resolving FOIA related legal issues. A total of fifty licenses were distributed to the USDA FOIA and Privacy Council members.

Privacy Act: 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 2012, the USDA Privacy office conducted numerous Privacy Threat Assessments (PTAs) and Privacy Impact Assessments (PIAs). In some cases an assessment and review of a single system proved some systems contain multiple FISMA children or system components. In these instances, multiple PIA and PTA documents were created to address the system and each of its system components. In one such case an agency elected to combine 28 child systems, components of a single system, under a single PIA. The Privacy Office also reviewed and processed System of Records Notices (SORNs) for USDA systems, assisted with 67 Personally Identifiable Information (PII) Incidents, and recorded 37 systems that removed SSN/TIN. Another 40 USDA systems containing SSN have been encrypted, and 44 systems containing SSN/TINs have been encrypted. The Privacy Office also implemented annual reviews and updates of agency privacy documentation. In 2008, USDA established a Privacy Council. Council members include a Senior Agency Official for Privacy (SOAP), USDA's Privacy Act Officer (PAO) and Agency Privacy Officers (APOs). The Council meets monthly and works collectively to facilitate and build a comprehensive Department-wide privacy program in addition to ensuring awareness of current Privacy issues. The Council also ensures compliance with applicable laws regulations, requirements and guidelines.

In 2012 the Privacy Council created the USDA National Institute of Standards and Technology (NIST) Standard Publication (SP) 800-53 Revision 4 Appendix J – Privacy Controls Subcommittee. The subcommittee meets on a monthly basis to review and research privacy controls as well as to ensure a parallel implementation with NIST. To

further its efforts, the Privacy Office also garnered a professional contact with a Senior Security Analyst at NIST. Tapping into extended resources will assist in strengthening USDA's privacy portfolio.

The Privacy Office has established weekly meetings with the PII Incident Manager to collaborate on PII incidents/events. These meetings assist with resolution and provide mitigation recommendations/suggestions, report reviews, and metrics for our monthly Privacy Council Meetings.

The Privacy Office drafted Information Sharing Environment (ISE) Privacy Policy in compliance with Executive Order 13388, October 25, 2005), "Further Strengthening the Sharing of Terrorism Information to Protect Americans," which mandates that in the course of operating within the ISE, agencies shall protect the privacy rights of Americans. Finalization of the policy will assist USDA in its facilitation of the National Strategic Initiative on Suspicious Activity Reporting.

The SSN/TIN Initiative for 2012, which complies with OMB M 07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information, yielded an approximately 88 percent compliance rate for USDA agencies. Several initiatives were implemented, including weekly contact with agencies, ensuring accountability by promoting Plan of Action and Milestones, incorporating a Memorandum for Compliance, and being available to assist agency's needs. With continuous monitoring and privacy consciousness, the USDA Privacy Office anticipates a 99 percent compliance rate.

In 2012, the Privacy Office implemented specialized privacy training for Privacy Officers and related disciplines, i.e. ISSPM, CISO, etc. The Privacy Office is currently modifying the training to a condensed light version that would be recommended for everyone within USDA. The extended training is currently being modified to include new test questions. As the light version is developed it will include similar questions. Education will strengthen the awareness of the privacy program.

The Privacy Office, in conjunction with Cyber Security, collects quarterly and annual metrics for Federal Information Security Management Act (FISMA) reporting to OMB. Metrics are collected for the SAOP report which identifies reviews mandated by the Privacy Act of 1974, e-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007. Quarterly and annual reports are submitted into Cyber Scope by the Cyber Security Audit Liaison. This reporting helps to analyze the current state of the privacy program.

Cyber Security: OCIO continues to operate its progressive strategy to improve USDA's information security via: 1) information security awareness training; and 2) revising and updating standardized computer security policies, processes and controls within the Department. The consolidation in 2012 of the Agriculture Security Operations Center (ASOC) and assessment and authorization program responsibilities has provided a unified approach for the integration of operational security management and oversight and compliance functions at USDA. We now can generate a common operating picture of the environment. OCIO has also re-constituted the role of Chief Information Security Officer (CISO) within ASOC.
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) Assessment and Authorization process 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 is underway synchronizing with newly issued Federal guidance.

OCIO is beginning to transition/implement a NIST compliant Continuous Monitoring process, as defined by FISMA, via independent assessment of 1/3 of controls each year. OCIO will identify yearly key controls to more rapidly perform annual assessments, identify weaknesses, and more rapidly remediate identified issues. The integration of enterprise-wide risk assessments is important to the selection of standardized controls sets to be assessed and authorized each fiscal year. ASOC is leading the shift to a continuous assessment and authorization model that will integrate the automation investment of the SSA with the near real-time risk management requirements emerging across the federal government. All systems entering service in the USDA must undergo a complete assessment and authorization (A&A) via the risk management framework (RMF) process described in NIST SP 800-37 Revision 1. This effort presents a snapshot of the risk the system presents to the department at that point in time. Switching to a continuous assessment of a specific subset of controls annually, and eliminating the requirement to assess all controls every three years, reduces the testing effort (and expense) by up to 40 percent.

The Annual Information Security Awareness Training classes were revised, reducing the class length by 40 percent, and are now available online. The classes include the option of 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. USDA consistently achieves over 99 percent completion rates across the entire organization for the FISMA required information security awareness training each fiscal year.

To provide more complete oversight, concurrency reviews of all system security plans (SSPs) are required at two key points throughout the RMF as designed by NIST SP 800-37 Revision 1. Specifically, the first concurrency review is completed after step 3 of the RMF and once again after Step 4 of the RMF, after controls testing is 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. Annual concurrency reviews will be required for oversight and compliance for systems moving into the continuous assessment and authorization implementation plan. These efforts are expected to reduce the on-going costs of security operations over time as a phased approach to a full RMF.

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 A&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, OCIO completed the following initiatives:

- Transitioned CSAM to the Platform as a Service (PaaS) Cloud environment at NITC.
- Modernized CSAM through major upgrade to Version 3.0

In 2012, OCIO will continue to improve and implement the following within CSAM:

- Implementation of common controls (program, policy and data center inheritable controls) in CSAM
- Leverage the new features afforded with CSAM Version 3.0 to support the transition into continuous monitoring as required by FISMA

In 2013 the Center of Excellence (COE) will continue implementation of continuous monitoring as designed in the RMF prescribed in NIST SP 800-37 Revision 1 through the USDA 6 step RMF Process addressing OIG audit recommendations and strengthening the USDA enterprise security posture. Continuing initiatives include:

- Conducting training sessions to continue to improve the quality of USDA A&A packages and the overall A&A process as needed

- Continue the outreach from the Department to the Agencies through the COE Liaisons to assist 100% of all agencies in achieving FISMA compliance. This includes FISMA related oversight and compliance support for 17 agencies and 15 offices supporting over 650 systems 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 working to update 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 National Level Exercise 2012 which crossed multiple government agencies/departments. The purpose of NLE 2012 was to examine the Nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a series of significant cyber events over four distinct exercises. The four exercises were an information exchange tabletop, a Cyber Incident Management Tabletop, the NLE Capstone event, and the Eagle Horizon Continuity exercise. The NLE 2012 exercise series successfully highlighted the challenges in detecting, assessing, and responding to a significant cyber event and emphasized the critical importance of coordinating national response efforts. In addition to validating important concepts, the exercise also drew attention to areas requiring further improvement. USDA was a front-runner of the Federal Departments that participated in these 4 exercises.

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 accomplished:
A full review of the ATT / Network Contract and associated contracting information, requested additional security architecture information, created a detailed review of current AT&T security capabilities, and reconfigured necessary network taps to maximize our view of USDA traffic. In addition, ASOC plans on working with AT&T to see what information is needed for additional or increased capabilities, requesting information on how to include the AT&T VPN Exchange in the Security Sensor Array (SSA) data feed, implementing network upgrades in four USDA locations, meeting with Microsoft to gathering information on Office365 data flows, integrating SEIM information from three agencies into our tool Trustwave, and continuing to tune our SSA.

1. ASOC Incident Handling Division (IHD) and Monitoring and Analysis Division (MAD) have been collocated in Kansas City Beacon Building G25 space. This action will enable divisions to refine cyber security monitoring, incident handling, and threat assessment operational procedures. Some the services provided to USDA and the USDA agencies include: Incident Handling and Investigation, Monitoring Enterprise Security Systems, Enterprise Cyber Security Threat Analysis, and Devolution activities.

2. With the current reorganization that aligns cyber security at Department-level under a recently appointed CISO, the ASOC has initiated this study and gap analysis, performed by Mischel Kwon and Associates, LLC (MKA), to review the existing USDA Cyber Security Programs and provide a gap analysis and recommendations to strengthen the Department-level Cyber Security Program at the USDA. The study of the Cyber Security Program will include a review of the programmatic, governance, communications, and USDA agency relationships as they relate the main responsibilities of a Department-level CISO Program – Cyber Security (FISMA) Compliance, Security Operations, and Remediation. Like all strong programs, reviewing the program is required to ensure it is providing the best services possible. This gap analysis report will document the "as-

is" state and the "to-be" state is based on core FISMA requirements and provides initial recommendations that will enable the CISO to integrate the operational and compliance portions of FISMA across USDA, improving the cyber security posture of USDA to focus on risk, not compliance, and ultimately being able to influence USDA's annual FISMA evaluation and score.

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. Ten interns have completed the program and accepted full-time employment within the USDA as Federal employees. The success of the program is also indicated by a doubling of the number of applicants from 2011 to 2012.

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 Devolution Facility opened in October 2011.

The ASOC 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 2013, 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 under development. A business case will be drafted in order to gain program funding to procure required systems: Joint Worldwide Intelligence Communications System (JWICS) and Crisis Management System (CMS). If the business case approval and funding is allocated at the start of 2013, the systems can be installed and operational by the end of 2013. 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.

In addition, the ASOC publishes formal USDA Early Warning Indicators (UEWI) to the government cyber security community via the several classified and controlled collaboration mechanisms (including the US Cyber Emergency Response Team's GFIRST Mercury Portal, the Department of Homeland Security's Data Network (SIPRNet) ASOC blog, and via direct distribution to other government agencies (OGA)). The UEWI's provide timely, relevant, and technical analysis indicators based on recent nation state actor activity, spear phishing attacks, and malicious content. This effort has allowed the ASOC to become one of the government leaders in cyber security-related technical indicator sharing and has bolstered the ASOC's presence in the community.

USDA signed a MOA with DHS NCSD Network Security Deployment (NSD) and utilizes EINSTEIN first and second generation sensors. USDA was the second Federal Department after DHS to have the Einstein II system

placed into formal production. An aggressive scanning and wireless security program in conjunction with the endpoint protection program better addresses the realities of contemporary computing where mobile computing devices routinely operate outside the network perimeter. Intrusion detection and prevention are essential at all levels of network operations with an integrated framework that aggregates, correlates, and stores all events at the agency and Department level.

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 2013 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.

Cyber Security Policy Remediation: USDA's OCIO has accumulated open Office of Inspector General (OIG) audit findings directly related to cyber security policy and procedures. To date, OCIO has agreed to the OIG audit recommendations and utilized an OIG Remediation Plan to document agreed steps that would be taken to close audit findings. As planned, draft policies and procedures were drafted by OCIO resources however none have been routed completely through the departmental clearance process to reach published status. In January 2013, a Cyber Security Working Group have been established to execute a fast track effort to transition a backlog of OCIO cyber security draft policies and procedures to the Departmental clearance process. The expected outcome of this effort is to close outstanding audit recommendations, refresh cyber security policies and procedures to match expected USDA practices, demonstrate USDA efforts to be FISMA compliance.

USDA Fusion Center: A ribbon-cutting ceremony to officially dedicate the USDA Fusion Operations Center located at the Beacon Facility in Kansas City, Missouri, took place on October 16, 2012. . The USDA Fusion Operations Center is a combined effort of the Office of the Chief Information Officer (OCIO), Agriculture Security Operations Center (ASOC), and the Office of Homeland Security and Emergency Coordination (OHSEC). This facility will be home to the ASOC whose efforts to combat cyber attacks will be enhanced by the ability to combine their team of cyber monitoring and forensic analysts, cyber incident investigators, and cyber security engineers working in an environment that fuses all their skills and tools in a central location.

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 to be reinvested by the agencies that have benefitted from the collective savings of these enterprise-wide contracts.

Identity, Credential, and Access Management (ICAM) in USDA: The ICAM program is a centralized enterprise-wide security service, providing access control and identity management for USDA.

The eAuthentication component of ICAM provides authentication and authorization for over 450 USDA web applications. eAuthentication provides secure access for over 100,000 Federal employees, contractors and affiliates using HSPD-12 PIV (Personal Identity Verification) cards issued by GSA. Additionally eAuthentication enables nearly 400,000 public citizens and partners to access USDA services with secure identity validated credentials.

The identity management component of ICAM supports HSPD-12 and FICAM (Federal Identity, Credential and Access Management) initiatives by managing the digital identity for all employees, contractors and affiliates. This component improves the overall USDA security posture by facilitating automated provisioning and de-provisioning of accounts and access permissions based the user's role, position and employment status.

The eAuthentication and identity management components of ICAM enhance compliance with FISMA, A-123 and NIST 800-53. Additionally, ICAM provides the mechanism for USDA agencies and offices to achieve compliance with OMB M-11-11.

The ICAM Service developed and implemented procedures for secure digital signatures using the HSPD-12 PIV card. Digital signatures are a type of electronic signature that offers assurance of the signer's identity. The use of digital signatures is helping USDA move from a paper-based to an electronic workflow, streamlining processes and improving security.

Key ICAM 2013 Activities include:

- ICAM is working with GSA and the US Postal Service on pilot initiatives to leverage commercially provided credentials for public citizens to access online government services. This supports the OMB mandate regarding the use of external credentials and the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC is a White House initiative designed to work collaboratively with the private sector, and public sector agencies to improve the privacy, security, and convenience of sensitive online transactions;
- ICAM is working with GSA and other Federal Agencies to enable interoperability of PIV credentials, providing secure access and streamlining inter-agency collaboration;
- ICAM is supporting the USDA mobility initiative by providing secure authentication methods for mobile devices;
- ICAM is supporting the Data Center Consolidation initiative by migrating off legacy infrastructure to the USDA Enterprise Data Center;
- ICAM is supporting the USDA Administrative Streamlining initiative by migrating helpdesk services to the USDA Consolidated Helpdesk; and
- ICAM will continue to integrate USDA IT systems with ICAM centralized security services.

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; cost savings is approximately $450,000 per additional system purchased;
- Standardized connectivity and equipment improved ease of use (and therefore utilization) and reduced helpdesk support and maintenance costs. The Tandberg video management control system that USDA installed at NITC

provides a centralized address book, centralized network and device monitoring (MCU, gateway, and gatekeeper), configuration, video endpoint management and control, system wide device provisioning and software updates, remote device monitoring and problem diagnostics and notification, and performance monitoring and tracking. OCIO has eliminated the need for additional commercial services for an estimated 1,000 calls at a base cost of $30 per call for a cost avoidance of $30,000. Additional cost avoidance for the maintenance for the original infrastructure was $29,665;

- Security, access control, and monitoring are done from a central location and are invisible to the end user; and
- Consolidated equipment purchases have achieved significant cost savings. During 2012, USDA Agencies and Staff Offices saved over $2.25 million by using the Custom User Purchase Agreement (CUPA) that was in place for the purchase of video products. The savings is based on 2012 purchases of $4.02 mil. The total savings amounts to 56% off List Price.

Enterprise Geospatial Management Office (EGMO): The EGMO establishes and sustains the executive responsibility, accountability, and optimization for the $370 million Departmental investment in geospatial solutions and GIS technologies. The EGMO guides increased maturity of enterprise geospatial capabilities to serve senior executives for policy, strategic alignment, tactical decision-making, government data exchange and shared services, and participatory governance with external stakeholders. The EGMO employs a lifecycle portfolio and product management approach to orchestrate enterprise capital investments and increase value, and improves operations capacity through shared technologies and workflows, joint ventures, and enterprise services. The EGMO strategically expands GIS user community to include professionals such as economists, scientists, policymakers, financial, and program managers. Moreover, EGMO creates web application and map services design and develop innovations demonstrating successful cloud-based solutions, which support efficiency and effectiveness in the Administration's agriculture and natural resources missions, as well as the adoption and migration of the federal government-wide National Geospatial Platform.

Roles

- Department Geospatial Information Officer (GIO) – directs, guides and coordinates geospatial and geographic information system (GIS) strategic planning, policy, acquisition, data quality management, governance, audit reporting, and portfolio and budget investment management and approvals; facilitates enterprise innovations, prototypes, and partnerships; Federal Geographic Data Executive Committee senior executive representative; Agency executive liaison with Federal, State, local, and tribal governments; and
- Department Senior Agency Official for Geospatial Information (SAOGI) – oversees, coordinates, and facilitates the agency's implementation of the geospatial-related requirements, policies, investments, and activities; serves as the policy-level official to represent each selected agency on the FGDC Steering Committee (OMB Circular A-16).

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. Array currently scans approximately 4 terabytes of data per day and is able to identify an average of 1,500 critical events per week (system tuning in process). With the Security Sensor Array in place, advanced persistent threats are now visible hours and days ahead of notification received from intelligence and external partners.

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 has reduced average incident age from 18.14 days in 2009 to 10 days in 2011 to 5.56 days in 2012.

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). This provides unprecedented visibility into software products and vulnerability patching and configurations settings across the department. ASOC has been using the end point health check tool to communicate vulnerabilities to agencies and track progress in mitigating those vulnerabilities. The software allows OCIO to provide analytics and reporting to the agencies on a number of key configuration issues, including software distribution patching, version control, and licensing on a bi-weekly basis. This reporting effort has resulted in significant and measurable drops in the number of at risk systems in USDA. By implementing enterprise endpoint security software on over 140,000 end user devices (desktops, laptops, and servers), ASOC has also positioned USDA to be ready to meet all challenges of mobility and telework Federal-wide initiatives.

Secure Communications: 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 the Office of Human Resources Management to utilize Monster Automated Hiring Systems for the processing and ranking of approximately 2,235 applications for the 2012 Information Technology Intern Program (ITIP) session. OCIO continues to increase leveraging of the portal by creating web pages for posting information on Departmental Management intern and other USDA job 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.

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. Developed the *ASOC Software Update Notices* and the *ASOC Situational Awareness Reports,* that share critical event and issue data with agencies in a repeatable and dependable format, informing agencies on the appropriate and necessary actions to take to reduce risks posed by new or emerging threats, focusing agency CIO's and IT personnel on enterprise cyber security risk in a consistent manner. Topics included 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. In addition, 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. The ASOC currently develops and distributes 14 monthly network security reports encompassing all 29 USDA agencies. The purpose of these monthly reports is to track and monitor the number of computers with outdated, unpatched and/or vulnerable software installations such as Adobe Acrobat. These reports help maintain awareness at the agency level and also help to strengthen the agency's security posture. The ASOC requires the agencies to report back their plan of action to mitigate these threats and not accept the risk of these vulnerabilities. The ASOC conducts follow-up collaboration to discuss the reports and any mitigation actions taken.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Statement of 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.

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

Agency Strategic Goal	**Agency Objectives**	**Programs that Contribute**	**Key Outcomes**
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.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
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.	Technology Planning, Architecture and E-Government	5: Increase in the number of projects using standardized and enterprise solutions and services.
	Leverage enterprise and cloud-based investments wherever possible to enable flexible and scalable solutions that minimize cost and risk.	Architecture and Systems Integration Division Cyber Policy and Oversight	6: Increase in the number of IT investments aligned with Enterprise Architecture. 7: High-level of customer satisfaction of services and solutions.
	Enhance information sharing across USDA through improved data definitions, standards, and governance and supporting technology solutions that enable interconnectivity.		8: Reduced number of non-EDC computer facilities.
	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.		

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
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.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
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.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
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.

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	2008 Actual	2009 Actual	2010 Actual	2011 Actual	2012 Actual	2013 Target	2014 Target
Performance Measure #1 Percent of SSN/TINs eliminated from USDA systems.							
a. Units	N/A	N/A	N/A	N/A	85%	85%	90%
b. Dollars (in thousands)	$7,741	$8,328	$6,246	$4,068	$4,166	$4,194	$4,628
Performance Measure #2 The number of non-Enterprise Data Center (EDC) computer facilities.							
a. Units	97	97	97	74	41	33	33
b. Dollars (in thousands)	$4,676	$5,030	$6,246	$4,068	$4,696	$4,921	$4,390
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	Est. baseline	10%	50%	50%
b. Dollars (in thousands)	N/A	N/A	$5,267	$3,430	$3,567	$3,592	$3,570
Performance Measure #4 Percent of systems tested using 800-53 rev. 3 security controls.							
a. Units	N/A	N/A	N/A	N/A	90%	95%	95%
Number of program security reviews completed.							
a. Units	N/A	N/A	N/A	8	24	24	24
Number of General Support Systems inventoried, base lined, and assessed.							
a. Units	N/A	N/A	N/A	Est. baseline	99%	99%	99%

Performance Measure	2008 Actual	2009 Actual	2010 Actual	2011 Actual	2012 Actual	2013 Target	2014 Target
Percent of ASOC incident report calls that are answered live by an incident handler.							
a. Units	N/A	N/A	N/A	Est. baseline	80%	80%	80%
Percent of security incidents closed within 30 days.							
a. Units	N/A	N/A	Est. baseline	90%	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	90%	90%	90%	90%
b. Dollars (in thousands)	$3,700	$3,981	$37,443	$24,388	$28,000	$28,000	$28,000
Performance Measure #5 Percent of eligible employees approved to telework.							
a. Units	N/A	N/A	N/A	67%	73%	78%	78%
b. Dollars (in thousands)	N/A	N/A	$5,960	$3,883	$3,568	$3,593	$3,571

Selected Accomplishments Expected for the 2014 Proposed Resource Level:

- An integrated Program Management Review for each IT investment in the Department's IT portfolio.
- OCIO will conduct monthly TechStat reviews of major IT investments.
- 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.
- Fully progress into continuous Assessment and Authorization process for all new and continuing systems in USDA's inventory.
- Provide oversight and compliance to ensure that complete and comprehensive assessments of all USDA systems comply with NIST 800-53 Revision 3 controls.
- Provide oversight and compliance to ensure that 100 percent of USDA personnel, contractors, volunteers and business partners complete FISMA required Information Security Awareness Training.
- 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 monitor agency/staff office EVM updates to the Capital Planning Investment Repository (CIMR) to track actual performance data for all IT investments that meet USDA's EVM threshold.
- OCIO will monitor agency EVM process maturity.
- OCIO will monitor IT investments to improve the quality of the business cases.
- 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.
- OCIO will establish a continuous monitoring program focused on continuous vulnerability assessments of all security technologies and processes.
- 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 is 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 reconfigure the ASOC Security Sensor Array to an inline security state in 2014. This architecture will give the ASOC the ability to actively 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 complete training of agency security and operational personnel from all USDA agencies on the Security Sensor Array tools. By training agency personnel on ASOC tools and methods, connectivity can be extended to the SSA in a secure manner and USDA can double or triple the number of simultaneous analysis sessions performed. Agency personnel will also bring their subject matter expertise regarding agency data and activities, allowing the SSA tools to be further enhanced and tuned for more accurate monitoring.
- OCIO will develop a USDA true testing facility for Accessibility & Section 508 compliance and continue to provide Enterprise solutions to check websites, documents, and training materials for accessibility.
- 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.
- Develop guidelines to protect Controlled Unclassified Information (CUI), in accordance with Northwest Advanced Renewable Alliance guidelines. CUI classification replaces sensitive but unclassified and for official use only classifications for documents.
- In conjunction with the CM activity, OCIO will continue to fine-tune the identification and development of program metrics and key performance indicators. This will be achieved through a cross-OCIO management effort that will identify and measure critical interdependencies, and the portion of those elements that can be met from existing data resources.
- OCIO will ensure that all current outstanding USDA cyber security policies and procedures will be updated and completed as needed to ensure compliance with federal mandates, guidelines and recommendations.

DEPARTMENTAL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

Strategic Goal Funding Matrix
(Dollars in thousands)

Program / Program Items	2011 Actual	2012 Actual	2013 Estimate	Change	2014 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	$4,068	$4,166	$4,194	+434	$4,628
Staff Years	20	21	22	+4	26
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	4,151	4,696	4,921	-531	4,390
Staff Years	22	23	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	3,430	3,567	3,592	-22	3,570
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					
Office of the Chief Information Officer	24,388	28,000	28,000	-	28,000
Staff Years	39	41	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	3,883	3,602	3,593	-22	3,571
Staff Years	8	9	10	-	10
Total Costs, All Strategic Goals	39,920	44,031	44,300	-141	44,159
Total FTEs, All Strategic Goals	97	102	112	4	116

Full Cost by Strategic Objective
(Dollars in thousands)

Program / Program Items	2011 Actual	2012 Actual	2013 Estimate	2014 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)	$2,676	$2,741	$2,843	$3,133
Indirect costs	1,392	1,425	1,351	1,495
Total Costs	4,068	4,166	4,194	4,628
FTEs	20	21	22	26
Performance Measure: Percent of SSN/TINs eliminated from USDA systems. Measure	N/A	100%	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)	$2,676	$3,089	$3,336	$2,931
Indirect costs	1,392	1,607	1,585	1,459
Total Costs	4,068	4,696	4,921	4,390
FTEs	22	23	24	24
Performance Measure: Number of non-Enterprise Data Center computer facilities. Measure	74	41	33	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)	$2,257	$2,347	$2,435	$2,384
Indirect costs	1,173	1,220	1,157	1,186
Total Costs	3,430	3,567	3,592	3,570
FTEs	8	8	9	9
Performance Measure: Percent of incidents managed through the Case Management tracking tool across the USDA-wide enterprise. Measure	Est. baseline	10%	50%	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)	$16,043	$18,419	$18,981	$18,697
Indirect costs	8,345	9,581	9,019	9,303
Total Costs	24,388	28,000	28,000	28,000
FTEs	39	41	47	47

Performance Measure:				
Percentage of systems tested using 800-56 rev. 3 security controls.				
Measure	N/A	90%	90%	95%
Performance Measure:				
Number of program security reviews completed.				
Measure	24	24	24	24
Performance Measure:				
Percent of General Support Systems inventoried, base lined, and assessed.				
Measure	Est. baseline	99%	99%	99%
Performance Measure:				
Percent of ASOC incidence report calls that are answered live by an incident handler.				
Measure	Est. baseline	80%	80%	80%
Performance Measure:				
Percent of security incidents closed within 30 days.				
Measure	Est. baseline	90%	90%	90%
Performance Measure:				
Percent of all incidents following USDA Security Incident processes and procedures to the designated authorities.				
Measure	N/A	90%	90%	90%

<u>Agency Strategic Goal 5:</u> 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)…	$2,554	$2,347	$2,435	$2,384
Indirect costs	1,329	1,221	1,158	1,187
Total Costs	3,883	3,568	3,593	3,571
FTEs	8	9	10	10
Performance Measure:				
Percent of eligible employees approved for telework.				
Measure	67%	73%	78%	78%
Total Costs, All Strategic Goals	39,837	43,997	44,300	44,159
Total FTEs, All Strategic Goals	97	102	112	116