2010 Explanatory Notes

Office of the Chief Information Officer

Table of Contents

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

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

OCIO also has direct management responsibility for the IT component of the Service Center Modernization Initiative through the Information 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, 2008, there were 928 full-time permanent employees funded by appropriated, reimbursed, and Working Capital Funds.

Location	Full-time permanent
Washington, D.C.	
OCIO Direct	56
OCIO WCF	74
Subtotal	130
Field Units	
OCIO Direct	6
OCIO WCF	792
Total	928

OFFICE OF THE CHIEF INFORMATION OFFICER

Open Audits (During FY 2008)

Office of Inspector General Reports:

50501-4-FM 10/2005
Review of the USDA's Certification and Accreditation Efforts

50501-8-FM 2/2007
Review of USDA Controls Over Stolen or Lost Computer Equipment

50501-9-FM 7/2008
Management & Security over USDA's Wireless Connections

88501-7-FM 3/2007
General Controls Review - FY06 OCIO-ITS

Government Accountability Office Reports:

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

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

GAO-08-925 7/2008
Information Technology: Agencies Need to Establish Comprehensive Policies to Address Changes to Projects' Cost, Schedule, and Performance

Closed Audits (During FY 2008)

Office of Inspector General Reports:

88501-6-FM 8/2006
Management & Security over USDA's UTN

Government Accountability Office Reports:

GAO-04-49 2/2004
Information Technology Management – Government-Wide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved

OFFICE OF THE CHIEF INFORMATION OFFICER

Available Funds and Staff Years

2008 Actual and Estimated 2009 and 2010

Item	2008 Actual		2009 Estimated		2010 Estimated	
	Amount	Staff Years	Amount	Staff Yeas	Amount	Staff Years
Direct Appropriation	$16,361,000	62	$17,527,000	63	$63,579,000	88
Rescission…….....	-114,527	--	--	--	--	--
Total, Agriculture Available…	16,246,473	62	17,527,000	63	63,579,000	88
Obligations under Other USDA appropriations:						
Reimbursements:						
E-Gov Presidential Initiative...……	11,674,819	--	11,185,000	--	11,185,000	--
E-Gov HSPD12.....	14,813,000	--	12,783,000	--	12,783,000	--
E-authentication……..	7,627,843	--	--	--	--	--
Ag Learn.....	362,808	--	375,000	--	375,000	--
Content Management……..	1,310,000	--	1,500,000	--	1,500,000	--
Enterprise Services…….....	5,500,000	--	5,500,000	--	5,500,000	--
LDRPS…….....	956,000	--	880,000	--	880,000	--
WCF Activities….....	574,974	3	575,000	3	575,000	3
IT Infrastructure...……...	--	--	3,000,000	--	3,000,000	--
NTIA Spectrum……..	1,325,818	--	1,593,000	--	1,593,000	--
Subtotal, Reimbursements	44,145,262	3	37,391,000	3	37,391,000	3
Working Capital Fund (WCF) a/						
Information Technology.....	371,714,233	821	334,333,000	925	336,871,000	925
NITC (Non-USDA)…….....	15,361,783	21	16,887,000	25	17,131,000	25
Capital Equipment…….....	11,745,527	--	4,500,000	--	4,500,000	--
Subtotal, WCF…….....	398,821,543	842	355,720,000	950	358,502,000	950
Total, OCIO…….....	459,213,278	907	410,638,000	1,016	459,472,000	1,041

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

OFFICE OF THE CHIEF INFORMATION OFFICER

Permanent Positions by Grade and Staff Year Summary

2008 Actual and Estimated 2009 and 2010 a/

Grade	2008 Wash DC	2008 Field	2008 Total	2009 Wash DC	2009 Field	2009 Total	2010 Wash DC	2010 Field	2010 Total
Senior Executive Service	4	--	4	5	--	5	6	--	6
GS-15…….……..	12	1	13	13	1	14	17	2	19
GS-14…….……..	20	3	23	19	3	22	24	5	29
GS-13…….…...	9	--	9	14	--	14	17	--	17
GS-12…….…...	2	1	3	2	1	3	7	3	10
GS-11…….……..	3	--	3	2	--	2	2	--	2
GS-10…….……..	1	--	1	1	--	1	1	--	1
GS-9…….……..	2	1	3	--	1	1	1	1	2
GS-7…….……..	2	--	2	2	--	2	3	--	3
GS-6…….……..	1	--	1	1	--	1	1	--	1
GS-5…….……..	1	--	1	1	--	1	1	--	1
Total Permanent Positions	57	6	63	60	6	66	80	11	91
Unfilled Positions end-of-year.....	-1	--	-1	- -	- -	- -	- -	- -	--
Total, Permanent Full-Time ..... Employment, end-of-year.....	56	6	62	60	6	66	80	11	91
Staff Year Estimate	56	6	62	60	6	66	80	11	91

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

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

SIZE, COMPOSITION AND COST OF MOTOR VEHICLE FLEET

The 2010 Budget Estimates propose no additional purchases or leases of vehicles.

OCIO-ITS is the in-house provider of information technology, service and support for over 40,000 USDA Service Center Agency employees and their networked computers, IT equipment, and the shared infrastructure of Common Computing Environment (CCE) that agency networks and applications run on. Our customers are FSA, NRCS, and RD and their respective partner organizations that provide crop insurance, credit, environmental, conservation, and emergency assistance programs for farmers and ranchers; maintenance, and improvement to natural resources and housing, community facilities, and utilities and other services to increase rural American's economic opportunities and improve quality of life.

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

Current fleet is based on mission and geographic needs. As of April 1, ITS had 52 leased GSA vehicles, but ITS plans on expanding fleet to approximately 220 vehicles by end of FY'09. Vehicles will be leased from GSA.

Changes to the motor vehicle fleet. No changes are proposed to the fleet for FY 2010.

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

Impediments to managing the motor vehicle fleet. None at this time.

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

Size, composition and cost of agency motor vehicle fleet as of April 1, 2009, are as follows:

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

	Number of Vehicles by Type								
Fiscal Year	Sedans and Station Wagons	Light Trucks, SUVs and Vans		Medium Duty Vehicles	Ambulances	Buses	Heavy Duty Vehicles	Total Number of Vehicles	Annual Operating Cost ($ in thous)
		4X2	4X4						
FY 2007	3	4	1	0	0	0	0	8	$35
Change from 2007	-1	+2	0	0	0	0	0	+1	$2
FY 2008	2	6	1	0	0	0	0	9	$37
Change from 2008	+118	+84	+9	0	0	0	0	+211	$463
FY 2009	120	90	10	0	0	0	0	220	$500
Change from 2009	0	0	0	0	0	0	0	0	$
FY 2010	120	90	10	0	0	0	0	0	$1,030

OFFICE OF THE CHIEF INFORMATION OFFICER

Appropriation Language

For the necessary expenses of the Office of the Chief Information Officer, [$17,527,000] $63,579,000.

Lead-off Tabular Statement

Appropriations Act, 2009	$17,527,000
Budget Estimate, 2010	63,579,000
Increase in Appropriation	+46,052,000

Summary of Increases and Decreases
(On basis of appropriation)

Item of Change	2009 Estimated	Pay Costs	Program Changes	2010 Estimated
Office of the Chief Information Officer	$17,527,000	+$252,000	+$45,800,000	$63,579,000

Project Statement
(On basis of appropriation)

	2008 Actual		2009 Estimated		Increase or	2010 Estimated	
	Amount	Staff Years	Amount	Staff Years	Decrease	Amount	Staff Years
Chief Information Officer	$16,116,625	62	$17,527,000	63	+$46,052,000	$63,579,000	88
Unobligated Balance	+129,848	--	--	--	--	--	--
Total available or estimate	16,246,473	62	17,527,000	63	+46,052,000	63,579,000	88
Rescission	114,527	--	--	--			
Total, Appropriation	16,361,000	62	17,527,000	63			

OFFICE OF THE CHIEF INFORMATION OFFICER

Justification of Increases and Decreases

(1) An increase of $46,052,000 for the Office of the Chief Information Officer consisting of:

a) An increase of $252,000 to fund increased pay costs.

This increase is needed to maintain the current level of staffing to ensure that OCIO can carry out its full range of responsibilities and agency goals. Funding is needed to cover pay and benefit cost increases for existing staff.

b) A total increase of $45.8 million and 25 staff years to improve the Department's information technology security.

OCIO has been actively working with all USDA agencies and has partnered with the United States Computer Emergency Response Team (U.S. CERT), the Federal Bureau of Investigation and others to defend against cyber security threats. Ongoing activities to improve USDA's defense in depth include: (1) implementing an enterprise-wide security operations center that employs state of the art monitoring, incident response, threat analysis and forensics capabilities; (2) migrating decentralized agency IT systems (currently in locations that do meet data center standards for security and continuity of operations) to enterprise data centers; (3) centralizing the Department's e-mail systems; (4) standardizing identity management; (5) establishing common desktop security configuration using the Federal Desktop Common Configuration (FDCC) settings; (6) continuing efforts to protect personally identifiable information through SSN elimination and whole disk encryption; and (7) working with U.S. CERT to deploy the latest monitoring and reporting technologies to strengthen incident response capabilities.

Resources are needed for this critical area to ensure the confidentiality, integrity and availability of USDA information and will improve the efficiency and effectiveness of USDA program service delivery. The FY 2010 budget includes an increase of $45.8 million for cyber security efforts. Components of this request are as follows:

- An increase of $19.0 million to conduct network security assessments.

This funding will enable USDA to carry out comprehensive security assessments of each USDA network to determine the pervasiveness and magnitude of infection and vulnerability in each agency so that networks and systems can be cleaned, redesigned/rebuilt (as necessary) and added into healthy enclaves within USDA's Enterprise Data Centers. This strategy ensures that networks, systems and applications will operate in a secure core and not pollute known good operations should breaches occur. USDA/OCIO has conducted limited assessments on some of its highest risk networks and is moving these into a trusted core. Because of the pervasive and evolving nature of the security threats, existing resources are not adequate to address the immediate needs. This funding is essential to secure contract resources to conduct individual assessments of each and every agency and staff office IT infrastructure. These assessments will enable the Department to identify core and essential functions, locate potential vulnerabilities in its systems and networks, and develop real-world modeling data that will allow for the redesign and rebuilding of those systems needing enhanced functions and security. This funding will also provide for network security improvements as the agencies migrate to Enterprise Data Centers. With this migration, agency systems will be moved to security facilities that provide continual support, security and monitoring to greatly improve the

Department's security posture and real-time awareness. Critical to securing the Department's network infrastructure is the development of a comprehensive cyber security Department–wide architecture which is essential to the Department's ability to implement IT security standards to securely transmit and share data. Additionally, this funding will enable USDA/OCIO to acquire resources to implement a compliance organizational structure to conduct cyber security and personally identifiable information assessments; and penetration testing across the Department to implement a compliance model that allows targeted remediation and compliance enforcement monitoring where the risk is greatest.

- An increase of $14.5 million to procure security tools to be deployed across the USDA network.

  This increase provides security software tools, services, and the platforms and storage to improve logging, monitoring, threat detection and prevention. These tools are a critical component to ongoing monitoring and prevention of attacks in real time and/or near real time and support a robust defense-in-depth posture. In addition, the funding would provide for the necessary hardware to fully utilize, store, and host the security tools and securely retain the multiple terabytes of data the tools will generate. The tools and services are necessary to ensure that USDA can monitor and aggregate all of the data traffic inside its network. This monitoring will afford the Department the ability to view and log incoming and outgoing information and review it for malicious activity, viruses, bots, or other security threats. In addition, this monitoring will allow the Department to better confirm the identities of individuals accessing its systems, and any unauthorized uses made of its corporate data. This analysis capability will be critical to securing the non-traditional social media and "Web 2.0" services that the Department is implementing to increase public transparency. The data aggregation functions of the tools and services will provide USDA with the capability to conduct in-depth activity and trend analysis across its component agencies. As the sophistication of malicious software increases, the demand grows for USDA to be able to identify blended threats, where multiple targets and exploits are activated simultaneously. USDA cannot establish an effective security operations function without the capital investment that these tools and services represent. These tools and services will also allow OCIO contract resources to effectively monitor the overall application and effectiveness of the security tools use in the security operations center and make adjustments, where necessary to increase overall effectiveness of the tool suite.

- An increase of $12.3 million and 25 staff years to establish the Agriculture Security Operations Center (ASOC).

  USDA, following industry and government best practices (U.S. CERT, Carnegie Mellon CERT, Telecommunications Industry), is standing up a Security Operations Center that coordinates continuous 24x7x365 security operations to defend USDA information, assets, network and systems. The ASOC will provide round the clock threat analysis, incident handling, incident response and overall command and control for defense of the USDA in cyberspace and ensure the security of operations directly supporting the national food supply chain, the agricultural economy, research and development, and an active Departmental loan portfolio of over $120 billion. The requested increase of $12.3 million, and 25 staff years will provide USDA with around-the clock security operations capability to protect and defend the data and businesses of USDA. The ASOC team of contract and direct-hire professionals would conduct continuous monitoring, triage, analysis, protection, and incident response for the Department's world-wide information assets. The creation of an efficient and effective security operations center is an essential prerequisite to creating the trust and assurance that USDA's business partners and the public demand, to build and expand the engagement of these vital participants in the current and emerging technology-based business initiatives.

OFFICE OF THE CHIEF INFORMATION OFFICER

Geographic Breakdown of Obligations and Staff Years
2008 Actual and Estimated 2009 and 2010

	2008		2009		2010	
	Amount	Staff Years	Amount	Staff Years	Amount	Staff Years
District of Columbia	$15,457,515	56	$16,836,000	57	$59,015,000	77
Kansas	659,110	6	691,000	6	4,564,000	11
Unobligated balance	129,848	--	--	--	--	--
Total, Available or Estimate	16,246,473	62	17,527,000	63	63,579,000	88

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects

2008 Actual Estimated 2009 and 2010

		2008	2009	2010
Personnel Compensation:				
Washington, D.C.		$5,784,759	$6,008,000	$7,815,000
Kansas.		527,288	552,000	1,318,000
11	Total personnel compensation	6,312,047	6,560,000	9,133,000
12	Personnel benefits	1,481,238	1,539,000	2,179,000
13	Payments to prior employees	254	--	--
	Total personnel comp. & benefits	7,793,539	8,099,000	11,312,000
Other Objects:				
21	Travel	117,198	117,000	117,000
22	Transportation of things	1,961	4,000	4,000
23.3	Communications, utilities, and misc. charges	466,718	419,000	3,219,000
24.0	Printing and Reproduction	58,816	153,000	153,000
25.2	Other services	3,352,722	4,353,000	25,212,000
25.3	Purchases of goods and services from Government Accounts	4,198,103	3,942,000	20,442,000
26	Supplies and materials	70,148	143,000	143,000
31	Equipment	57,419	297,000	2,977,000
43	Interest and Dividends	1	0	0
	Total other objects	8,323,086	9,428,000	52,267,000
Total direct obligations		16,116,625	17,527,000	63,579,000
Position Data:				
Average Salary, ES positions		$160,182	$177,182	$177,761
Average Salary, GS positions		$111,104	$119,844	$123,269
Average Grade, GS positions		14.5	14.6	14.7

OFFICE OF THE CHIEF INFORMATION OFFICER

STATUS OF PROGRAMS

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.

Expanding Electronic Government

Current Activities:

USDA Initiatives: Progress made this year allows USDA to continue its Department-wide approach to delivering shared services. USDA's shared services are described in the USDA IT Strategic Plan. A copy of the plan is available at http://www.ocio.usda.gov/n_USDA_IT_Strategic_Plan.pdf. Participation in these services is strong, with USDA agencies actively involved in the Enterprise-wide shared services (USDA's eAuthentication Service, AgLearn, and the common infrastructure provided through USDA's Enterprise Shared Services, Enterprise Correspondence Management Modules, the Enterprise Architecture Repository (EAR), and capital planning investment tools). For example, there are over 112,000 active AgLearn accounts across USDA, and in a typical month over 40,000 users complete 1,135 different courses, and the USDA eAuthentication Service protects 296 Web-based applications that require username/password protection. In addition, USDA opened a secure communications facility to provide shared enterprise access to the Homeland Security Data Network through a Federal partnership with the Department of Homeland Security.

USDA Participation in Presidential Initiatives: USDA continues to support the goals of the President's Management Agenda (PMA) by participating in 31 Presidential Initiatives and Lines of Business (LoB). USDA is also an active participant in the development of a government-wide infrastructure to support Homeland Security Presidential Directive 12 (HSPD-12) and is also making significant progress implementing continuity of operations communications capabilities to meet the requirements of the National Communications System Directive 3-10 (NCSD 3-10).

USDA will provide an estimated $12.3 million to support 10 Presidential Initiatives and 6 LoBs in FY 2009. In addition to financial contributions, USDA employees serve on committees, work groups and executive governance boards of the various Presidential Initiatives.

By participating in the Presidential 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 OCIO customers.

Table1: Presidential E-Government Initiatives and Lines of Business

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

Note: See page 4g-26 for additional information on Initiatives and LoBs.

Selected Examples of Recent Progress:

USDA's eAuthentication Service:

- USDA's eAuthentication Service protected 296 USDA Web-based applications, including 32 new integrations in FY 2008;
- More than 96,800 employees and approximately 214,000 customers owned an eAuthentication credential in a typical month in FY 2008; and
- USDA eAuthentication Service customers' use their credentials for nearly 2,200,000 authentications of personal identify and over 46,000,000 Web site authorizations for access to protected content every month.

E-Training and AgLearn:

- AgLearn developed and executed a variety of marketing approaches that increased discretionary training by 275 percent over FY 2007;
- AgLearn is USDA's implementation of the E-Training Presidential Initiative. During FY 2008 124,728 AgLearn users, which include employees, contractors and partners, completed 12,845 different courses;
- AgLearn delivered Department-wide Security Awareness, Privacy Basics, and Ethics mandatory trainings;
- Aglearn has 14,648 active courses available. As of Setember 30, 2008, 6,598 agency-sepcifc courses were deployed;
- AgLearn obtained an enterprise license for Books 24 X 7 and Ninth House scenario-based behavioral training for USDA-wide use at significantly reduced costs; and
- AgLearn continued to serve as the Department's sole official resource for processing external training requests using its built-in SF-182 form and approval process. AgLearn processes, on average, over 1,000 SF-182s monthly.

Other Presidential Initiatives:

- USDA posted 112 funding opportunities on Grants.gov in FY 2008, and 100 percent included matching application packages;
- In the fourth quarter of FY 2008, USDA through the Grants Management LoB, signed a Letter of Intent with the Department of Health and Human Services, Administration for Children and Families for the operation of the Grants Center of Excellence consortium;
- USDA identified 10 internal programs related to disaster benefits and updated information about those programs on GovBenefits.gov in FY 2008;
- USDA continues to meet or exceed requirements to process 95 percent or greater of background investigations through the Electronic Questionnaires for Investigations Processing system (eQIP), a single electronic system that ensures compliance with government standards. USDA processed 100 percent of all National Security and Public Trust investigations for new employees in FY 2008;
- All USDA Federal Register rules, proposed rules, and notices continued to be available for public comment on E-Rulemaking's Regulations.gov;
- USDA acquired and implemented continuity of operations communications capabilities for senior leadership in response to NCSD 3-10 requirements and recommendations from the White House Office of Science and Technology Policy; and
- The Department supported an initiative to improve the management of the Nation's increasingly scarce radio spectrum. Per Presidential memoranda issued on June 5, 2003, and November 30, 2004, USDA updated a biennial *USDA Strategic Spectrum Plan* to the Department of Commerce, contributed to a *Federal Strategic Spectrum Plan*, participated on the President's Task Force for a 'Spectrum Policy Initiative' and actively contributed to Working Level Group G activities on strategic planning and reform.

Enterprise Shared Services:

Enterprise Shared Services (ESS) is a suite of tools, standards, and business applications that facilitate USDA's Department-wide effort to deliver citizen-centric, online information and services. USDA developed these shared services with the goal of maximizing efficiency, reducing cost, and improving customer service. ESS saves costs by eliminating stovepipe systems developed by individual agencies. The ESS was established by a cross-Departmental effort of agencies identifying needs and requirements. Agencies continued using the ESS components in FY 2008 for:

- Web Content Management: This service provides content creation, content control, editing, and many essential Web maintenance functions for USDA Web sites;
- IBM WebSphere Portal: This product enables application integration by helping business applications exchange information across different platforms, sending, and receiving data as messages; and
- Document Management: This service allows USDA agencies to track and store electronic documents and/or images of paper documents.

Expanding Electronic Government: Security:

Current Activities:

Cyber Security: OCIO continues to implement its aggressive strategy to improve USDA's information security by providing training and establishing standardized computer security policies, processes and controls within the Department. OCIO Cyber Security Division continues to focus on activities that align with security best practices, Federal laws and oversight requirements. USDA participates in two Office of Management and Budget (OMB) mandated Information Systems Security LoB, one for Federal Information Security Management Act (FISMA) Reporting and the other for Security Awareness Training.

Systems Certification and Accreditation: Security accreditation is the official management decision to authorize operation of an information system. Security accreditation, which is required under OMB Circular A-130 and FISMA, challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical, operational, cost and schedule constraints, and mission requirements. To meet this security requirement, OCIO has developed an aggressive strategy for certifying and accrediting USDA's information systems.

This strategy includes policy, guidance, training, contract and staff support, and on-going program management. While it is difficult to assure that all systems are always in a state of full accreditation because of the changing universe including new systems, developing systems and expiring accreditations, the Department's goal is to ensure that all systems are accredited. This is accomplished through a rigorous program including, but not limited to, policy compliance reviews, certification concurrency reviews, independent verifications and validations, distribution of

USDA-specific guidance grounded in National Institute of Standards and Technology (NIST) and other Federal standards, and proactive communication efforts.

OCIO has fully incorporated its use of the Cyber Security Assessment and Management System (CSAM), the Department of Justice's LoB for the FISMA reporting tool, in its certification and accreditation (C&A) process. OCIO uses CSAM as the official repository for C&A documents and controls testing. OCIO has also cooperated with the Office of the Chief Financial Officer (OCFO) to incorporate the OMB A-123 Appendix A testing for general computer controls. In doing so, OCIO has implemented a process to minimize duplication of testing control while simultaneously improving the quality and effectiveness of testing.

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

Encrypted mobile satellite equipment and services were acquired for senior leadership and will be issued as part of the orientation process early in calendar year 2009. OCIO issued a memorandum to ensure that continuity of operations representatives supporting senior leadership are issued mobile communications devices, Government Emergency Telecommunications Services, and Wireless Priority Services. Provisions were made for fixed secure satellite communications capabilities at COOP facilities. COOP facility circuits were upgraded with Telecommunications Service Priority assignments. OCIO began working with individual agencies to extend equipment and service compatibility with NCSD 3-10 requirements throughout the Department. OCIO also updated the communications annex of the USDA Headquarters COOP Plan, incorporating NSCD 3-10 requirements.

OCIO established geographically separated primary and alternate points-of-contact to manage priority services within each USDA component agency and staff office. This has resulted in highly effective support for priority service requests prior to and after national disaster events, such as Hurricane Gustav in 2008.

After USDA field offices experienced extended power outages following Hurricanes Katrina and Rita, the Department became a key contributor to a National Communications System Report to the President on *Communications Dependency on Electric Power*. The Department sponsored a group of graduate students from Johns Hopkins University to research telecommunications infrastructure vulnerabilities to electric power outages. Additionally, USDA personnel examined existing documentation and processes that address interdependencies between telecommunications infrastructure and the electric grid, and produced diagrams and tables illustrating resource strengths and weaknesses. USDA provided regular status reports to the Committee of Principals on working group progress.

USDA Radio Program: OCIO submitted lessons learned to the National Telecommunications and Information Administration (NTIA) regarding the relocation of Forest Service microwave systems to accommodate the Federal Communications Commission auction of 4,000 USDA frequencies under the Commercial Spectrum Enhancement Act. USDA contributed the largest number of frequencies to the auction and has released all but 138 frequencies to date. Only four major systems remain in remote, mountaintop locations. Their replacement requires specialized personnel with experience replacing microwave systems in non-traditional environments. The Forest Service anticipates their replacement late in the third quarter and/or early in the fourth quarter of 2009, which will fall within the final timeline schedule submitted to the NTIA by the USDA during the Fall of 2006.

USDA paid $1.4 million in spectrum management fees to the NTIA in FY 2008 and will pay $1.3 million in FY 2009 based on a reduction in frequency assignments. The primary use for Federally assigned radio frequencies is to support the Forest Service mission to fight Wildland fires.
OCIO participated in working group activities to produce the National Emergency Communications Plan (NECP) and is contributing to an intergovernmental reference library hosted by the Department of Homeland Security Office of Emergency Communications.

Secure Communications: USDA completed the build-out and certification of a secure communications facility to provide shared enterprise access to the Homeland Security Data Network (HSDN) through a Federal partnership with the Department of Homeland Security. The HSDN supports the transmission of classified data.
In addition, USDA joined the Committee on National Security Systems (CNSS) as an observer, and is engaging in data calls and policy reviews. USDA is currently leading a CNSS "tiger team" in updating the CNSS wireless policy, CNSSP-17.

Intrusion Detection: OCIO continues to improve the security management of Departmental networks by hardening the Department's Intrusion Detection System to detect and mitigate intrusions that could potentially compromise or damage critical information assets. In FY 2008, OCIO, working with the Department of Homeland Security (DHS), implemented the United States Computer Emergency Readiness Team's (US-CERT) Einstein system with USDA. This system augments the Department's intrusion detection capability and allows US-CERT to expand its information gathering and government-wide threat detection.

Telecommunications Policy: USDA was tapped to lead a National Security Agency Wireless Policy Team made up of representatives from twelve Departments and agencies to update the *Committee on National Security System Policy No. 17, National Information Assurance (IA) Policy on Wireless Capabilities.*

Asset Management: USDA has used its collective buying power to establish a number of Enterprise agreements for IT hardware, software and services that are security-specific. OCIO has led these efforts by identifying products that many USDA agencies purchase and then establishing a lead agency for each Enterprise agreement. USDA continues to research an asset management approach that provides for strategic consolidations and the elimination of duplicative efforts.
USDA detailed an OCIO representative to the General Services Administration to support the Federal Strategic Sourcing Wireless Initiative (FSSI) to issue a blanket purchase agreement for Telecommunications Expense Management Services to track and control expenditures for telecommunication rate plans. The FSSI team was successful in awarding a contract to three vendors. USDA helped create and review the Statement of Work and participated on the vendor selection panel.

Enterprise Data Centers: USDA released its Enterprise Data Centers and Critical Systems memo on January 4, 2008, requiring critical IT to be hosted in the Department's ESS data centers. These critical information technology solutions include mission critical systems, mixed-financial systems, disaster support systems, incident response systems, and information systems that handle privacy, sensitive and personal identifiable information (PII).

Core Applications Systems Framework Model: Security vulnerabilities exist in a number of areas including software application and processes. In the fourth quarter of FY 2008, the OCFO established a Core Application Systems Framework (CASF), which will be used as a foundation for all IT solutions at USDA. This is also the foundation for the Department's Enterprise Architecture to support the customers and business requirements of the mission of USDA. By establishing a CASF, the Department's technology can be developed and integrated in the most efficient, low cost manner to provide the proper level of security and controls.

Trusted Internet Connections: OMB Directive (M-08-05) titled, "Implementation of Trusted Internet Connections (TIC)" is intended to create a secure cyber defense perimeter between the Federal government and the Internet. During FY 2008, USDA staff participated in many working group sessions with OMB to develop the TIC requirements. USDA has two Internet Gateways. Many of the TIC requirements are currently being met under the Universal Telecommunications Network contract.

Selected Examples of Recent Progress:

Systems Certification and Accreditation:
USDA continues its efforts toward improving its C&A process. The concurrency review, for instance, is designed to increase oversight and improve the quality; accuracy and efficiency of documentation that supports the C&A process. Originally implemented in FY 2006, the concurrency review process is made more robust each year. In FY 2007 the process ensured that C&A packages met minimum IT security requirements; in FY 2008, the strictness of the review increased and additional documentation requirements were scrutinized including improving the privacy assessments. The focus in FY 2009 will be on improving the quality of C&A documentation submitted to identify and correct root causes of non-compliance. Reviewers have worked with agencies individually to improve agency C&A documentation and mitigate weaknesses. Plans of action and milestones are established to address non-critical deficiencies noted in concurrency reviews. Currently, over 90 percent of all USDA agency and contractor systems have been certified and accredited. In its 2008 FISMA report, the Office of Inspector General recognized the improvement in the Department's C&A process as a result of the concurrency review process.
The C&A policy, guides, and document templates were updated in FY 2008, and OCIO continues to refine it processes and expand on its training and compliance work to ensure USDA has an effective C&A process. In FY 2009, OCIO will continue to use a blanket purchase agreement for agencies to use in acquiring the services of qualified C&A contractors; and will expand its education of agencies and contractors using lesson learned sessions.

Information Survivability:
OCIO continues its efforts to improve information survivability. USDA will continue to provide a centralized storage capability for disaster recovery plans and is now using CSAM tool as the data repository. CSAM also maintains artifacts of agency disaster recovery testing. OCIO sponsored and worked with the Department's Contingency Planning Working Group to develop NIST compliant templates for disaster recovery planning.

In FY 2009, OCIO continues its efforts on improving the Department's information survivability by conducting reviews of agencies' plans and the quality and effectiveness of their testing.

Security Awareness and Training:

- USDA has an aggressive security awareness program that uses the ISSLOB for security awareness training as its foundation. This program is supplemented with town-hall meetings for individuals that are not able to take the on-line training, an active communications strategy that notifies individuals of the requirement to take the training. This year, USDA implemented a program that requires individuals to review a banner that identifies safe computing practices and protecting personally identifiable information before being allowed to access computing resources. USDA also instituted a poster contest that highlights safe computing and protecting information.

- Nearly 98 percent of Agriculture personnel received security awareness training in FY 2008.

Federal Desktop Common Configuration (FDCC) and Department-wide Security Monitoring Tools:

- In March 2007, OMB required the deployment of FDCC to all systems that employ Windows XP and Windows Vista. To ensure compliance with OMB 07-11 and 07-18 requirements, USDA assigned an FDCC lead to direct agency/staff office coordination; provide Departmental updates; and facilitate consolidated communications to OMB, NIST, vendors and other entities as required. An FDCC working group was established with security and technical representatives from USDA agencies and offices. To date, seven agency/offices have met all the testing requirements of FDCC. USDA will continue to test FDCC settings with its mission critical applications, and implement those FDCC settings. USDA will continue its efforts until it is 100 percent compliant with the FDCC requirements.
- USDA has developed and awarded an enterprise security tools acquisition that will greatly enhance the Department's ability to proactively monitor its network from end-to-end, and more quickly respond to IT security threats. Implementation of the tools selected under this acquisition will provide the Department with a standard set of tools across all agencies that will allow for centralized monitoring and reporting of inventory, file and application management, data loss prevention, vulnerability scanning and penetration testing.

Updated Incident Handling Procedures:

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

Information Security Technical and Management Controls:

- Continued efforts with the Chief Financial Officer toward improving information security though the Department's Executive Steering Committee, aimed at focusing attention and necessary resources to remove the Department's information technology material weakness;
- Worked with the Department of Justice ISS LOB to improve reporting capabilities so that the impact of security weaknesses across the Department can be seen at a glance; and
- Developed, coordinated and submitted the first USDA Strategic Spectrum Plan to the NTIA in accordance with the President's Spectrum Policy Reform Initiative.

Expanding Electronic Government: Information Technology Governance:

Current Activities:

Enterprise Architecture: The use of an Enterprise Architecture (EA) is key to providing the technology data and information that is essential for the Department to achieve its goals and objectives. Moreover, the Clinger-Cohen Act of 1996, the eGovernment Act of 2002, and guidance from both OMB and the Government Accountability Office (GAO) have all encouraged or in some cases mandated the development and use of EA in order to effectively manage and make IT investment decisions more prudent.
The USDA EA Program is a collaborative effort between OCIO, USDA agencies, and supporting EA communities through membership, and active participation. For example, OCIO reviews and provides comments on EA Practice Guides and criteria for assessments for the Industry Advisory Council. Based on the Federal Enterprise Architecture Reference Models, USDA developed a current architecture, target architecture, and transition plan. USDA's Department-wide EA effort provides a "corporate" view of an EA, and builds on the architectures already under development within USDA's agencies. At the center of the USDA EA knowledge base is the EAR that supports the basic elements of the architecture. This system

can be aligned with other knowledge repositories based on common key data points. It also enables the creation of value-added reports, the sharing of key information, the development and storage of models, and other important functions.
Primary users of the USDA EA include strategic planners, enterprise architects, business process owners, program managers, project managers, vendors, budget officers, investment decision-makers, acquisition personnel, developers, and security personnel.
USDA is currently focused on the development of its EA. This analysis identifies areas of duplication and redundancy across the Department, and highlights opportunities for collaboration. This can result in substantial savings from common purchases and through the redundant expenditures on resources. In FY 2009, USDA will continue to develop its data, security, and technical architectures.

FY 2009 EA activities include:

- Integration of EAR with the USDA eAuthentication Service;
- Continued development of executive and management reports and dashboards;
- Enhancement of data quality through the development and implementation of data entry templates; and
- Development of training DVD for Adaptive 4.2.

Capital Planning and Investment Control (CPIC)
OCIO is responsible for ensuring that the Department's IT investments deliver products that result in an effective and efficient set of business benefits to agencies. The outcome of this work is oriented around the assurance of a positive return on the investment in IT within the USDA for taxpayers. To accomplish this goal, USDA established the CPIC Program in 1997 for selecting, managing, and evaluating the results for all major IT investments. The Department's E-Board, which is chaired by the Deputy Secretary and is made up of the Subcabinet, is the CPIC senior authoritative body at USDA that is charged with the oversight of all investments categorized as "major," according to OMB protocol. Capital planning requirements for investments that are not considered in the "major" category are managed by the OCIO Capital Planning Division, under the guidance of the Information and Technology Management unit, and are done so with consideration to government "best practices," as well as OMB Federal Acquisition Regulation and USDA official guidance.
CPIC is a key component of USDA's Integrated Information Technology Governance Process (IGP) and 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;
- Evaluate alternative options using a cost/benefit/return profile;
- Meet security mandates, as well as commonly accepted standards;
- Manage the use of telecommunications technologies and resources;
- Support the PMA;
- Conform to Federal EA standards applied within the Department;
- Manage the risks of the investment lifecycle; and
- Comply with Federal mandates (GAO, OMB, etc.) to include appropriate guidance.

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

The key focus in FY 2009 continues to be the IGP. This is critically important to maturing the overall management of IT across USDA. OCIO is aggressively analyzing the details of its investment plans that were defined and completed in the FY 2010 IT investment budget cycle. Greater integration of these policies will occur as OCIO begins the FY 2011 IT investment budget cycle in January 2009. OCIO places significant focus on the use of EA, the quality of business cases, supporting project management documentation, and the use of earned value management (EVM) discipline to manage investments. In FY 2009, USDA will begin migration to a tool that will make it easier for agencies and OCIO staff to manage the IT portfolio.

IT Acquisition Approval Process: The IT acquisition approval process is an OCIO control activity that involves a technical review of USDA IT acquisitions for $25,000 and above for conformity with USDA, Federal Enterprise Architecture (FEA), PMA, USDA telecommunications standards and practices, IT security considerations, and the adequacy of IT investment supporting documentation. The OCIO works with agencies to ensure that approved IT acquisition requests provide the necessary information as part of the Integrated IT process for managing the USDA IT portfolio of major and non-major investments. USDA is working to automate the IT Acquisition Approval request process in FY 2009.

IT Workforce Planning and Development: USDA agencies participate in a wide variety of training and professional development activities to help ensure that USDA's IT workforce has the skills necessary to accomplish USDA's mission. This initiative, managed by the Office of Personnel Management (OPM), involved agency IT professionals, on a volunteer and anonymous basis, assessing competencies using a Web-based tool available for the Federal workforce. OPM provided analysis data of gaps for agencies to prepare their report and plans. As a requirement for the PMA, the OCIO continues to track USDA's IT Workforce proficiency across several key competencies.

IT Project Management: OCIO continues to provide IT Investment and Project Management training to improve the management of IT investments and to ensure efficient and cost-effective investments at USDA. Training supports project and earned value management, as well as performance-based acquisitions for IT. OCIO is currently managing one Project Management training course in Riverdale, Maryland. In FY 2009, OCIO plans to offer these trainings online via AgLearn.

Asset Management: In FY 2009, OCIO plans to expand Enterprise-wide acquisition solutions to the workstations (personal computers to include thin client devices, desktops, and laptops), office automation software, and database software. OCIO is in the process of finalizing a Departmental Regulation to provide workstation standards and standards for commercial off-the-shelf software that operate on the workstations. Standardized Enterprise workstation refreshment rates will enable USDA to maximize its investment in personal computer equipment while minimizing the use of out-dated technology that can have a detrimental effect on the overall IT infrastructure. These standards will enable USDA to increase effectiveness in acquiring and administering resources by promoting compatibility and interchangeability of workstation hardware and software; improve USDA's IT security position; and ensure that these standards are aligned with the EA business goals and processes.

OCIO will also perform more robust production utilization and pricing analysis to aid in determining software licensing strategies and hardware implementations. OCIO will undertake a significant pilot with smaller more efficient hardware devices as an alternative to more expensive office desktops.

Selected Examples of Recent Progress:

Enterprise Architecture: A strategic information asset base which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. A summary of EA accomplishments in FY 2008 follows:

- Implemented EA Value Measurement process;
- Developed EA process guide;
- Developed and implemented EAR executive and management dashboards;

- Continued full segment architecture build-out for the Geospatial and Human Resources Management LoBs;
- Utilized EA data to evaluate agency IT investments and acquisitions;
- Developed governance and configuration management programs;
- Continued support for the identification and refinement of the target architecture and transition plan;
- Continued development of common EA elements, particularly those supporting Enterprise-wide projects;
- Continued alignment of investments to the FEA Reference Models;
- Continued support of the EA Working Group and various tasks and activities associated;
- Upgraded EAR software, which provides greater ease of use and enhanced reporting capabilities;
- Continued alignment of USDA EA information to the FEA Reference Models;
- Supported NIST standards activities; and
- Supported EA communities of practice; specifically, the Chief Architects Forum, the Architecture and Infrastructure Committee, the Data Architecture Subgroup and the Enterprise Process Improvement Committee.

Capital Planning and Investment Control (CPIC): The USDA IT Investment Portfolio for FY 2008 included 269 investments funded at $2.3 billion; the OCIO used the IGP for conducting investment reviews to evaluate the FY 2010 business cases on all major and non-major investments. The work done in FY 2008 provided a marked improvement of these business cases over past years. In addition, the quality of documentation for these investments continued to improve, and enabled the Department to acquire supporting details concerning its IT investments critical for the management of the IT portfolio.
This work resulted in an improved authoritative knowledge base used to support investment planning and decision-making at all levels of USDA, which is the nucleus of OCIO's Integrated IGP. The knowledge base is being established using a combination of the EAR and capital planning datasets, as well as other quality project management-based datasets.
In conjunction with the processes for capturing the necessary data, OCIO defined a new IT governance structure that brings greater visibility to business transformation and cost saving opportunities. The governance structure employs standard system development life cycle disciplines and formalizes change planning and impact analysis processes. A summary of capital planning accomplishments in FY 2008 follows:

- Completed the FY 2010 IT investment review process;
- Provided leadership and technical documentation for meetings with senior officials from OCIO and all agencies and offices to discuss their FY 2010 IT budget requests;
- Reviewed all USDA FY 2010 IT investment documentation and assessed them relative to IT management "best practices." Worked closely with agencies in ongoing discussions and technical support to ensure excellence of documentation provided to OMB;
- Created detailed financial plans for better understanding the investments plans and creating opportunities for consolidation;
- Submitted deliverables to OMB on time as required in the PMA Scorecard and worked with OMB to provide additional documentation and answer questions concerning submission;
- For the first time at USDA, created a tool to provide near-real-time reporting and a feedback mechanism to support agencies with access to the FY 2010 budget document reviews;
- Developed an alternatives analysis for USDA's CPIC support tool and finalized meetings with capital planning staff across the Federal government and prepared and published a resulting report. Began migration to a cheaper, better tool that will make it easier for agencies and OCIO staff to manage the IT portfolio; and

- Earned Value Management:
  - 14 Investments are now ANSI-748 EVM compliant (including MIDAS, the Modernize and Innovate the Delivery of Agricultural Systems project, and the Financial Management Modernization Initiative);
  - Conducted a Lean 6 Sigma review of EVM reporting process and modified process accordingly;
  - Submitted monthly EVM Reports to OMB as required in Scorecard; and
  - Finalized the preparation for OMB approval of USDA EVM.

IT Acquisition Approval Process:

- Processed 220 Acquisition Approval Requests (AAR) with an asset value of $1 Billion (FY 2008 & FY 2009). Worked closely with agencies and offices to ensure excellence and accuracy in documentation for CIO approval;
- Revised AAR guidance document set, which will be published as a revision to Agriculture Acquisition Regulation (AGAR) 53;
- Created an AAR Web site on the OCIO Intranet;
- Developed a comprehensive AAR database, with significant reporting capabilities;
- Supported Lean Six Sigma process improvement analysis of the AAR process;
- Designed a proto-type automated AAR processing system;
- Successfully re-mediated three A-123 internal control deficiencies for the AAR process in the OCIO;
- Conducted 4 AAR orientation sessions as part of the Project Management Professional Training Program operated by OCIO and Robins-Gioia;
- Maintained threshold for IT investments requiring approval at $25,000 to ensure that Department is spending IT resources on its highest priorities; and
- Used the AAR process to attain USDA's IT architecture goals and to ensure that investments do not replicate services that are already available through a USDA solution or an inter-Departmental service provided through the President's e-Government Initiatives; services adhere to the Section 508 requirement for accessibility; telecommunication resources are shared at co-located office sites; and that much greater emphasis is placed on security.

Workforce Planning and Development: In FY 2007, OCIO outlined a plan to improve the proficiency of its current IT workforce in the USDA Gap Analysis Report in April 2007. The four mission critical occupations and corresponding competencies as identified by the OPM in the GS-2210 Federal occupational series are provided in Table 2 below.

Table 2: IT Mission Critical Occupations and Corresponding Competencies

Mission Critical Occupation	Corresponding Competencies	
IT Project Management	Decision Making	Leadership
IT Security	Information Assurance	Information Security/Network Security
Enterprise Architecture	Strategic Thinking	Technology Awareness
Solutions Architecture	Requirements Analysis	Information Technology Architecture

In July 2008, OCIO submitted an IT Workforce Gap Analysis Status report measuring progress toward closing the identified gaps through the third quarter of FY 2008. In September 2008, OCIO provided an update as a part of the government-wide Human Capital Management Report and provided projections for the IT Workforce through FY 2013. Through training and development, organizational intervention, and talent recruitment, USDA continues to close the current competency gaps in IT and work towards improving electronic government.

IT Project Management:
Sponsored by OCIO, USDA's IT Investment/Project Management training provides USDA IT professionals with skills, tools, and techniques needed to manage IT projects effectively. It also emphasizes the management issues encountered within the USDA CPIC process and other Federal requirements mandated by the Clinger-Cohen Act of 1996. The training covers Federal best practices as well as the nine knowledge areas specified by the Project Management Institute (PMI) in the Project Management Body of Knowledge, the industry standard for project management training. At the end of the training, participants are eligible to take the examination administered by PMI for Certification as a Project Management Professional. As of September 30, 2008, 576 USDA employees completed the training and 314 graduates passed the PMI exam and obtained professional certification as Project Managers (PM). Recent progress in IT Project Management includes:

- Provided leadership and coordination of training for a total of 104 graduates in FY 2008 – breakdown is as follows:
  - PM Class 24 Alexandria, VA – 19 students graduated February 2008;
  - PM Class 25 Alexandria, VA – 20 students graduated February 2008;
  - PM Class 26 Kansas City, MO – 25 students graduated March 2008;
  - PM Class 27 Kansas City, MO – 20 students graduated September 2008; and
  - PM Class 28 Alexandria, VA – 20 students graduated September 2008.
- Following are the current statistics on the PM Training Program:
  - Total PM Program Certified Count 314
  - PM Program Total 606
  - USDA PM Program Total 576

Asset Management:
In FY 2008, OCIO published a Departmental Regulation to provide workstation standards and standards for commercial off-the-shelf software that operate on the workstations. Blanket Purchase Agreements were established for IT hardware (servers, personal computers, laptops, tablets, monitors, printers, faxes, plotters and telephone systems). These acquisitions have allowed ITS, and the Office of Procurement and Property Management to streamline the purchase process and ensure that IT hardware and equipment is available to the SCAs in a timely manner to meet their program operations.

OFFICE OF THE CHIEF INFORMATION OFFICER
Summary of Budget and Performance
Statement of Goals and Objectives

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcome
Goal 1: Provide customers and employees with access to the information they need.	Objective 1.1: Enhance service delivery by: 1) improving citizens knowledge and access to USDA services, 2) Collaborating with public and private partners, and 3) Achieving internal efficiency through Department-wide solutions. Objective 1.2: Provide high quality, secure, and reliable telecommunications services to USDA agencies and customers, enabling them to obtain timely and accurate data.	Presidential e-Gov Initiatives Departmental e-Gov Initiatives Enterprise Architecture Telecommunications	Key Outcome 1: Customers and employees have access to the information they need.
Goal 2: Ensure the privacy of customer data and protection and safety of USDA information.	Objective 2.1: Strengthen the security of USDA information assets. Objective 2.2: Promote awareness and understanding of USDA Cyber Security Program by enhancing communications within all levels of USDA and implement mechanisms to enhance information sharing and interoperability among all agencies within USDA. Objective 2.3: Centrally manage and monitor all USDA network and security systems across the diverse USDA IT environment and intelligently and proactively mitigate security breaches and vulnerabilities.	Systems Certification and Accreditation Cyber Security Enterprise Architecture Security Operations Center	Key Outcome 2: USDA programs are delivered in a safe, secure IT environment that protects the confidential data of customers and program recipients.
Goal 3: Strengthen the management and use of USDA IT resources.	Objective 3.1: Focus IT spending on high priority modernization initiatives. Objective 3.2: Leverage security spending to ensure consumer trust in established and emerging IT services.	Capital Planning and Management Asset Management and Risk Assessment Asset Management and Risk Management	Key Outcome 3: USDA acquires, manages and uses IT resources in cost efficient ways; and achieves economies of scale. USDA demonstrates effective, efficient and proactive security practices and risk management strategies that demonstrate the trustworthiness of its IT resources, enabling private and public partners to expand their use of USDA IT services with confidence and reliance.

OFFICE OF THE CHIEF INFORMATION OFFICER

Selected Accomplishments Expected at the FY 2010 Proposed Resource Level:

- USDA agencies will continue integrating their online services with USDA's enterprise eAuthentication Service.
- Continue ongoing Certification and Accreditation (C&A) process for all new and continuing systems in its inventory.
- Document and maintain security costs for each system within each mission area.
- Cross-walk the Federal Information Security Management Act list of systems to the Enterprise Architecture Repository.
- Ensure IT Security is embedded in the system development life cycle.
- Complete consolidating security operations into a centrally managed facility for USDA in its Kansas City regional center (which will be funded through Working Capital Fund).
- OCIO will continue to offer a variety of training on Earned Value Management (EVM) and other project management issues.
- Staff will monitor agency updates to CIMR (USDA's name for the proprietary software, WorkLenz) to ensure that actual performance data is being tracked for all IT investments that meet USDA's EVM threshold. CIMR is the capital planning and EVM monitoring tool that USDA's agencies use to record IT investment data. In addition, it formulates investment files for the electronic submission to OMB.
- Staff will also monitor agency EVM process maturity. OCIO will continue to monitor IT investments on OMB's "watch list" to ensure the quality of the business case documentation is strengthened.
- Complete comprehensive security assessments of 100 percent of the network and infrastructure General Support Systems across USDA, as identified in the Cyber Security Assessment and Management tool.
- Stand up the Agriculture Security Operations Center (ASOC) program to provide continuous, 24x7x365 IT security monitoring, security trend analyses and incident response.
- Identify standard security tools and techniques for the ASOC; and create a corresponding multi-year, multi-vendor blanket purchase agreement for the USDA agencies use that both consolidates the technical approach and provides economies of scale in bulk purchasing.
- Provide real-time asset tracking and inventory data through enterprise deployment of BigFix™ software.
- Provide USDA CIO and senior managers with an effective monitoring and reporting tool that integrates real-time situational data into a common operating picture the overall USDA security posture.

OFFICE OF THE CHIEF INFORMATION OFFICER

Summary of Budget and Performance
Key Performance Outcomes and Measures

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

Key Outcome: Customers and employees have access to the information they need.

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

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

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

Key Performance Measures:
- Percent of USDA IT systems that are certified, accredited or otherwise authorized as being properly secured.
- Percent of identified population that completed annual security awareness refresher training.
- Number of program security reviews completed.
- Number of security incidents closed within 30 days.
- Number of General Support Systems inventoried, baselined, and assessed.
- Number of ASOC incident first phone calls that are answered live by an incident handler.

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

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

Key Performance Measures:
- Number of investments in USDA IT portfolio.
- Through the use of Earned Value Management, maintain 100 percent of USDA IT projects that are within 10 percent of cost/schedule/performance objectives.
- Number of ASOC-conducted penetration tests to validate the system security controls of the USDA General Support Systems undergoing certification and accreditation in FY 2010 (in accordance with NIST special publication 800-53).

Key Performance Targets:

Performance Measure	2005 Actual	2006 Actual	2007 Actual	2008 Actual	2009 Target	2010 Target
Increase return on investment (ROI) for eGovernment and Lines of Business (LoB) common solutions.	N.A.	5%	5%	5%	5%	5%
Percent of USDA IT systems that are certified, accredited or otherwise authorized as being properly secured.	90%	93.7%	100%	100%	100%	100%
Percent of identified population that completed annual security awareness refresher training.	90%	90%	99%	100%	100%	100%
Number of program security reviews completed	8	10	8	8	8	12
Number of security incidents closed within 30 days.	N.A	N.A	N.A	N.A	N.A	Est. Baseline
Number of General Support Systems inventoried, and assessed.	N.A	N.A	N.A	N.A	N.A	Est. Baseline
Number of ASOC incident first phone calls that are answered live by an incident handler.	N.A	N.A	N.A	N.A	N.A	Est. Baseline
Number of investments in USDA's IT portfolio.	320	300	300	300	300	300
Through the use of Earned Value Management maintain 100 percent of USDA IT projects that are within 10 percent of cost/schedule/ performance objectives.	Est. Baseline	100%	100%	100%	100%	100%
Number of ASOC-conducted penetration tests to validate the system security controls of the USDA General Support Systems undergoing certification and accreditation in FY 2010	N.A.	N.A.	N.A.	N.A.	N.A.	Est. Baseline

Full Cost by Agency Strategic Objectives

	Dollars in thousands		
	FY 2008	FY 2009	FY 2010
Strategic Objective 1.1: Enhance service delivery by: 1) improving citizens knowledge and access to USDA services, 2) collaborating with public and private partners, and 3) achieving internal efficiency through Department-wide solution.			
IT support to OSEC and Office of Communications			
Administrative Costs (Direct)	$1,200	$1,259	$1,290
Telecommunications Services and Operation			
Administrative Costs (Direct)	1,100	1,100	1,103
Strategic Objective 1.2: Provide high quality, secure, and reliable telecommunications services to USDA agencies and customers, enabling them to obtain timely and accurate data.			
Information and Technology Management			
Administrative Costs (Direct)	5,441	5,580	5,660
Total Costs	7,741	7,939	8,053
FTEs	22	22	22
Performance Measure:			
Increase ROI for e-Government and LoB common solutions	5%	5%	5%
Strategic Objective 2.1: Strengthen the security of USDA information assets.			
Strategic Objective 2.2: Promote awareness and understanding of USDA Cyber Security Program by enhancing communications within all levels of USDA and implement mechanisms to enhance information sharing and interoperability among all agencies within USDA.			
Cyber Security Program Office			
Administrative Cost (Direct)	$2,283	$3,341	$36,889
Strategic Objective 2.3: Centrally manage and monitor all USDA network and security systems across the diverse USDA IT environment and intelligently and proactively mitigate security breaches and vulnerabilities.			
Information Security and Compliance			
Administrative Costs (Direct)	1,417	1,453	1,474
Total Costs	3,700	4,794	38,363
FTEs	17	18	38
Performance Measure:			
Percent of USDA IT Systems that are certified, accredited, or otherwise authorized as being properly secured	100%	100%	100%
Percent of identified population that completed annual security awareness refresher training	100%	100%	100%
Number of program security reviews completed	8	8	12
Number of security incidents closed within 30 days	NA	NA	Est. Baseline
Number of General Support Systems inventoried, baselines, and assessed	NA	NA	Est. Baseline
Number of ASOC incidence first phone calls that are answered live by an incident handler	NA	NA	Est. Baseline
Strategic Objective 3.1: Focus IT spending on high priority modernization initiatives.			
Program Management Office			
Administrative Costs (Direct)	$502	$515	$555
Capital Planning and Other Strategic Goal 3 Activities			
Administrative Costs (Direct)	4,174	4,279	4,608
Strategic Objective 3:2 Leveraging security spending to ensure consumer trust in established and emerging IT services.			
Administrative Costs (Direct)	0	0	12,000
Total Costs	4,676	4,794	17,163
FTEs	23	23	28
Performance Measure:			
Number of investments in USDA's IT Portfolio	300	300	300
Through the use of EVM, increase the percentage of a USDA IT projects that are within 10% of cost/schedule/performance objectives.	100%	100%	100%
Number of ASOC tests controls undergoing C&A in FY 2010	NA	NA	Est. Baseline
Total Cost all Program	$16,117	$17,527	$63,579
FTEs	62	63	88