2017 President's Budget
Office of the Chief Information Officer

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 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 data center operations, application development 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 Enterprise Network Services 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 IT desktop and end-user services through the Client 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, 2015, there were 999 full-time permanent employees funded by appropriated, reimbursed, and Working Capital Funds.

OIG Reports – Completed

#88501-0001-IT	3/2012	International Technology Services Selected Controls Audit Report - This audit contained seven recommendations. OCFO has granted final action on all recommendations.
#88501-0001-12	8/2012	Review of Selected Controls of the eAuthentication System Report - This audit contained six recommendations. OCFO has granted final action on all recommendations.

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 11. Remediation action on remaining recommendations is ongoing. Closure on two recommendations is dependent on final publication of two Departmental Regulations (Privacy and IT Security Configuration Management)
#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 nine. Remediation action on remaining recommendations is ongoing.

#50501-01-IT	08/2011	USDA's Management and Security over Wireless Handheld Devices - The audit resulted in five recommendations for corrective action by OIG. Remediation actions are underway. Two recommendations are closed. Remediation actions are still underway and OCIO is in the process of documenting remediation actions status.
#50501-2-12	11/2011	Fiscal Year 2011 Federal Information Security Management Act Report - OCIO and OIG have reached Management Decision on all of the 10 recommendations from this audit. OCFO has granted final action on five. Remediation action on remaining actions is ongoing.
#50501-0001-12	4/2012	USDA's Configuration, Management and Security over Domain Name System Servers Report - This audit contained six recommendations. CIO and OIG have reached Management Decision on all recommendations. OCFO has granted final action on five recommendations. Remediation action on the one remaining recommendation is ongoing.
#88401-0001-12	08/2012	OCIO FY'S 2010 and 2011 Funding Received for Security Enhancements Report – This audit contained four recommendations. OCFO has granted final action on three recommendations. Remediation action on the one remaining recommendation is ongoing.
#50501-0003-12	11/2012	Fiscal Year 2012 Federal Information Security Management Act Report - This audit contained six recommendations. CIO and OIG have reached Management Decision on all recommendations. Remediation action on the recommendations is ongoing.
#50501-0004-12	11/2013	Fiscal Year 2013 Federal Information Security Management Act Report - This audit contained five recommendations. CIO and OIG have reached Management Decision on all recommendations. OCFO has granted final action on two recommendations. Remediation action on the remaining three recommendations is ongoing.
#88501-0002-12	8/2014	Management and Security over USDA's Universal Telecommunications Network Report - This audit contained 21 recommendations. OCFO has granted final action on 18 recommendations. OCIO and OIG continue to work closely to achieve Management Decision on the remaining three recommendations.
#50501-0005-12	9/2014	USDA's Implementation of Cloud Computing Services Report - This audit contained seven recommendations. CIO and OIG have reached Management Decision on all recommendations. OCFO has granted final action on two recommendations and remediation action on the remaining five recommendations are ongoing.
#50501-0006-12	11/2014	Fiscal Year 2014 Federal Information Security Management Act Report - This audit contained two recommendations. OCIO and OIG have achieved Management Decision on the two recommendations and remediation is underway.
#50501-0006-12	11/2015	Fiscal Year 2015 Federal Information Security Management Act Report - This audit contained 4 recommendations. OCIO is currently working on the sixty - day response.

GAO Reports - Completed

#11-42SU	3/2011	Wireless Network Security: GAO closed all recommendations as implemented based on the USDA provided evidence.
#11-751	3/2011	Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards: GAO closed all recommendations as implemented based on the USDA provided evidence.

GAO Reports – In Progress

#08-525	6/2008	Information Security - Federal Agency Efforts to Encrypt Sensitive Information are Under Way, but Work Remains - 1/24/11 – The report contained three recommendations. GAO closed two recommendations as implemented. GAO closed the remaining one recommendation as not implemented. They found that USDA had not developed and implemented procedures for encryption key establishment and management.
#12-756	7/2012	Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned – USDA has provided periodic GAO updates on progress against the two recommendations directed to USDA. Progress has been made in addressing the recommendations but additional work needs to be completed in FY15.
#12-629	7/2012	Information Technology Cost Estimation: Agencies Need to Address Significant Weaknesses in Policies and Practices - USDA has provided periodic updates to GAO on progress against the two recommendations directed to USDA. Progress has been made in addressing the recommendations but additional work needs to be completed in FY16 to develop policy and guides for Information Technology Project Cost Estimating.
#12-791	9/2012	Organizational Transformation: Enterprise Architecture Value Needs to Be Measured and Reported - USDA has provided periodic updates to GAO on progress against the two recommendations directed to USDA. We are awaiting a response on whether the evidence we provided is sufficient to close the recommendations.
#13-524	6/2013	Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects - USDA has provided periodic updates to GAO on progress against the one recommendation directed to USDA. Progress has been made in addressing the recommendations but additional work needs to be completed in FY16 to mature the TechStat process.
#14-65	11/2013	Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings - USDA has provided periodic updates to GAO on progress against the four recommendations directed to USDA. Progress has been made in addressing the recommendations but additional work needs to be completed in FY16 to mature the PortfolioStat process.
#14-44	02/2014	Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation - USDA has provided periodic updates to GAO on progress against the one recommendation directed to USDA. Progress has been made in addressing the recommendation but additional work needs to be completed in FY16 to issue a policy and to mature the Data Integrity Board process.
#14-413	05/2014	Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide – USDA developed and submitted to GAO a Statement of Action to address the five USDA recommendations in July 2014. USDA is in the process of implementing actions to expand and mature software license management practices across the Department.

#14-713	09/2014	Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings. USDA has provided periodic updates to GAO on progress against the one recommendation directed to USDA. Progress has been made in addressing the recommendation but additional work needs to be completed in FY16 to report all data center consolidation cost savings and avoidances to OMB in accordance with established guidance.
#14-753	09/2014	Cloud Computing: Additional Opportunities and Savings Need to Be Pursued – USDA developing a Statement of Action to address the two USDA recommendations. USDA is in the process of developing guidance to ensure that all IT investments are assessed for suitability for migration to a cloud computing service.
#15-431	08/2015	Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services. USDA has submitted the Statement of Action and remediation is underway for the two recommendations.

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Item	2014 Actual		2015 Actual		2016 Enacted		2017 Estimate	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
Salaries and Expenses:								
Discretionary Appropriation	$44,031	115	$45,045	111	$44,538	136	$65,716	225
Rescission	-	-	-	-	-	-	-	-
Sequester	-	-	-	-	-	-	-	-
Adjusted Appropriation	44,031	115	45,045	111	44,538	136	65,716	225
Lapsing Balances	-318	-	-119	-	-	-	-	-
Obligations	43,713	115	44,926	111	44,538	136	65,716	225
Obligations under other USDA appropriations:								
Reimbursements:								
Geospatial IS	8,130	-	8,952	-	8,507	-	8,507	-
NTIA Spectrum	1,784	-	2,190	-	2,332	-	2,332	-
Other Activities	507	-	348	-	348	-	348	-
Total, Agriculture Appropriations	10,421	-	11,490	-	11,187	-	11,187	-
Working Capital Fund: a/								
Information Technology	474,041	855	415,915	844	388,966	937	397,724	978
NITC (Non-USDA)	19,626	32	31,067	41	40,473	83	39,917	48
Capital Equipment	-	-	-	-	-	-	-	-
Purchase Card Rebate	-	-	-	-	-	-	-	-
Total, WCF	493,667	887	446,982	885	429,439	1,020	437,641	1,026
Total, OCIO	547,801	1,002	503,398	996	485,164	1,156	514,544	1,251

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 a/

Item	2014 Actual			2015 Actual			2016 Enacted			2017 Estimate		
	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total
ES.....	7	-	7	7	-	7	7	-	7	7	-	7
GS-15.....	18	4	22	18	4	22	20	4	24	32	4	36
GS-14.....	50	6	56	46	6	52	48	6	54	84	6	90
GS-13.....	13	7	20	16	7	23	19	7	26	53	7	60
GS-12.....	10	3	13	12	3	15	12	3	15	18	3	21
GS-11.....	4	-	4	4	-	4	4	-	4	5	-	5
GS-10.....	1	-	1	1	-	1	1	-	1	1	-	1
GS-9.....	4	-	4	3	-	3	3	-	3	3	-	3
GS-8.....	1	-	1	1	-	1	1	-	1	1	-	1
GS-5.....	-	-	-	1	-	1	1	-	1	1	-	1
GS-4.....	1	-	1	-	-	-	-	-	-	-	-	-
Total Perm. Positions.....	109	20	129	109	20	129	116	20	136	205	20	225
Unfilled, EOY	14	-	14	18	-	18	-	-	-	-	-	-
Total, Perm. Full-Time Employment, EOY.....	95	20	115	91	20	111	116	20	136	205	20	225
Staff Year Est.....	109	20	129	91	20	111	116	20	136	205	20	225

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

OCIO-Client Technology Services (CTS) 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-CTS 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. CTS 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. CTS 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. CTS also use the fleet to address issues with malfunctioning IT equipment at these locations.

All vehicles are leased through GSA. For 2017 OCIO has no plans for adding vehicles to fleet. 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 CTS' ability to meet our Service Level Agreements.

OCIO's current fleet is based on mission and geographic needs. As of September 30, 2015, CTS' has 257 leased GSA vehicles and NITC has 2 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. Replacement of approximately 52 vehicles and no increase has been proposed for 2017.

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.

OFFICE OF THE CHIEF INFORMATION OFFICER

MOTOR VEHICLE FLEET DATA

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

	Number of Vehicles by Type								
Fiscal Year	Sedans and Station Wagons	Light Trucks, SUVs and Vans		Medium Duty Vehicles	Ambulances	Buses	Heavy Duty Vehicles	Total Number of Vehicles	Annual Operating Cost ($ in 000)
		4X2	4X4						
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
Change	+38	-15	-2	0	0	0	0	+21	+$4
2015	164	77	18	0	0	0	0	259	$1,029
Change	+15	-4	-6	0	0	0	0	+5	-$115
2016	179	73	12	0	0	0	0	264	$914
Change	0	0	0	0	0	0	0	0	$0
2017	179	73	12	0	0	0	0	264	$914

OFFICE OF THE CHIEF INFORMATION OFFICER

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

For necessary expenses of the Office of the Chief Information Officer, [$44,538,000] $65,716,000, of which not less than $38,000,000 is for cybersecurity requirements of the Department.

Lead-off Tabular Statement

Budget Estimate, 2017	$65,716,000
2016 Enacted	44,538,000
Change in Appropriation	+21,178,000

Summary of Increases and Decreases
(Dollars in thousands)

	2014 Actual	2015 Change	2016 Change	2017 Change	2017 Estimate
Discretionary Appropriations:					
Office of the Chief Information Officer	$44,031	+$1,014	-$507	+$21,178	$65,716

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

Program	2014 Actual		2015 Actual		2016 Enacted		Inc. or Dec.		2017 Estimate	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
Discretionary Appropriations:										
Office of the Chief Information Officer	$44,031	115	$45,045	111	$44,538	136	+$21,178 (1)	+89	$65,716	225
Total Available	44,031	115	45,045	111	44,538	136	+21,178	+89	65,716	225
Lapsing Balances	-318	-	-119	-	-	-	-	-	-	-
Total Obligations	43,713	115	44,926	111	44,538	136	+21,178	+89	65,716	225

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Program	2014 Actual		2015 Actual		2016 Enacted		Inc. or Dec.		2017 Estimate	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
Discretionary Obligations:										
Office of the Chief Information Officer	$43,713	115	$44,926	111	$44,538	136	+$21,178 (1)	+89	$65,716	225
Total Obligations	43,713	115	44,926	111	44,538	136	+21,178	+89	65,716	225
Lapsing Balances	318	-	119	-	-	-	-	-	-	-
Total Appropriation	44,031	115	45,045	111	44,538	136	+21,178	+89	65,716	225

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. In addition to Departmental Administration funding used for human resources operational services, current year and budget year base funds may also be used to support expedited and enhanced classification, staffing and processing efforts.

(1) An increase of $21,178,000 and 89 staff years for the Office of the Chief Information Officer ($44,538,000 and 136 staff years available in 2016).

The funding change is requested for the following item:

a. An increase of $379,000 for pay costs ($60,000 for annualization of the 2016 pay increase and $319,000 for the 2017 pay increase).

The proposed funding level is needed to cover pay and benefit cost increases for existing staff. This will ensure adequate resources are available for the office to carry out its full range of responsibilities and support USDA program delivery.

b. An increase of $10,000,000 and 23 staff years for Cyber Security Assessments and Addressing Risk ($28 million and 62 staff years available in 2016).

The proposed funding is critical in providing design, implementation, and support for the Agriculture Security Operations Center's (ASOC) Big Data initiative, updating other cyber security tools, and acquiring additional, highly trained cyber security staff to meet the growing demands of cyber security threats and known vulnerability risks. This funding would allow ASOC to implement capabilities that address the President's Management Council (PMC) Cyber Assessment findings at USDA. (The PMC Cyber Assessment was an across-government inquiry that was the result of the OPM data breach.)

The Department's PMC Cyber Assessment findings also correspond to deliverables identified in the Office of Management and Budget (OMB) memorandum M16-04, Cyber Security Strategy and Implementation Plan ("CSIP") which include Federal Departments and Agencies (USDA/ASOC) addressing vulnerabilities and conducting activities that offer:

1. High value information and assets identification / protection;
2. Rapid cyber incidents detection and response;

3. Rapid incident recovery;
4. Recruiting / retaining highly-qualified Cyber security workforce talent; and
5. Efficient / effective technology deployment

The requested funding will be used to:

Implement Big Data architecture tools at an enterprise level, to collect and process security related meta-data (attacks, vulnerabilities) aimed at high value information and assets for the purpose of conducting behavioral analysis, malicious pattern identification, deep forensic analysis for incidents that potentially span multiple months, long-term security metrics and trending, and providing a scalable and adaptable data repository (to allow for rapid cyber incidents detection and responses, like black listing and emergency blocks). The Big Data tools will allow ASOC to apply predictive analytics to USDA network traffic in order to create a unique real-time profile of the network and monitor it against up-to-date government / commercial cyber intelligence threats and act accordingly. Big Data employs heuristic analytics and reporting designed to spot anomalous traffic patterns and when this data is combined with more traditional cyber security methods. Acquiring Big Data tools enables the ASOC analysts to have additional insight and allows an enhanced ability to monitor / deflect rogue activities aimed at high value information and assets and so that ASOC can alert the appropriate Agencies to take steps to identify, deflect and protect these high value assets (based on heuristic patterning of thousands of data pings that occur at any given moment in a 24 hour period).

Implement Cyber Security Governance and Compliance tools that integrate with the DHS Continuous Diagnostics and Monitoring (CDM) security tools, the ASOC security sensor array tools, and leverages automation of a subset of technical security controls. This further modernizes the USDA IT system inventory, enabling more accurate identification of high value information and assets, as well as contributes ***additional*** data to the USDA IT Security Dashboard across the Department (which is fed to DHS and OMB). These tools provide a consistent and effective approach to the Department's cyber risk management framework that applies to all risk management processes and procedures and will ultimately assist in reducing vulnerabilities across the Department, by identifying patching vulnerabilities and tracking them until they are addressed.

Restore funding that was previously reduced for the ASOC team responsible for the development and implementation of the IT security governance project in 2011 which, continues to be a major Federal Information Security Modernization Act (FISMA) audit finding for USDA that contributes strongly to the historically poor FISMA scores at the Department. Without this added funding ASOC cannot ensure that it has a consistent and effective approach to risk management that applies to all IT risk management processes and procedures within the Department. ASOC staff is responsible for providing a comprehensive governance framework for ensuring the effectiveness of information security controls that support federal operations and assets; establishing effective government-wide management and oversight of related information security risks, including coordination of the Department's information security efforts; and, providing both the development and maintenance of minimum controls required to protect the Department's federal information and information systems (all of which support USDA agencies' efficient / effective technology deployment for patching known system vulnerabilities).

All of these efforts when implemented will drastically reduce the PMC Cyber Assessment findings at USDA and will reduce the Department's across-the-board vulnerabilities noted in that assessment.

c. An increase of $500,000 and 3 staff years to implement and support the new Federal Information Technology Acquisition Reform Act (FITARA) legislation (no funding in 2016).

The proposed funding along with other funds will be used to hire staff to implement new policies, guidance, and processes associated with the requirements of the FITARA legislation. FITARA gives the Chief Information Officer (CIO) authority to enhance transparency, improve risk management in IT investments, and maximize benefits of the Federal strategic sourcing initiatives. The additional staff will review pre-budget and budget submission artifacts to satisfy the FITARA requirement that the CIO is involved in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily IT oriented).

Additionally, the new personnel will define the processes by which the program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives and to develop sound estimates of the necessary IT resources for accomplishing those objectives. This team will assist in the reviewing and approvals of the major IT investments portion of this budget request; work jointly with the CFO to affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and the IT Portfolio (formerly Exhibit 53) includes appropriate estimates of all IT resources included in the budget request. The team will define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources, assist Capital Planning and Enterprise Architecture in defining the development processes, milestones, review gates, and the overall policies for all capital planning, enterprise architecture, and project management and reporting for IT resources, and assist Office of Procurement and Property Management in developing a strategy, process, and procedure for approving the acquisition strategies or acquisition plans at the agency level.

d. An increase of $1,043,000 and no staff year for 508 compliance and accessibility tools ($663,000 and 3 staff years available in 2016).

The proposed funding is needed to procure a suite of tools used to test software applications, websites, and digitally published information for Section 508 accessibility and compliance. This tool will expand OCIO's capacity to discover and remediate issues within USDA digital publications to avoid future settlement costs related to Equal Opportunity Employment and Section 508 compliance matters. As a result of USDA not being able to properly equip the Section 508 Test and Training Center, over the past four years, USDA Office of Civil Right has paid out over $2.5 million in the last 4 years as a result of formal EEO disability complaints.

e. An increase of $7,600,000 and 44 staff year to develop a Digital Service team (No funding or staff years available in 2016).

At a very high level, USDA's strategy over Information Technology (IT) over the next several years is to optimize our assets and reduce our liabilities. The goal is to improve our ratio of spending for Development, Modernization, and Enhancement to spending for Operations and Maintenance. At a more tactical level, we will not try to tackle all IT investments at once, but rather will target our efforts toward building capacity in OCIO and those of USDA's component agencies with investments or projects most public facing, most imminent, and most capable of incorporating additional digital services talent into their project plans and budgets. Without the Digital Service Team resources it will take USDA longer to transition from the legacy technology that underpins many of the public facing systems in use today.

The success rate of government digital services is improved when agencies have digital service experts on staff with modern digital product design, software engineering and product management skills. To ensure agencies can effectively build and deliver digital services, the 2017 budget request includes additional funding for staffing costs to enable the Department to build Digital Service teams to manage the agency's digital services that have the greatest impact to citizens and businesses.

To support the development of the Digital Service Teams at each agency, OMB's United States Digital Services and the Office of E-Government (E-Gov) and IT will provide the following services and support functions:

- Support agencies in identifying quality talent to serve in the various digital service roles, particularly senior executive candidates.
- Serve as USDA subject matter experts to offer technical guidance and operational support to agency Digital Service teams.
- Assist agencies in addressing any other policy barriers (such as legal or security) that may arise during implementation.
- Support agencies in managing and developing program-related procurements (e.g. develop statement of objectives) to improve delivery of high quality digital services.

f. An increase of $1,656,000 and 1 staff year for Records Management ($1,893,000 and 13 staff years available in 2016).

The proposed funding will allow OCIO to create an electronic records management prototype for Records Group 16 (RG-16), which is comprised of the Office of the Executive Secretariat, Departmental Management, Office of Budget and Program Analysis, Office of the Chief Economist, Office of Communications, Office of Congressional Relations, Office of Inspector General, and the Office of the General Counsel. Benefits of this initiative include: improved performance and promotion of openness and accountability by better documenting agency actions and decisions; further identification and transfer to the National Archives and Records Administration (NARA) of the permanently valuable historical records through which future generations will understand and learn from our actions and decisions; and assistance to executive departments and agencies (referred to collectively as agencies) in minimizing costs and operating more efficiently.

The Records Management prototype will allow the USDA to proof out the requirements identified in NARA/OMB Policy M-12-18. With the prototype implemented, the department will be able to manage records in accordance to the file plan and records schedules identified by the agencies and staff offices. We will be able to retrieve and respond to FOIAs, Congressional, and Litigation Requests. It will also enable the department to transfer records to NARA electronically, reducing or eliminating the expense of paper records storage.

The agencies and Staff Offices can leverage the Record Group (RG)-16 Implementation via a seat cost model, thereby reducing or eliminating tool redundancy across the portfolio.

g. An increase of $0 and 18 staff years to convert 12 contractors and add six additional FTE in Security Operations (Cyber Workforce)

No additional funding will be used to convert twelve cyber security operations contract positions into federal positions and add six federal positions. The current contract rates for these skills far exceed the salary and benefits for skilled federal employees. This conversion would improve the Department's ability to provide a seamless continuity of operations for critical mission areas, specifically avoiding a lapse in service to the USDA Offices and Agencies due to fluctuations in support during contract wind-down / ramp-up. This would also allow ASOC to fully develop the surge support required to better manage the newly leveled requirements associated with two federally mandated cyber security programs: the President's Binding Operational Directive (BOD) and Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program.

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

State/Territory	2014 Actual		2015 Actual		2016 Enacted		2017 Estimate	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
District of Columbia..	$41,317	95	$42,506	91	$42,046	116	$63,184	205
Kansas City, MO.....	2,396	20	2,420	20	2,492	20	2,532	20
Obligations.....	43,713	115	44,926	111	44,538	136	65,716	225
Lapsing Balances.....	318	-	119	-	-	-	-	-
Total, Available.....	44,031	115	45,045	111	44,538	136	65,716	225

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects
(Dollars in thousands)

		2014 Actual	2015 Actual	2016 Enacted	2017 Estimate
Personnel Compensation:					
Washington D.C.		$10,536	$10,748	$12,824	$24,421
Kansas City, MO		1,873	1,907	1,942	1,961
11	Total personnel compensation	12,409	12,655	14,766	26,382
12	Personal benefits	3,413	3,749	4,171	7,317
13.0	Benefits for former personnel	1	-	-	-
	Total, personnel comp. and benefits	15,823	16,404	18,937	33,699
Other Objects:					
21.0	Travel and transportation of persons	167	186	209	254
22.0	Transportation of things	24	-	74	164
23.1	Rental payments to GSA	-	984	458	467
23.3	Communications, utilities, and misc. charges	874	457	558	642
24.0	Printing and reproduction	87	126	195	195
25.2	Other services from non-Federal sources	11,365	14,681	11,675	11,717
25.3	Other purchases of goods and services from Federal sources	12,949	10,097	11,981	14,239
26.0	Supplies and materials	429	680	216	256
31.0	Equipment	1,995	1,311	235	4,083
	Total, Other Objects	27,890	28,522	25,601	32,017
99.9	Total, New Obligations	43,713	44,926	44,538	65,716
DHS Building Security Payments (included in 25.3)		$ -	$124	$63	$69
Position Data:					
Average Salary (dollars), ES Position		$166,000	$170,000	$171,500	$173,215
Average Salary (dollars), GS Position		$104,722	$106,090	$108,537	$113,216
Average Grade, GS Position		13.6	13.7	13.8	13.9

Shared Funding Projects
(Dollars in thousands)

	2014 Actual	2015 Actual	2016 Enacted	2017 Estimate
Working Capital Fund:				
Administration:				
Beltsville Service Center	$46	$59	$70	$74
HR Enterprise System Management	-	-	8	8
Mail and Reproduction Management	140	9	205	172
Integrated Procurement System	395	436	446	443
Financial Management Services	582	301	367	313
Procurement Operations	2,613	3,675	4,168	3,960
Subtotal	3,776	4,480	5,264	4,970
Communications:				
Creative Media & Broadcast Center	17	2	17	23
Finance and Management:				
NFC/USDA	283	1,124	281	2,149
Controller Operations	953	1,355	1,399	1,250
Financial Systems	413	-	-	-
Internal Control Support Services	196	143	171	186
Subtotal	1,845	2,622	1,851	3,585
Information Technology:				
NITC/USDA	33,633	9,065	4,804	4,986
International Technology Services	6,279	12,825	12,566	12,486
Telecommunications Services	15,764	11,610	14,221	17,884
Subtotal	55,676	33,500	31,591	35,356
Correspondence Management	30	23	19	18
Total, Working Capital Fund	61,344	40,627	38,742	43,952
Departmental Shared Cost Programs:				
1890's USDA Initiatives	27	30	32	32
Classified National Security Information	-	11	11	11
Continuity of Operations Planning	19	23	23	23
Emergency Operations Center	22	25	26	26
Facility and Infrastructure Review and Assessment	4	5	5	5
Faith-Based Initiatives and Neighborhood Partnerships	2	4	4	4
Federal Biobased Products Preferred Procurement Program	3	-	-	-
Hispanic-Serving Institutions National Program	19	20	22	22
Honor Awards	1	1	1	1
Human Resources Transformation (inc. Diversity Council)	16	19	19	19
Identity and Access Management	63	74	74	74
Medical Services	6	13	17	17
People's Garden	5	8	7	7
Personnel and Document Security	54	47	47	47
Preauthorizing Funding	34	41	41	41
Retirement Processor/Web Application	5	7	7	7
Sign Language Interpreter Services	10	-	-	-
TARGET Center	9	15	16	16
USDA 1994 Program	7	8	9	9
Virtual University	18	22	22	22
Visitor Information Center	2	-	-	-
Total, Departmental Shared Cost Programs	326	373	383	383

	2014 Actual	2015 Actual	2016 Enacted	2017 Estimate
E-Gov:				
Budget Formulation and Execution Line of Business	1	1	1	1
Enterprise Human Resources Integration	21	23	21	21
E-Rulemaking	9	9	-	-
E-Training	26	30	31	-
Financial Management Line of Business	2	2	2	1
Geospatial Line of Business	-	-	8	13
Human Resources Line of Business	3	3	3	3
Integrated Acquisition Environment - Loans and Grants	18	21	-	-
Integrated Acquisition Environment	6	7	14	-
Total, E-Gov	86	96	80	39
Agency Total	61,756	41,095	39,204	44,374

OFFICE OF THE CHIEF INFORMATION OFFICER

Status of Program

The Clinger-Cohen Act of 1996 required the establishment of a Chief Information Officer (CIO) for all major Federal agencies. The Act 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.

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 wo (EAR), capital planning investment tools, and Enterprise IT Solutions. In 2015, AgLearn won two outstanding awards that reflect AgLearn's success in learning innovations, process improvement, marketing, and general program management. The Skillsoft 2015 Innovation Award for influencing learning in the public sector. The Brandon Hall Group¹s Excellence in Learning/Talent award which is associated with ELearning Magazine.

OCIO is working with the Department of Interior - Interior Business Center (IBC) and USDA National Finance Center (NFC) in pilots for ICAM-as-a-Service (ICAMaaS). USDA's ICAMaaS solution will enable federal agency customers of the NFC and IBC to use their own agency credentials to access NFC and IBC web-based HR and payroll applications via an E-Authentication service. This solution provides an improved user experience for NFC and IBC federal agency customers, promotes the use of PIV credentials across federal agency boundaries, reduces operating costs and simplifies security compliance.

USDA Participation in E-Government Initiatives: USDA participates in 11 E-Government Presidential Initiatives and Lines of Business (LoB). In 2016, the OCIO plans to provide $9,133,127 to fund 7 E-Government Presidential Initiatives and 4 Lines of Business (LoB) Initiatives (see "OCIO Funded E-Government Presidential Initiatives and Lines of Business" table). 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	
Integrated Acquisitions Environment (IAE)	
Integrated Acquisitions Environment (IAE) – Loans and Grants	
Grants.gov	

Enterprise Architecture: Enterprise Architecture (EA) 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 purpose of USDA's EA Program 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. The Enterprise Architecture Division (EAD) provided new insight into EA, encouraged new approaches, and implemented new ideas to improve the enterprise architecture planning and decision making processes across the USDA. The FY2015 accomplishments include:

- The EAD developed and published the first USDA EA Guide and two IT Standards regulations: "End User Workstation Configuration" and "Information Technology Standards" to standardize and establish a baseline for EA across USDA, and ultimately help component Agencies and Staff Offices establish and/or enhance their EA programs;
- The team developed an Application Rationalization Plan, which will provide a better understanding of the application landscape and identify and reduce redundancy and opportunities for consolidation, cost savings and cost avoidance;
- The EAD mapped all of the USDA investments and systems to the FEA Framework version 2 (Business Reference Model (BRM), Performance Reference Model (PRM), etc.);
- The team created architecture diagrams that provide the electronic communication processes and directional flow between connected systems;
- The EAD built alliances with Agencies and Staff Offices by collaborating with agencies CIOs and other key stakeholders to build strategic relationships and achieve common EA goals and requirements;
- EA training materials were developed and three training sessions were conducted department-wide in an effort to enhance EA knowledge and understanding;
- An USDA Enterprise Architecture Newsletter was developed, in order to improve EA awareness across the Department; and
- The Enterprise Architecture Repository (EAR) was rebuilt based on the OMB FEA version 2 and houses the system data, reference model data, and architectural diagrams.

Enterprise Architecture Planned Activities for 2016:

- Complete USDA Enterprise Architecture Departmental Regulation;
- Enhance Enterprise Architects value and awareness at USDA by completing and executing a communications plan;
- Achieve GAO Enterprise Architecture Management Maturity Framework at USDA;
- Enhance USDA's methodology and tools to allow agencies to align with common vision and architecture;
- Complete USDA Application Rationalization framework;
- Continue refining standards, conduct system mapping, and start building out system specific standards profile;
- Develop Agency-specific performance reports to enable analysis to identify areas and opportunities for improvement (engineering, consolidation, de-commissioning, etc.); and
- Participate in USDA investment technology and portfolio reviews to ensure business and IT optimization.

Capital Planning and Investment Control (CPIC) and IT Governance: CPIC is mandated by the Clinger-Cohen Act and Federal Information Technology Acquisition Reform Act (FITARA) that requires agencies to use a disciplined process to acquire, use, maintain and dispose of IT. One of the main goals of the program is to ensure alignment between Agency Program IT investments and USDA priorities throughout the investment life cycle. Investment reporting is done through quarterly reports to the Office of Management and Budget (OMB) as well as yearly Tech/Portfolio Stats with the USDA Senior Leaders.

The OCIO Capital Planning and IT Governance Division (CPIGD) is responsible for ensuring that the Department's IT investments deliver products that result in business value to the agencies, while providing a positive return on the IT investments for taxpayers. The Department's Executive IT Information Resources Board (E-Board) serves as the USDA senior authoritative body charged with the oversight of IT investments with consideration to government "best practices," as well as OMB's Federal Acquisition Regulation and USDA official guidance.

Capital Planning and IT Governance 2016 activities will include:

- Continue training Executive Board members, CIO Council, CPIC Administrators, Program and Project Managers, Enterprise Architecture Community, Agency and Staff office CIOs on the Enterprise IT Governance process and framework - Training 201;
- Successfully manage and process Agencies and Staff Offices Acquisition Approval Requests on the behalf of the USDA CIO in collaboration with Office of Property and Procurement Management Senior Procurement Executive (SPE) and CFO;
- Continue to provide expert guidance regarding the revised OMB and Federal Acquisition Institute (FAI) Policy on Federal Acquisition Career Program and Project Managers (FAC-PPMs) certification program;
- Provide FAC-PPM training for USDA IT Investment Program Managers and certify applicants FAC-PPM levels 1-3;
- Lead and coordinate the quarterly PortfolioStat and Integrated Data Collection (IDC) required by OMB;
- Coordinate the requirements of the OMB led FedStat for the CIO and Deputy Secretary; and
- Lead and coordinate the USDA TechStat review process.

Information Management: Information management (IM) is the collection and management of information from one or more sources and distributes that information to one or more audiences. USDA's current information management environments comprise legacy information resident within LoB applications; e.g.: Enterprise Content Management (ECM), Electronic Records Management, Business Process Management, Email Management, Information Organization and Access, Knowledge Management, Web Content Management, Document Management and Enterprise 2.0 technology solutions. 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 digital channels including mobile phones and web interfaces.

Information Management Program plans for 2016 include:

- Conduct a Digital Records Management pilot with one or more select agencies to evaluate using a version of National Archives and Records Administration's (NARA) Capstone approach to retrieve and store records and emails as permanent records for archiving. The pilot will define, test, validate, and implement filters on records and non-records currently stored in USDA's email archiving solution, to determine if the technology meets NARA's requirements.

- Initiate an Electronic Records Project (ERP) to test the integration of a sophisticated records management application with *USDA's* email archiving solution as an archive repository, and implement an electronic records management system for all electronic records including mail to meet the 2016 and 2019 requirements of the Managing Government Records Directive (MGRD).

- Promote mandatory records management training, Section 508 training, and partnering with USDA agencies to improve accessibility for persons with disabilities.

Policy and IT Strategic Planning: OCIO provided 193 reviews on 40 IT related Departmental Directives, Manuals, Notices, and other guidance. In addition, OCIO processed 35 non-IT related Departmental Directives, Manuals, Notices, and other guidance. There were over 49 new and revised IT directives in development to address key policy gaps, audit recommendations, and OCIO management priorities at the end of 2015. Based on a policy program assessment and roadmap conducted in 2014, OCIO initiated two projects in 2015: Workflow Tool Assessment, and Directives Improvement. The Workflow Tool Assessment identified the best tool to automate the directives workflow process. The Directives Improvement project generated a service catalog, refined metrics, and a defined communications plan. OCIO initiated the development of new policy training modules.

Privacy Office: 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 record by Federal agencies. In 2015, the Privacy Office established the USDA Connect Privacy Community Forum for policy collaborations, hot topics, and platform for agencies to share and highlight privacy awareness and communicate enterprise-wide. Agencies developed and shared newsletters, training resources, best practices, and industry standards. Improvements were made to Computer Matching Program Guidelines and Template, Privacy Impact Assessment, and work flow

process. Additionally, the Privacy Office became more involved with other OCIO initiatives including: Open Data Working Group (ODWG), Integrated Advisory Board (IAB), Federal Information Technology Acquisition Reform Act (FITARA), and Information Sharing Environment (ISE). The Chief Privacy Officer received an award and recognition from USDA's Assistant Secretary for Administration for efforts related to OPM's Data Breach Response and Cyber sprint. The Chief Privacy Officer served as the focal point of contact for USDA employees impacted by the OPM breaches, transforming the role of the Chief Privacy Officer from one of strictly oversight to one of enhanced outreach and communications. As information was released to agencies from OPM, six messages were crafted, modified and sent to all employees. Recognizing that email transmission was not enough, the Privacy Officer communicated to the Chief Information Officer Council and offered to meet with agency personnel to answer questions regarding the OPM breaches; the USDA Privacy mail box was leveraged to answer questions and provide guidance.

Freedom of Information Act (FOIA): In accordance with the FOIA, 5 U.S.C § 552, Presidential Memorandum for Agencies Concerning the FOIA (74 F. R. 4683) and the Attorney General's FOIA Memorandum for Agencies Concerning the Freedom of Information Act (75 F. R. 51879), the USDA must promptly disclose agency records to requesters unless withholding is permissible under one of the nine FOIA exemptions or three statutory exclusions.

In 2015, the Department processed 19,559 FOIAs, a 316 FOIA increase from the prior fiscal year. To accommodate the continued increase, the Policy, E-Government, and Fair Information Practices (PE&F) Division continued its execution of a plan to streamline processing procedures, increase productivity, and reduce backlog across the Department. This plan resulted in increased processing for the Department, a 20% decrease in PE&F's backlog, and a 12.63% decrease in the Department's overall backlog. To further facilitate the streamlining of the Department's processing procedures, PE&F in collaboration with the Office of the General Counsel General Law and Research Division (OGC-GLRD) and the FOIA Training Subcommittee continued development of its extended FOIA training module for USDA's FOIA professionals. Lessons 1-6 are scheduled for publication in early January while the remaining lessons are undergoing a legal sufficiency review by the OGC-GLRD.

Protecting Networks and Information - Prevent Malicious Cyber Activity

The Agriculture Security Operations Center (ASOC) is actively monitoring a rapidly growing volume of IT threat vector data for USDA. In 2015 ASOC created 2,006 incidents of those 697 were types of malicious code (phishing, malware, Trojans, bots etc.) The ASOC continues to evolve from detecting to preventing cyber-attacks through improved visibility into the network and inspection of web traffic. Sharing information across the enterprise will increase knowledge of our adversaries and their targets. Advances in USDA perimeter defenses are crucial to effectively stopping and repelling malicious activity from our IT resources.

Phishing is the attempt to electronically acquire sensitive information by masquerading as a trustworthy source. In 2016, the ASOC is deploying advanced anti-phishing resources to protect vulnerable USDA IT resources from phishing.

Improving Cyber Security Governance, Risk & Compliance capabilities are critical to the ongoing protection of the USDA IT infrastructure. System upgrades will provide the operational transparency needed to enable the USDA to proactively address operational IT infrastructure governance, risk management, and compliance risk identification and evaluation. Tying risks to mitigating controls and resolution tracking reduces their likelihood and impact, minimizing service interruptions. These improvements will support security programs and compliance management across the department, providing situational awareness and improving the USDA IT Security profile.

Detect, Analyze, and Mitigate Intrusions

The dramatic growth in the volume of USDA IT system generated data presents a situation where malicious activity is not detected due to the limitations of current security solutions. Upgrading the existing Intrusion Detection/Protection solution and increasing data storage capacity, processing power capability and analysis skills will provide actionable intelligence the ASOC needs to proactively improve IT security and agency program operations without service interruption. In 2016, the USDA will implement Big Data technologies to collect and process massive amounts of security related information for the purposes of:

- Conducting system and user behavior analytics;
- Identifying malicious patterns;

- Deep forensic analysis for incidents that potentially span multiple months;
- Long-term security metrics and trending; and
- Providing a scalable and adaptable data repository.

ASOC is focused on improving Incident Handling and Incident Response capabilities within USDA. This 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.

The ASOC has increased its Incident Response capability by adding staff to obtain full 24x7 Incident Monitoring and Response coverage. Additionally, the ASOC updated its Service Desk Incident ticketing/tracking system using the latest guidance from DHS US-CERT on Threat Vectors. The ASOC is coordinating USDA agencies to utilize this guidance and improve Service Desk Incident ticketing/tracking.

Continuous Monitoring

USDA has deployed a comprehensive and cohesive integrated security solution called the Security Sensor Array (SSA) that provides the foundation for USDA enterprise-wide security monitoring, detection, and protection. 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.

In 2016 the ASOC plans to review the design of the SSA to:

- Enhance visibility of USDA network traffic;
- Increase coverage of the security array; and
- Reduce/Re-use stacks that may have redundant or overlapping capabilities.

The ASOC provides system and service resources in support of the federally mandated Continuous Diagnostics and Mitigation (CDM) security program. This support will continue and expand to USDA agencies Department-wide.

Shaping the Cybersecurity Environment - Planning, Policy Development, Workforce Training, and Force Management

Expanded reporting requirements demand additional technical expertise and collaboration with USDA program area IT security staff to provide this data and meet program area needs. Federalizing the Cyber Security Liaison positions will improve Agency Liaison and Vulnerability remediation capability and capacity. Deploying Customer Relationship Management (CRM) software to capture and manage information about each USDA component agency and office will enable faster responses to security events. Additional expertise to develop and disseminate a comprehensive risk management strategy to agency program staffs will be required to increase USDA Cyber Security Governance, Risk & Compliance capabilities. Additional FISMA staff resources applied to conduct audits will improve USDA agency program compliance with FISMA requirements. Developing and updating IT security policy is a continuous, ongoing endeavor, which requires additional cyber security policy resources and expertise to properly meet USDA IT security needs. In 2016, OCIO will continue the cyber security remediation process to update aged cyber security policies and align them with FISMA, OMB, and NIST requirements.

In 2016, ASOC began addressing five of the twelve NIST SP 800-53 control families that need new or updated policies. Additional work on other cyber security policies in 2016 addresses gaps in the USDA IT security program identified by the OIG and the CISO. In 2017, ASOC plans to continue work on updating/superseding outdated cyber security policies so that USDA cyber security policy:

- Aligns to and complies with changes in Federal laws and regulations, evolving OMB requirements and DHS operational directives, current NIST SP 800-53 control families, and new and updated NIST guidance documents;
- Addresses gaps in the IT security program identified by the CISO; and
- Ensures policy gaps identified by OIG audits are addressed.

Shaping the Cybersecurity Environment - Public-Private Partnerships

In 2016, ASOC plans to upgrade the existing cryptographic devices and will continue its support of the secure video Teleconference System using DHS' Homeland Secure Data Network (HSDN) Secure Video Teleconferencing System. This system supports the USDA's participation in multiple Secret level teleconferences with multiple other Departments/Agencies and with our Foreign Agricultural Service staff assigned to various State Department locations across the globe. USDA continues to subscribe to classified communications services available via agreements with partner agencies versus developing, managing, and operating our own system.

Enterprise Project Management Services (EPMS) is focused on the strategic goals to align IT investments, improve security and optimize the use and value of information technology. As such EPMS leads Department-wide project implementations for the OCIO; some examples include:

- Microsoft Desktop and Office 365 (O365) email contracts. Under this contract, USDA will have an unlimited archiving capability which will result in a cost avoidance/reduction of service cost of approximately $12 million over three years. In addition to the savings on archiving, the USDA has saved over $19 million over the last 3 years based on A.T Kearney's evaluation of our contract. The contract also provides the following additional features:
  - Reduced maintenance (by Agencies) to maintain Office, Exchange Client acces licenses (CAL), and SharePoint CALs on their EA Enrollments.
  - Mobile device compatibility on Apple and Android devices.
  - The current contract requires the USDA to maintain a baseline minimum of 120,000 users. The USDA will be able to true down to this number. Under the existing contract there was no option to true down. True ups and true downs are processed on the anniversary date of the agreement.
  - SharePoint Enterprise is part of the E3 offering and will be available to all users. (Currently the USDA is licensed for only 40K users).
  - Data Loss Prevention
  - Hosted Voice Mail
- Windows 2003 - consolidation of support services. Not only does this contract ensure that USDA systems receive critical security patches but also ensures that it is done at a lower cost. The projected cost avoidance of the consolidated contract is expected to exceed $1.2 million for the almost 400 servers being supported.

- Salesforce platform – system owner for all of USDA. Having a single System Owner streamlines the Authorization and Assessment (A&A) process and reduces costs for all agencies. EPMS is now responsible for reviewing specific aspects of the A&A process for agency-specific Salesforce applications.

- Strategic Sourcing Early Opportunities – leading the workgroup and helped identify several opportunities that are being evaluated and implemented. Some of these opportunities include: consolidation of PC and Laptop purchases, Cisco purchase and support, renewal of ActiveIdentity software, Microsoft Office 365 software consolidation, Microsoft Premier Support, and digital signature.

- EPMS led the implementation of the IT Intern program and served as the program's first co-coach. The program is designed to strengthen the leadership skills of USDA IT employees through a proven combination of innovative coursework, best practices benchmarking, challenging action-learning projects and executive coaching – all tailored to the USDA IT workforce's unique operating environment. The program was a major success, resulting in 100% positive feedback by program participants and their managers and helped to launch

several successful projects including USDA's initial response to FITARA, the development of USDA's innovation lab, changes to IT support for wild land fire, and many other notable accomplishments.

- EPMS provided efficient contract support for over 31 contracts totaling more than $75 million. Several of these contracts required extensive work to monitor and maintain.

Selected Examples of Recent Progress:

Enterprise Architecture Division:
Revised and published Departmental Regulations 3170-001 "End User Workstation Configurations" and 3180-001"Information Technology Standards"

- Published USDA Enterprise Architecture Guide, USDA Enterprise Roadmap and Business Functional Activity Model;
- Established an Agriculture Information Exchange Standards;
- USDA System reconciliation and verification completed;
- Added reporting fields and Federal Enterprise Architecture codes to the Enterprise Architecture Repository;
- Coordinated USDA Agency Application Reference Model Data Call for OMB; and
- Completed USDA Bureau Enterprise Architecture training sessions.

Capital Planning and Investment Control (CPIC) and IT Governance:
OCIO led the implementation of USDA's Integrated Information Technology (IT) Governance Board which uses an Integrated IT Governance Framework (IITGF) to improve management of major IT investments. The IT Governance organization is made up of Department-level and Agency Executives responsible for making the investment decisions based on the performance of major USDA investments. The IITG is a comprehensive decision gate review that accommodates both traditional program/project management methodology (Waterfall) and the modular (iterative/agile) methodology.

Through partnerships and collaboration amongst the USDA Chief Executive Offices (CXOs), OCIO successfully submitted its Federal Information Technology Acquisition Reform Act (FITARA) Implementation Plan, and CIO Self-Assessment and CIO Delegation of Authority memorandum. OMB has used USDA's FITARA package as a model to assist other federal agencies with their FITARA planning efforts.

OCIO led the successful completion of the third USDA Portfolio Review where the agencies and staff offices briefed their entire IT portfolio to senior business and information technology executives. In addition, the OCIO Capital Planning and IT Governance organization implemented a new IT Portfolio Management tool called AgMAX. AgMAX enables OCIO to automate workflow and streamline acquisition approval processes, assist in choosing investment proposals, approve or disapprove the funding business cases. The USDA Portfolio Management process will facilitate a method to strategically prioritize, plan, and execute our IT enterprise suite of initiatives and investments. OCIO also developed an extensive Earned Value Management (EVM) Directive and Departmental Manual to enhance the effective planning and performance management of IT investments. Training on EVM methodology was developed and delivered to USDA Executives.

Policy and Planning: OCIO provided 193 reviews on 40 Departmental Directives, Manuals, Notices, and other guidance. In addition, OCIO processed 35-non-IT related Departmental Directives, Manuals, Notices, and other guidance. There were over 49 new and revised IT directives in development to address key policy gaps, audit recommendations, and OCIO management priorities at the end of FY15. Based on a policy program assessment and roadmap conducted in FY14, OCIO's policy division initiated and managed two projects in FY15. The Workflow Tool Assessment project mapped the workflows for all steps in the OCIO and Departmental policy clearance process. The Workflow Tool Assessment project also provided the cost benefit analysis and alternatives analysis for workflow solutions. The Directives Improvement project generated a service catalog, refined metrics, and defined a communications plan. OCIO initiated the development of new policy training modules.

Privacy Office: In 2015, the Privacy Office produced in collaboration with multiple agencies the first PII newsletter. The PII newsletter provides an overview of the Privacy Act, and how to protect personally identifiable information as well as how to report breaches.

Cyber Security: ASOC performs annual penetration testing of all agency/office environments and identifies vulnerabilities to provide actionable intelligence that supports timely remediation. As part of the process ASOC scans applications to verify secure coding is active to reduce accidental deployment of software with security vulnerabilities (including defects, bugs and logic flaws) that can be exploited.

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 2016, ASOC plans to oversee Agency migration of USDA IT Systems into the NIST 800-53 Revision 4 control sets (upon publication of NIST 800-53a Rev 4 control implementations), and continue to participate in the Department of Justice's CSAM Executive Advisory Board to provide input and guidance to refine the CSAM tool to meet FISMA requirements.

ASOC continues to support the Whitehouse's Cyber Security Strategy and Implementation Plan on behalf of the Department to identify / mitigate high value assets and systems, and to understand the potential impact to those assets. ASOC ensures robust security protections are in place while reducing vulnerabilities and intrusions through improved management of user accounts on Federal information systems.

Contracting Agreements/Strategic Sourcing: OCIO has led strategic sourcing efforts by using its collective buying power to establish or re-negotiate a number of enterprise-wide agreements for IT hardware, software and services. These new contracts include: Microsoft Office 365, Windows 2003, Salesforce, consolidation of PC and laptop purchases, Cisco purchase and support, Active Identify software, Microsoft Premier Support and digital signatures.

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 IT issues. OCIO provides leadership for the Department's information and IT management activities in support of USDA program delivery.

USDA Strategic Goal 5: *Create a USDA for the 21st century that is high performing, efficient, and adaptable*

USDA Strategic Objective 5.1: *Develop a customer-centric, inclusive, and high-performing workforce by investing in and engaging employees to improve service delivery*

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
Enable information as a strategic asset for decision makers and citizens at any level.	Enable innovative business driven solutions. Enable mobile workforce with information that is device independent. Develop, implement, and institutionalize a One USDA Digital Strategy. Promote data quality, transparency, accessibility, standardization, reuse, information sharing, cost saving/avoidance by minimizing redundancy rework, and collaboration.	Enterprise Architecture Open Data Initiative Records Management Freedom of Information Act (FOIA) Program Lean Six Sigma Capital Planning and IT Governance (CPIGD)	An enterprise architecture that includes a baseline architecture, target architecture, and a transition plan that is a strategic information asset base that defines the necessary information and enabling technologies to meet USDA's mission needs. A Transitional Roadmap that defines required process reengineering efforts and new technologies in response to changing mission needs. Increased quantity and quality of datasets released for public consumption and economic growth opportunities Increased access to enterprise-wide information to identify opportunities for shared services. Matured Controlled Unclassified Information Program Apply a standardized and rigorous framework for measuring IT investment's value to the Agency and department.

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
Develop a high-performing workforce to support the USDA mission today and tomorrow.	Improve Leadership Skills of IT Workforce. Promote a Customer-Centric, Agile, and Diverse Workforce. Develop a Professional Program Manager Workforce. Mature USDA's Compliance with 508.	IT Workforce Planning Team AgLearn IT Intern Program Enterprise Management 508 Accessibility Program Lean Six Sigma	Pipeline of trained leaders and IT Program Managers. Better managed IT investments with trained Program Manager Professionals An IT Program Management Career Field with formal training program and curriculum. An engaged workforce motivated and ready to improve the workplace Reduction of 508 claims against USDA

Key Performance Measures

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate/ Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.1	508	N/A	N/A	N/A	1%	1%	1%	Met	1%	45%

Allowable Data Range for Met The tolerance range for the measure to be "met" is +/- 5 percent. Range is determined by number of websites that are compliant with the to the Office of Communications (OC) provided by each Staff Office and Mission Area that maintains a website within USDA, state and local government supported (local & state USDA websites and International websites supported by USDA).

Assessment of Performance Data

Data source – The proposed solution, when implemented, automatically scans the USDA environment and identifies the number of USDA websites, and the % that complies with Section 508 mandates.

Completeness of Data – The 508 Compliance tool is an enterprise-wide appliance that scans the USDA network on a regular basis and produces reports which are reviewed by the 508 Program Manager and the Agency 508 Coordinator. Since websites are dynamic and change frequently, new or changes to existing pages may be missed for a few weeks but the data will be captured during the next scan and reporting cycle.

Reliability of Data – Since the tool is specificly manufactured to retrieve 508 compliance data, the data is reliable

Quality of Data – The quality and accuracy of the data is based on the metrics and guidelines established by OMB, the Access Board, GSA and Web Content Accessibility Guidance 2.0 compliance regulations.

Analysis of Results

Selected Past Accomplishments toward Achievement of the Key Outcome FY 2015:
OCIO has furthered the Secretary's goal in making USDA a model employer by launching a Section 508 Training and Testing Center that provides valuable assistance to agencies and staff offices in developing Section 508 compliant training material, briefings, and other documents. The center has been instrumental in getting employees with and without disabilities trained on accessibility equipment and software.

An Open Data Council and Open Data Working Group were established to implement Office of Management and Budget (OMB) Memorandum M-13-13, Open Data Policy. OCIO has collaborated with agencies to successfully facilitate quarterly submissions to the public via Data.Gov website; including 67 Disaster Relief Datasets to support USDA's Disaster Relief Portal Project. As of January 2016, USDA has published 721 data sets and 83 application programming interfaces (APIs); 568 datasets were releasable to the public and 153 non-releasable.

The OCIO has developed a comprehensive IT governance process that incorporates an integrated governance framework and provides the executive teams with a process for reviewing investments and providing guidance to investment managers throughout a project's Agriculture System Development Life Cycle (AgSDLC). The framework integrates Capital Planning, Program Management, Enterprise Architecture (EA), Security, and the budget process. USDA reviewers and decision-makers evaluate program performance on planning, acquiring, designing, developing, constructing, testing, implementing, operating, maintaining, and retiring IT, as well as on sound management of facilities, hardware, software, and personnel that are associated with those IT investments.

Selected Accomplishments Expected at the FY 2017 Proposed Resource Level/Challenges for the Future:

- USDA will be able to monitor all of its web sites for Section 508 compliance, and be able to provide proactive support in making documents compliant before posting to the web or distributing communications internally as well as externally. The program office will work collaboratively with agencies and staff offices to provide regular reports to designated individuals who are responsible for correcting non- compliant websites thus reducing lawsuits resulting from complaints.
- Continue training Executive Board members, Agencies Administrators, CIO Council, Capital Planning and Investment Control (CPIC) administrators, Program and Project Managers, Enterprise Architecture community, agency and staff office CIOs on the Enterprise IT governance process and framework;
- Full implementation of the Enterprise IT governance process and framework;
- Continue building Program and Project Manager work force using Federal Acquisition Career Program and Project Managers (FAC-PPMs) certification programs;
- Increase and promote Shared Service Solutions;
- Develop innovative programs that will improve our ability to recruit, and retain USDA IT talent; and
- Raise capability maturity of enterprise geospatial, remote sensing, and geographic information systems (GIS) to support complex policy and administration decision making.

The Capital Planning and IT Governance Division (CPIGD) continues to ensure alignment of IT investments with mission and business priorities through governance and sound portfolio management. To continue the improvement and compliance of adhering to the Clinger-Cohen Act of 1996 as well as OMB Circular A-11, CPIGD in collaboration with the Agriculture Security Operations Center (ASOC) has secured a portfolio management tool that will enable a single repository for Capital Planning & IT Governance which includes OMB required monthly and annual Investment submissions, CIO monthly and quarterly scoring and reviews of investments, Acquisition Approval Requests (AARs), Detailed Life Cycle Costs (DLCCs) updates, monthly and ad hoc required Earned Value Management updates, Re-baseline Performance Changes, IT Governance Decision Gates reviews and the CIO's Annual Portfolio Reviews of Agencies and Staff Offices. In addition, other OCIO critical partners will utilize the tool for their daily operational needs such as but not limited to the Enterprise Architecture, Cyber Security, and Information Management.

The EA organization completed a comprehensive redesign of the Enterprise Architecture Repository (EAR) to provide near real-time information on USDA's IT Portfolio. This effort supported the Federal Enterprise

Architecture Framework. In addition, the EA organization successfully coordinated Department-wide quarterly data calls to produce valuable information required by OMB.

Earned Value Management (EVM) Departmental Regulation and Manual were developed to enhance the skill level of IT Program Managers for major IT investments. Training on EVM methodology was developed and will be delivered to USDA Executives.

Major Investment Definition Directive, Non-Major Investment Directive, IT Governance Directive, and Capital Planning Directive were all developed to ensure Capital Planning and IT Governance on the behalf of the CIO provides guidance and policy direction to the agencies and staff offices of USDA regarding sound quality management over IT Investments.

USDA Strategic Objective 5.2: *Build a safe, secure, and efficient workplace by leveraging technology and shared solutions across organizational boundaries*

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
Protect and defend the enterprise information infrastructure, critical assets, and capabilities.	Produce timely and actionable intelligence on the state of the enterprise. Develop a cyber-security threat dashboard. Build a cadre of cyber security professionals ready to engage and implement a synchronized response.	Agriculture Security Operations Center Cyber Security Policy Remediation Intrusion Detection Incident Handling Program	Secure IT Systems and Infrastructire Modernize and streamline the security assessment process shifting the paradigm to continuous monitoring. Timely and actionable intelligence on the State of the Enterprise A cadre of well-trained Cyber Security Professionals

Key Performance Measures

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate/ Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.2.1	Patch and Vulnerability	N/A	N/A	N/A	N/A	N/A	N/A	N/A	90%	95%

Allowable Data Range for Met - The tolerance range for the measure to be "met" is +/- 5 percent. Range is determined by percent of patched vulnerabilities within 30 days of the common vulnerabilities and exposure (CVE) release date per DHS Cyber Hygiene Assessment report per DHS Binding Operational Directive 15-01.

Assessment of Performance Data

Data source – BigFix Security and compliance analytics, Enterprise Vulnerability Solution (EVS), ForeScout CounterACT, Continuous Diagnostics and Mitigation (CDM) Dashboard.

Completeness of Data – DHS scans critical vulnerability data on a daily basis.

Reliability of Data – Reliable; Critical vulnerability data is collected using DHS scanning tools.

Quality of Data – The data is generally regarded as being accurate.

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate /Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.2.2	Overdue POAMs	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Est baseline	10%
Allowable Data Range for Met - The tolerance range for the measure to be "met" is +/- 5 percent. Decrease in one day of overdue Plans of Actions and Milestones (POAM) for remediation and vulnerabilities. Metric will use an average number of days to calculate metric.										
Assessment of Performance Data										
Data source – Cybersecurity Assessment and Management Tool (CSAM).										
Completeness of Data – The data collected from Agencies and updated regularly. Limited outages have no statistically significant impact on the measures.										
Reliability of Data – Data is maintained on a monthly basis by Agencies and is deemed reliable.										
Quality of Data – The data is maintained by Information System Security Program Managers and are generally regarded as being accurate.										

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate /Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.2.3	Incident Management	N/A	N/A	N/A	N/A	80%	85%	Met	85%	86%
Allowable Data Range for Met The tolerance range for the measure to be "met" is +/- 5 percent. Number of incidents closed within 30 days.										
Assessment of Performance Data										
Data source – The Remedy call tracking system, and the Department of Homeland Security's US CERT system**.**										
Completeness of Data – There is a manual review process to compare the number of incidents detected by USDA and the number of incidents reported through USCERT.										
Reliability of Data – Very reliable; the data is provided to ASOC from USCERT Department of Homeland Security on a monthly basis.										
Quality of Data –The data is generally regarded as being very accurate.										

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate /Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.2.4	ATO	N/A	N/A	N/A	35%	65%	65%	Met	70%	80%
Allowable Data Range for Met The tolerance range for the measure to be "met" is +/- 5 percent. Cybersecurity Assessment and Management Tool (CSAM).										
Assessment of Performance Data										
Data source – Cybersecurity Assessment and Management Tool (CSAM).										
Completeness of Data – The data collected from Agencies and updated regularly. Limited outages have no statistically significant impact on the measures.										
Reliability of Data – Data is maintained on a monthly basis by Agencies and is deemed reliable										
Quality of Data – The data is maintained by Information System Security Program Manager and is generally regarded as being accurate.										

Analysis of Results

Selected Past Accomplishments toward Achievement of the Key Outcome in FY 2015:
The USDA ASOC – CISO must provide FISMA mandated oversight and enforcement to ensure compliance with federally mandated cyber security initiatives and requirements from the Office of Management & Budget (OMB), National Institute of Standards in Technology (NIST) and Continuous Diagnostics Mitigation (CDM) program oversight, and risk mitigation. Improve departmental cyber security risk management, cyber security policy, continuous monitoring, and overall strengthening information assurance and security throughout the Department through the following initiatives:

1. Cyber Security Policy Reform
2. Implementation of an overall cyber security compliance and enforcement framework to provide increased oversight and FISMA, OMB, and GAO cyber security audit functions in fulfilling Federal mandates and the Risk Management Framework (RMF).
3. Implement, integrate and support of the Continuous Diagnostics Mitigation (CDM) program from Department of Homeland Security (DHS), and resulting workload.

The primary purpose of this program area is to ensure the confidentiality, integrity and availability of all USDA IT Systems and infrastructure which are critical to the safety of the nation's food supply and natural resources. Attacks from inside and outsider threats increase exponentially. If USDA is to continue to protect its' business and mission objectives, we must be ever-vigilant in continuously monitoring the safety of our data and technological assets by:

1. Modernizing the Department's cyber security policy and procedures to comply with the requirements of FISMA and provide structure to the response(s) required by ever growing, modernizing threats.
2. Implement increased compliance oversight and enforcement of the overall Risk Management Framework (RMF) process, as well as FISMA, OMB, and GAO audits, and the CDM program. Each system that handles USDA data is required to undergo the Assessment & Authorization (A&A) (formerly Certification & Accreditation) (C&A) process. USDA must continuously ensure the confidentiality, integrity and availability as well as the quality of the data and remediation measures produced to ensure compliance with the President's Management Agenda, OMB, A-123 and FISMA mandates.
3. Development of a strategic model and implementation methods for an improved executive structure providing for the compliance and enforcement of cyber security as related to information technology resources, continuous protection from threats and organizational defenses and countermeasures.
4. Development of and implementation of investigation, reporting and remediation of compliance related issues to Department policies, guidance, processes and procedures.
5. Compliance reporting to outside agencies (e.g., FISMA, OMB, GAO, House Appropriations Committee) and internal OIG audits.

Expected Outcomes:

- Modernized Departmental cyber security policies and procedures that comply with FISMA, OMB, and NIST mandates.
- Integration of compliance and enforcement tools with operational toolsets for increased capabilities in CDM and continuous monitoring requirements.
- Department level compliance, oversight and enforcement model and resources to strategically provide increased oversight of both Department and Agency-level cyber security compliance as mandated by FISMA, OMB, and NIST.
- Comprehensive compliance testing for compliance validation and evidence as required.
- Improved advanced planning for centralized continuous monitoring and ongoing A&A activities in support of CDM.
- Addressing and mitigation of the longstanding IT Material Weakness identified by a history of OIG FISMA Audits in the following areas:
  a. Logical Access Control
  b. Physical Access Control
  c. Contingency Planning/Disaster Recovery Planning

d. Configuration Management
7. Comprehensive reviews of security topics critical to the Department, including security of emerging technology and practices.
8. Tighter integration of cyber security compliance requirements and security operations to support external reporting (FISMA, OMB, OIG, GAO, A-123, etc.)

The Agriculture Security Operations Center (ASOC) is actively monitoring a rapidly growing volume of IT threat vector data for USDA. The ASOC continues to evolve from detecting to preventing cyber-attacks through an improved visibility into the network and inspection of web traffic. Sharing information across the enterprise will increase knowledge of our adversaries and their targets. Advances in USDA perimeter defenses are crucial to effectively stopping and repelling malicious activity from our IT resources. The ASOC has increased its Incident Response capability by adding staff to obtain full 24x7 Incident Monitoring and Response coverage. Additionally, the ASOC updated its Incident ticketing/tracking system using the latest guidance from DHS US-CERT on Threat Vectors.

USDA has deployed a comprehensive and cohesive integrated security solution that provides the foundation for USDA enterprise-wide security monitoring, detection, and protection. The security solution will perform a mix of critical security functions in near-real-time including:

- Intrusion detection and prevention,
- Network data loss detection,
- Network behavior analysis,
- Malware detection and prevention, and
- Network packet analysis.

Developing and updating IT security policy is a continuous, ongoing endeavor, which requires additional cyber security policy resources and expertise to properly meet USDA IT security needs. OCIO released five key Department wide policies in the 2013 and 2014 while these published policies have superseded 13 outdated policies and will assist in closing 12 OIG audit findings.

Selected Accomplishments Expected at the FY 2017 Proposed Resource Level/Challenges for the Future:
ASOC is focused on improving Incident Handling and Incident Response capabilities within USDA. This includes the implementation of USDA Incident Handling Best Practices and Guides, integrated Department and Agency Incident Response Plans, 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.

The dramatic growth in the volume of USDA IT system generated data presents a situation where malicious activity is not detected due to the limitations of current security solutions. The USDA will implement Big Data technologies to collect and process massive amounts of security related information for the purposes of:

- Conducting system and user behavior analytics,
- Identifying malicious patterns,
- Deep forensic analysis for incidents that potentially span multiple months or agencies,
- Long-term security metrics and trending, and
- Providing a scalable and adaptable data repository.

Upgrading the existing Intrusion Detection/Protection solution and increasing data storage capacity, processing power capability and analysis skills will provide actionable intelligence the ASOC needs to proactively improve IT security and agency program operations without service interruption.

In 2016, OCIO will continue the cyber security remediation process to update aged cyber security policies and align them with FISMA, OMB, and NIST requirements. OCIO released five key Department wide policies in the 2013

and 2014 while these published policies have superseded 13 outdated policies and will assist in closing 12 OIG audit findings.

ASOC plans to upgrade the existing cryptographic devices and will continue its support of the secure video Teleconference System using DHS' Homeland Secure Data Network (HSDN) Secure Video Teleconferencing System. This system supports the USDA's participation in multiple Secret level teleconferences with multiple other Departments/Agencies and with our Foreign Agricultural Service staff assigned to various State Department locations across the globe. USDA continues to subscribe to classified communications services available via agreements with partner agencies versus developing, managing, and operating their own system

USDA Strategic Objective 5.3: *Maximize the return on taxpayer investment in USDA through enhanced stewardship activities and focused program evaluations*

Agency Strategic Goal	**Agency Objectives**	**Programs that Contribute**	**Key Outcomes**
Align IT investments with mission and business priorities.	Maintain alignment between Program IT investments and USDA priorities throughout the investment life cycle. Strengthen partnerships with business sponsors. Provide proactive stewardship of tax dollars to ensure IT investments deliver maximum performance.	Capital Planning IT Governance Enterprise Architecture	Alignment of IT investment with mission priorities and business goals. Poorly performing investments (programs or projects) are turned around or terminated. Improved IT Governance, Program and Portfolio Management. Assessment of the evolution of existing information systems and the development of new information systems to ensure optimal alignment with mission needs, business priorities, and the target architecture.
Optimize the use and value of information technology.	Promote shared service solutions. Streamline the Department's IT Operations. Assemble performance metrics and rate structures for common services.	Enterprise Architecture Capital Planning & IT Governance Strategic Sourcing Enterprise Management Lean Six Sigma Information Management	Assessment of the standardization, interdependencies, and interrelationships among USDA's business operations and the enabling IT infrastructure. Increased number of investments on budget and on schedule. Increased number of shared solutions to reduce costs. .

Agency Strategic Goal	Agency Objectives	Programs that Contribute	Key Outcomes
Enable innovative business driven solutions by simplifying and unifying information technology.	Enhance delivery of cloud-based services to the Enterprise. Improve Wired and Wireless Capability to Support the evolving mission. Modernize existing data, web systems, and services.	Policy, Directives, and Strategic Planning Capital Planning & IT Governance Strategic Sourcing Enterprise Architecture Enterprise Management Open Data Initiative	USDA Cloud Computing Policy "cloud first" policy. Reduce maintenance and ops spending to re-balance with new solutions (Development, Modernization & Enhancement) spending A Marketing Strategy and Communications Plan for senior executives, management teams, and business units to keep them informed of innovative ideas and opportunities for shared services.

Key Performance Measures

Annual Performance Goals, Indicators, and Trends		Actual				Target	Actual	Result	Estimate /Target	Target
		2011	2012	2013	2014	2015			2016	2017
5.3	Duplicative IT	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Est baseline	1%
Allowable Data Range for Met The tolerance range for the measure to be "met" is +/- 5 percent. Range is determined by number of systems retired or transitioned to an existing platform.										
Assessment of Performance Data										
Data source – Enterprise Architecture Repository**,** Cybersecurity Assessment and Management Tool (CSAM), and AgMax is OCIO's Capital Planning and Portfolio Management repository will all be used to establish baseline as well as provide data on USDA systems.										
Completeness of Data – Agencies manually enter budget, schedule, and performance data on a monthly basis for major investments and quarterly for non-major investments.										
Reliability of Data – Data is maintained on a monthly basis by Agencies and is deemed reliable.										
Quality of Data – To ensure accuracy, there are multiple reviews of the data.										

Selected Past Accomplishments toward Achievement of the Key Outcome in FY 2015:
The Capital Planning & IT Governance has developed a comprehensive IT governance process that incorporates an Integrated Governance Framework and provides the executive teams with a process for reviewing investments and providing guidance to investment managers throughout a project's AgSDLC. The framework integrates Capital Planning, Program Management, EA, Security, and the budget process. USDA reviewers and decision-makers evaluate program performance on planning, acquiring, designing, developing, constructing, testing, implementing, operating, maintaining, and retiring IT, as well as on sound management of facilities, hardware, software, and personnel that are associated with those IT investments.

OCIO supported the Secretary's goal of achieving $100 Million in cost avoidances/savings through strategic sourcing by participating with members of the CIO Council in the Senior Overarching Planning Group (SOPG). The SOPG is a group

of senior managers and subject matter experts from across the Department of Agriculture brought together for this express purpose. The SOPG developed a detailed category profile across six IT categories ($169 M in annual spend) and identified key levers to achieve cost avoidance and savings including Best Price Evaluation, Volume Concentration, Product Specification Improvement and Demand Management. The SOPG selected six IT categories after performing initial spend analysis using recent Fiscal Year spending data, and assessing opportunity attractiveness. The SOPG formed sub-category teams for each opportunity and completed sourcing strategy development work with active involvement from more than 100 team members and subject matter experts from across the Department. The subcategory teams developed a spend baseline across the six categories by analyzing data from USDA procurement systems, vendor data calls, agency data calls, interviews with agency managers, price quotes and contracts. The teams finalized strategic sourcing recommendations with associated potential annualized benefits after multiple team deliberations and two rounds of SOPG reviews. The potential annualized benefits range from $23-49 Million across the six categories, expected to be fully realized by Fiscal Year 2019.

Selected Accomplishments Expected at the FY 2017 Proposed Resource Level/Challenges for the Future:

- Integrate Lines of Business operations and systems with the Enterprise Architecture mapping of the infrastructure, applications, and security reference model;
- Develop reference material of USDA's system architecture by mission area, agency, and reference framework and include the Farm Bill implementation as the business focus;
- Continue refining standards, conduct system mapping, and start building out system specific standards profile;
- Develop Agency-specific performance reports to enable analysis to identify areas and opportunities for improvement (engineering, consolidation, de-commissioning, etc.);
- Consolidate duplicative IT commodity services to identify opportunities for enterprise solutions; and
- Develop framework for measuring cost savings and associated re-investments;
- The OCIO will assess investments through the CPIC monthly portfolio reporting process and engage with the Business Sponsors. Furthermore, CPIGD will assess the development, modernization, and enhancement (DME) to obtain an optimum balance of the Department's IT portfolio at the lowest cost with minimal risk while ensuring mission and business goals are being met; and
- Perform formal governance gate reviews of major IT investments to determine the optimum path forward and the health of the investment.

Strategic Goal Funding Matrix
(Dollars in thousands)

Program / Program Items	2014 Actual	2015 Actual	2016 Enacted	Increase or Decrease	2017 Estimate
Department Strategic Goal 5: Create a USDA for the 21st century that is high performing, efficient, and adaptable.					
Department Strategic Objective 5.1: Develop a customer-centric, inclusive, and high-performing workforce by investing in and engaging employees to improve service delivery.					
Office of the Chief Information Officer.....	$5,591	$4,494	$4,494	+9,830	$14,324
Staff Years.....	18	17	18	+51	69
Department Strategic Objective 5.2: Build a safe, secure and efficient workplace by leveraging technology and shared solutions across organizational boundaries.					
Office of the Chief Information Officer.....	26,802	28,000	28,000	+10,000	38,000
Staff Years.....	48	46	62	+34	96
Department Strategic Objective 5.3:: Maximize the return on taxpayer investment in USDA through enhanced stewardship activities and focused program evaluations.					
Office of the Chief Information Officer.....	11,638	12,551	12,044	+1,348	13,392
Staff Years.....	49	48	56	+4	60
Total Costs, All Strategic Goals	44,031	45,045	44,538	21,178	65,716
Total FTEs, All Strategic Goals	115	111	136	+89	225

Full Cost by Agency Strategic Goal
(Dollars in thousands)

Department Strategic Goal 5: Create a USDA for the 21st century that is high performing, efficient, and adaptable.

Program / Program Items	2014 Actual	2015 Actual	2016 Enacted	2017 Estimate
Deliver				
Administrative costs (direct)	$7,222	$7,893	$6,923	$6,525
Indirect costs	4,098	4,539	5,121	6,867
Total Costs	11,320	12,432	12,044	13,392
FTEs	49	48	56	60
Performance Measure:				
Eliminate dupplicative IT investments				
Measure	N/A Est. Baseline		20%	50%
Innovate				
Administrative costs (direct)	$3,567	$2,853	$2,583	$6,979
Indirect costs	2,024	1,641	1,911	7,345
Total Costs	5,591	4,494	4,494	14,324
FTEs	18	17	18	69
Performance Measure:				
Percentage of USDA electronic documents that are 508 compliant and accessible.				
Measure	N/A	50%	75%	80%
Protect				
Administrative costs (direct)	$17,846	$18,644	$18,644	$25,302
Indirect costs	8,956	9,356	9,356	12,698
Total Costs	26,802	28,000	28,000	38,000
FTEs	48	46	62	96
Performance Measure:				
Percentage of USDA employees logging into the networks via Homeland Security Presidential Directive 12 (HSPD-12) using LincPass.				
Measure	50%	80%	85%	90%
Percentage of ASOC incidents closed within 30 days.				
Measure	92%	93%	95%	95%
Improve agency compliance with enterprise standards for cyber security tools and processes through outreach and training opportunities.				
Measure	50%	60%	70%	80%
Total Costs, All Strategic Goals	43,713	44,926	44,538	65,716
Total FTEs, All Strategic Goals	115	111	136	225