

2018 President's Budget  
Office of the Chief Information Officer

Contents

Purpose Statement .....	9-1
Statement of Available Funds and Staff Years .....	9-5
Permanent Positions by Grade and Staff Year Summary .....	9-6
Motor Vehicle Fleet Data .....	9-7
Salaries and Expenses	
Appropriations Language .....	9-9
Lead-Off Tabular Statement .....	9-9
Summary of Increases and Decreases .....	9-9
Project Statement .....	9-9
Justifications .....	9-10
Geographic Breakdown of Obligations and Staff Years .....	9-13
Classification by Objects .....	9-14
Shared Funding Projects .....	9-15
Status of Programs .....	9-17
Summary of Budget and Performance	
Key Performance Outcomes and Measures .....	9-24

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 Automated Data Processing 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, 2016, there were 992 full-time permanent employees funded by appropriated and Working Capital Funds.

	<u>Full-Time Permanent</u>
OCIO Direct	106
OCIO WCF	<u>886</u>
Total	992

OIG Reports – Completed

#50501-0001-12 4/2012 USDA's Configuration, Management and Security over Domain Name System Servers Report - This audit contained six recommendations. OCFO has granted final action on all.

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 13. Closure on the last recommendation is dependent on final publication of Privacy PII (Privacy Act) Departmental Regulation (DR).

#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 fifteen. Remediation on remaining four recommendations is ongoing. Final Action was denied on 2 recommendations. We are resubmitting these with additional

OFFICE OF THE CHIEF INFORMATION OFFICER

clarifying documentation. Closure on the remaining 2 recommendations is dependent on publication of Standard Operating Procedures.

- #50501-01-IT 08/2011 USDA's Management and Security over Wireless Handheld Devices - The audit resulted in five recommendations. OIG has granted final action on three recommendations. Remediation action is completed for the remaining two actions, we are gathering appropriate documentation to support final action.
- #50501-2-12 11/2011 Fiscal Year 2011 Federal Information Security Management Act Report - OCFO has granted final action on all of the 10 recommendations from this audit. OCIO and OIG have reached Management Decision on all of the 10 recommendations from this audit. OCFO has granted final action on seven recommendations and remediation on the remaining actions is ongoing.
- #88401-0001-12 08/2012 OCIO FY'S 2010 and 2011 Funding Received for Security Enhancements Report – This audit contained four recommendations. CIO and OIG have reached Management Decision on all recommendation. OCFO has granted final action on one recommendation, remediation action on the remaining three is completed, and we are gathering appropriate documentation to support final action.
- #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 and remediation action is completed, we are gathering appropriate documentation to support final action.
- #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 three recommendations. Remediation on the remaining two is dependent on final publication of Standard Operating Procedures and Departmental Regulation (Policy).
- #88501-0002-12 08/2014 Management and Security over USDA's Universal Telecommunications Network Report - This audit contained 21 recommendations. OCFO has granted final action on 20 recommendations. On the remaining recommendation, OIG has accepted a change in the Management Decision, and remediation efforts are underway.
- #50501-0005-12 09/2014 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 five recommendations and remediation on the remaining two is 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 both recommendations. OCFO has granted final action on one recommendation, remediation for the remaining recommendation is dependent on the issuance of a Departmental Regulation.
- #50501-0008-12 11/2015 Fiscal Year 2015 Federal Information Security Management Act Report - This audit contained 4 recommendations. Management Decision has been reached on all recommendations and remediation is underway.
- #50501-00012-12 11/2016 Fiscal Year 2016 Federal Information Security Management Act Report. This audit contained three recommendations. Remediation actions for the recommendations are underway.

OFFICE OF THE CHIEF INFORMATION OFFICER

#50501-00012-12 11/2016 Fiscal Year 2016 Federal Information Security Management Act Report (Security Protocols and Connections for USDA's Public-Facing Websites). This audit contained three recommendations. Remediation actions for the recommendations are underway.

GAO Reports - Completed

#08-525 06/2008 Information Security - Federal Agency Efforts to Encrypt Sensitive Information are Under Way, but Work Remains - The report contained three recommendations. GAO closed two recommendations as implemented and one was closed as not implemented.

#12-756 07/2012 Information Technology Reform: Progress Made but Future Cloud Computing Efforts should be Better Planned –GAO had two recommendations for this audit, and both recommendations have been implemented, audit closed.

#16-501 06/2016 Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. For this audit, GAO had no recommendations, audit closed.

#16-602 09/2016 Digital Services Program: Assessing Results and Coordinating with Chief Information Officers Can Improve Delivery of Federal Projects. For this audit, GAO had no recommendations, audit closed.

#16-667 09/2016 Freedom of Information Act: Litigation Costs for Justice and Agencies Could Not Be Fully Determined. For this audit, GAO had no recommendations, audit closed.

#16-686 09/2016 Chief Information Security Officer: Opportunities Exist to Improve Roles and Address Challenges to Authority. For this audit, GAO had no recommendations, audit closed.

GAO Reports – In Progress

#12-629 07/2012 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. Progress has been made in addressing the recommendations but additional work needs to be completed to develop policy and guides for Information Technology Project Cost Estimating.

#12-791 09/2012 Organizational Transformation: Enterprise Architecture Value Needs to Be Measured and Reported - USDA has worked closely with GAO on progress against the two recommendations. We expect to close the two recommendation by the end of 2017.

#13-524 06/2013 Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects - USDA has provided periodic updates to GAO on progress against the one recommendation. Progress has been made in addressing the recommendation but additional work needs to be completed 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. Progress has been made in addressing the recommendations but additional work needs to be completed 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 three recommendations. The Department Regulation, (Revised DR3450-001),

OFFICE OF THE CHIEF INFORMATION OFFICER

“Computer Matching Program Involving Individual Privacy Data,” continues to progress in the policy development process. The Cost Benefit Analysis was drafted and is currently being tested with Rural Development as it drafts its Computer Matching Agreement-March 2017. Additionally, a Data Integrity Board (DIB) Membership memorandum and DIB charters have been created and submitted for review.

- |         |         |  |
|---------|---------|--|
| #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 six USDA recommendations in August 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. Progress has been made in addressing the recommendation but additional work needs to be completed 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 developed 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 Recommendation 1 for implementation and it is currently under GAO final review. Remediation for the remaining recommendation is underway.  |
| #16-323 | 03/2016 | Data Center: Agencies Making Progress, but Planned Savings Goals Need to Be Established. Statement of action has been submitted, remediation action underway.  |
| #16-468 | 05/2016 | Information Technology: Federal Agencies Need to Address Aging Legacy Systems Statement of action has been submitted, remediation action underway.   |
| #16-494 | 06/2016 | IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments. The Statement of Action has been submitted, remediation action underway.  |
| #16-511 | 09/2016 | Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings. The Statement of Action has been submitted, remediation action underway.   |

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Item	2015 Actual		2016 Actual		2017 Estimate		2018 President's Budget	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
Salaries and Expenses:								
Discretionary Appropriation.....	\$45,045	111	\$44,538	106	\$44,453	107	\$58,950	116
Rescission.....	-	-	-	-	-	-	-	-
Sequester.....	-	-	-	-	-	-	-	-
Adjusted Appropriation.....	45,045	111	44,538	106	44,453	107	58,950	116
Lapsing Balances.....	-119	-	-147	-	-	-	-	-
Obligations.....	44,926	111	44,391	106	44,453	107	58,950	116
Obligations under other USDA appropriations:								
Reimbursements:								
E-GOV Initiative.....	-	-	9,133	-	8,521	-	8,731	-
Geospatial IS.....	8,952	-	6,099	-	6,000	-	6,000	-
NTIA Spectrum.....	2,190	-	2,362	-	2,300	-	2,300	-
EMS.....	-	-	18,735	-	18,500	-	18,500	-
EPMS.....	-	-	1,618	-	1,600	-	1,600	-
Project Definition.....	-	-	513	-	513	-	513	-
Other Activities.....	348	-	313	-	300	-	300	-
Total, Agriculture Appropriations	11,490	-	38,773	-	37,734	-	37,944	-
Working Capital Fund: <sup>a/</sup>								
Information Technology.....	415,915	844	453,375	839	436,427	952	440,739	952
NITC (Non-USDA).....	31,067	41	41,845	47	30,781	38	33,936	38
Total, WCF.....	446,982	885	495,220	886	467,208	990	474,675	990
Total, OCIO.....	503,398	996	578,384	992	549,395	1,097	571,569	1,106

<sup>a/</sup> 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	2015 Actual			2016 Actual			2017 Estimate			2018 President's Budget		
	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total	Wash. D.C.	Field	Total
ES.....	7	-	7	8	-	8	8	-	8	8	-	8
GS-15.....	18	4	22	21	2	23	16	2	18	17	2	19
GS-14.....	46	6	52	46	9	55	37	9	46	38	9	47
GS-13.....	16	7	23	10	6	16	11	6	17	18	6	24
GS-12.....	12	3	15	7	3	10	7	3	10	7	3	10
GS-11.....	4	-	4	2	-	2	2	-	2	2	-	2
GS-10.....	1	-	1	-	-	-	-	-	-	-	-	-
GS-9.....	3	-	3	5	-	5	5	-	5	5	-	5
GS-8.....	1	-	1	-	-	-	-	-	-	-	-	-
GS-5.....	1	-	1	-	-	-	-	-	-	-	-	-
GS-4.....	-	-	-	1	-	1	1	-	1	1	-	1
Total Perm. Positions.....	109	20	129	100	20	120	87	20	107	96	20	116
Unfilled, EOY .....	18	-	18	14	-	14	-	-	-	-	-	-
Total, Perm. Full-Time Employment, EOY.....	91	20	111	86	20	106	87	20	107	96	20	116
Staff Year Est.....	91	20	111	86	20	106	87	20	107	96	20	116

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 CTS 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 2018 OCIO has plans for adding 2 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 Technical Support Division (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, 2016, CTS has 270 leased GSA vehicles and NITC has 2 leased GSA vehicles. CTS continues to lease vehicles from GSA to provide IT support to the SCAs within USDA.

Changes to the motor vehicle fleet. Replacement of approximately 60 vehicles and 2 additional vehicles has been proposed for 2018.

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)

Fiscal Year	Number of Vehicles by Type							Total Number of Vehicles	Annual Operating Cost (\$ in 000)
	Sedans and Station Wagons	Light Trucks, SUVs and Vans		Medium Duty Vehicles	Ambulances	Buses	Heavy Duty Vehicles		
		4X2	4X4						
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	+43	-42	+5	0	0	0	0	+6	+32
2017	222	31	17	0	0	0	0	270	946
Change	+2	0	0	0	0	0	0	+2	+4
2018	224	31	17	0	0	0	0	272	950

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] \$58,950,000, [of which not less than \$28,000,000 is for cybersecurity requirements of the Department.]

Lead-off Tabular Statement

Budget Estimate, 2018.....	\$58,950,000
2017 Annualized Continuing Resolution.....	<u>44,453,000</u>
Change in Appropriation.....	<u>+14,497,000</u>

Summary of Increases and Decreases  
(Dollars in thousands)

	<u>2015</u> <u>Actual</u>	<u>2016</u> <u>Change</u>	<u>2017</u> <u>Change</u>	<u>2018</u> <u>Change</u>	<u>2018</u> <u>Estimate</u>
Discretionary Appropriations: Office of the Chief Information Officer.....	\$45,045	-\$507	-\$85	+\$14,497	\$58,950

Project Statement

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

Program	<u>2015 Actual</u>		<u>2016 Actual</u>		<u>2017 Estimate</u>		<u>Inc. or Dec.</u>		<u>2018</u> <u>President's</u> <u>Budget</u>	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
Discretionary Appropriations: Office of the Chief Officer.....	\$45,045	111	\$44,538	106	\$44,453	107	+\$14,497 (1)	+9	\$58,950	116
Total Available.....	45,045	111	44,538	106	44,453	107	+14,497	+9	58,950	116
Lapsing Balances.....	-119	-	-147	-	-	-	-	-	-	-
Total Obligations.....	<u>44,926</u>	<u>111</u>	<u>44,391</u>	<u>106</u>	<u>44,453</u>	<u>107</u>	<u>+14,497</u>	<u>+9</u>	<u>58,950</u>	<u>116</u>

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Program	<u>2015 Actual</u>		<u>2016 Actual</u>		<u>2017 Estimate</u>		<u>Inc. or Dec.</u>		<u>2018 President's Budget</u>		
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs	
	Discretionary Obligations:										
Office of the Chief Information Officer.....											
Officer.....	\$44,926	111	\$44,391	106	\$44,453	107	+\$14,497	(1)	+9	\$58,950	116
Total Obligations.....	44,926	111	44,391	106	44,453	107	+14,497		+9	58,950	116
Lapsing Balances.....	119	-	147	-	-	-	-	-	-	-	-
Total Appropriation.....	45,045	111	44,538	106	44,453	107	+14,497		+9	58,950	116

Justification of Increases and Decreases

Base funds will allow the Office of the Chief Information Officer to continue to provide guidance, leadership and coordination for the Department’s information management, technology investment and cyber security activities in support of USDA program delivery. 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) A net increase of \$14,497,000 and 9 staff years for the Office of the Chief Information Officer (\$44,453,000 and 121 staff years available in 2017).

The funding change is requested for the following item:

- a. An increase of \$532,000 for pay costs (\$133,000 for annualization of the 2017 pay increase and \$399,000 for the 2018 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 \$14,227,000 and 12 staff years for Continuous Diagnostics and Mitigation (CDM) Phase 1 (\$28 million and 62 staff years available in 2017).

The Continuous Diagnostics and Mitigation (CDM) Program, centrally managed by the Department of Homeland Security, and also implemented at USDA, is intended to create a common baseline of cybersecurity capability and protection across the Federal Government. The program provides federal departments and agencies with CDM-certified capabilities and tools that identify and prioritize cybersecurity risks on an ongoing basis and enable cybersecurity personnel to mitigate the most significant problems first. The CDM tools also allow departments and agencies to better manage their IT assets, helping to reduce their overall attack surface.

The CDM tools provide near real-time awareness of USDA networks and environments. Data from the tools are automatically ingested into an individual dashboard at USDA. The Agency Dashboard provides current visibility into the overall organization’s security posture based on a 72 hour data currency. With the full implementation of CDM, data from the individual agency dashboards across the federal government will be

## OFFICE OF THE CHIEF INFORMATION OFFICER

aggregated into one federal-level dashboard with planned synchronization every 8 hours. The Federal Dashboard is maintained by the CDM Program and allows DHS to monitor and respond to federal cybersecurity threats and incidents much more quickly and efficiently.

The CDM Program is currently managed under four phases. Since FY 2013, Congress has supported all four phases of CDM. CDM Phase 1 is “What is on your network.” The Phase 1 tools allow USDA to automate and in real time identify, classify, and count the number of agency computers, what software those computers run, and if they are vulnerable to attack. The result for this improved asset management is that it immediately reduces an USDA’s attack surface.

Historically, it has taken agencies days or weeks to determine that cybersecurity incidents have occurred in their environment. Once fully deployed, the CDM Program will shorten this timeframe to hours and minutes.

DHS, through the CDM Program Management Office, paid for the purchase and integration of Phase 1 tools, and paid for the annual license renewal and vendor support costs (that is, Operation & Maintenance costs) of the tools for FY 2017. If DHS covers the Phase 1 tools O&M costs for FY 2018, which DHS estimates at \$3.1 million, then the requested increase of \$14,227,000 for CDM Phase 1 will be adjusted.

The increased funding will cover other O&M costs such as hosting, additional FTEs, contractor services, training, governance, and program management costs, which DHS will not cover. The funding will provide:

- Operations and maintenance of the CDM Phase 1 tools, CDM dashboard, and the ancillary hardware and software that run and support the CDM Phase 1. This includes some additional FTEs and contractor services.
- Integration services for continuous research, evaluation, architecture, and design required for the development, modernization, and enhancement of the CDM Phase 1 tools and capabilities.
- Centralized management and delivery of cyber security analysis and services that directly support USDA agencies’ security and IT management and technical staff to enable them to efficiently and effectively use CDM Phase 1 tools and quickly identify, assess, prioritize, and mitigate risks continuously and in a timely manner.
- Protection, detection, analysis, response, and remediation services and support to USDA agencies and improves USDA’s overall information security continuous monitoring process and implementation using CDM Phase 1 solutions.
- Establish and maintain an inter-agency governance structure and management processes that provide USDA agencies greater insight into existing continuous monitoring capabilities, identify gaps, and assess areas for coordination, resource sharing, and deployment, and integrate USDA’s CDM CONOPs and CDM Phase 1 management processes into agency IT and security operations as mandated by OMB.
- Develop and deliver USDA-wide CDM training program, which will enable USDA’s cybersecurity workforce to continue to adapt and to design, develop, implement, maintain and continuously integrate and improve CDM capabilities and cybersecurity practices within their environments as cybersecurity threat and technology environment continuously.

Without the increased funding, USDA will not have the means to renew product licenses and vendor support nor continue to cover other O&M costs such as hosting, additional FTEs, contractor, services and support, training, governance, and program management costs. This will result in USDA ceasing operations and maintenance of CDM tools and services.

OFFICE OF THE CHIEF INFORMATION OFFICER

- c. An increase of \$1,600,000 for Operational Security Assessments and Penetration Testing (\$28 million and 62 staff years available in 2017).

For FY 2018, funding is needed to reopen the Operational Security Assessment and Penetration Testing programs. This program was not funded at the level it needs to be in FY 2017 focused only on a small number of agencies. The Office of Information Security's Operational Security Assessments and Penetration Testing programs are comprehensive security assessment programs that supports the Department's goal of improving the overall security posture of the USDA enterprise.

These programs are essential to identifying department-wide cybersecurity vulnerabilities and risks. The program examine and evaluate the Agency's information technology systems and the supporting operational policies and procedures. They provide USDA agencies with timely, real, actionable intelligence to assist in defending valuable agency business and mission assets against current and future cyber-threats and/or attacks. The programs enables USDA agencies to identify, prioritize, and remediate vulnerabilities and risks in a timely manner, improve their security posture, and strengthen the protection USDA information and associated assets overall.

The operational security assessment is a comprehensive analysis of an agency's information architecture, develops a threat profile for the agency's IT security components, or its layers and sub-layers of security. The security assessment identifies the nature of the threats and the likely vulnerabilities of the given piece of technology associated with an agency's business. The security assessment will also examine and evaluate the agency's operational security policies, procedures, and systems through the performance of technological reviews.

The penetration test probes and tests USDA's computer system, network or Web application to find vulnerabilities that an attacker could exploit. Penetration test helps agencies determine whether a system is vulnerable to attack, if the defenses were sufficient, and which defenses (if any) the test defeated. Vulnerabilities and security issues that the penetration test uncovers are promptly reported to the agency for review and remediation.

These programs are required on annual basis in order to continuously monitor and identify vulnerabilities and risks for remediation.

- d. A decrease of \$711,000 for support service contracts.  
OCIO will review, prioritize, and reduce support service contracts. Contractors will be the main focus of reduction and OCIO estimates three or four contractors will be affected by the reductions. Contracts will be reviewed for consolidation to minimize overhead resources and costs. Contracts supporting non-critical functions will be scaled back or will not be renewed.
- g. A decrease of \$600,000 for elimination of office space.  
OCIO will terminate its GSA office space lease at the Patriot Plaza III (PPIII) building in Washington, DC. The 44 staff and contractors will be moved to current OCIO vacant space in the Whitten and South buildings to accommodate the additional staff. OCIO will be reusing existing PPIII modular office furniture to reconfigure the vacant space as needed.
- e. A decrease of \$551,000 and 3 staff years by vacancies created through attrition.  
Vacancies will be monitored centrally as staff retire or leave and will be filled as needed to keep OCIO activities functioning efficiently. Responsibilities of these positions will be distributed among other areas of OCIO.

OFFICE OF THE CHIEF INFORMATION OFFICER

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

State/Territory	2015 Actual		2016 Actual		2017 Estimate		2018 President's Budget	
	Amount	SYs	Amount	SYs	Amount	SYs	Amount	SYs
District of Columbia.	\$42,506	91	\$42,793	86	\$42,850	87	\$57,341	96
Denver, CO.....	-	-	92	1	93	1	95	1
Kansas City, MO.....	2,420	20	1,426	18	1,429	18	1,432	18
St. Louis, MO .....	-	-	80	1	81	1	82	1
Obligations.....	44,926	111	44,391	106	44,453	107	58,950	116
Lapsing Balances.....	119	-	147	-	-	-	-	-
Total, Available.....	45,045	111	44,538	106	44,453	107	58,950	116

OFFICE OF THE CHIEF INFORMATION OFFICER

Classification by Objects  
(Dollars in thousands)

	2015	2016	2017	2018
	Actual	Actual	Estimate	President's Budget
<b>Personnel Compensation:</b>				
Washington D.C.....	\$10,748	\$10,454	\$10,951	\$12,213
Kansas City, MO.....	1,907	1,945	1,961	2,000
11 Total personnel compensation.....	12,655	12,399	12,912	14,213
12 Personal benefits.....	3,749	3,753	3,884	4,254
13.0 Benefits for former personnel.....	-	3	-	-
Total, personnel comp. and benefits.....	16,404	16,155	16,796	18,467
<b>Other Objects:</b>				
21.0 Travel and transportation of persons.....	186	265	265	277
22.0 Transportation of things.....	-	2	2	26
23.1 Rental payments to GSA.....	984	448	448	-
23.3 Communications, utilities, and misc. charges.....	457	494	494	518
24.0 Printing and reproduction.....	126	128	128	128
25.2 Other services from non-Federal sources.....	14,681	14,898	14,339	20,505
25.3 Other purchases of goods and services from Federal sources.....	10,097	10,637	10,637	17,685
26.0 Supplies and materials.....	680	254	254	254
31.0 Equipment.....	1,311	1,090	1,090	1,090
42.0 Insurance Claims.....	-	20	-	-
Total, Other Objects.....	28,522	28,236	27,657	40,483
99.9 Total, New Obligations.....	44,926	44,391	44,453	58,950
DHS Building Security Payments (included in 25.3)....	\$1,486	\$1,405	\$ -	\$ -
<b>Position Data:</b>				
Average Salary (dollars), ES Position.....	\$170,000	\$171,500	\$173,215	\$176,506
Average Salary (dollars), GS Position.....	\$106,090	\$108,537	\$113,216	\$115,367
Average Grade, GS Position.....	13.7	13.8	13.9	13.8

OFFICE OF THE CHIEF INFORMATION OFFICER

Shared Funding Projects  
(Dollars in thousands)

	2015	2016	2017	2018
	<u>Actual</u>	<u>Actual</u>	<u>Estimate</u>	<u>President's Budget</u>
<b>Working Capital Fund:</b>				
Administration:				
Beltsville Service Center.....	\$59	\$68	\$115	\$42
HR Enterprise System Management.....	-	8	8	8
Mail and Reproduction Management.....	9	197	187	169
Integrated Procurement System.....	436	446	443	436
ASC - Office of the Chief Information Officer Oversight...	-	895	1,124	1,023
Financial Management Services.....	301	367	367	421
Procurement Operations.....	3,675	4,753	4,137	4,270
Subtotal.....	4,480	6,734	6,381	6,369
Communications:				
Creative Media & Broadcast Center.....	2	22	23	52
Finance and Management:				
NFC/USDA.....	1,124	240	286	259
Controller Operations.....	1,355	1,208	1,475	1,414
ASC - Working Capital Fund Controller.....	-	1,098	1,370	1,237
Internal Control Support Services.....	143	171	171	173
Subtotal.....	2,622	2,717	3,302	3,083
Information Technology:				
NITC/USDA.....	9,065	10,011	7,933	8,430
International Technology Services.....	12,825	12,269	5,452	5,107
Telecommunications Services.....	11,610	14,205	14,542	15,214
Subtotal.....	33,500	36,485	27,927	28,751
Correspondence Management.....	23	19	17	15
Total, Working Capital Fund.....	40,627	45,977	37,650	38,270
<b>Departmental Shared Cost Programs:</b>				
1890's USDA Initiatives.....	30	34	42	38
Classified National Security Information.....	11	15	16	15
Continuity of Operations Planning.....	23	22	24	21
Emergency Operations Center.....	25	25	26	24
Facility and Infrastructure Review and Assessment.....	5	5	5	4
Faith-Based Initiatives and Neighborhood Partnerships.....	4	4	5	4
Hispanic-Serving Institutions National Program.....	20	19	22	20
Honor Awards.....	1	1	1	1
Human Resources Transformation (inc. Diversity Council)...	19	17	20	18
Identity and Access Management.....	74	73	76	68
Medical Services.....	13	13	15	14
People's Garden.....	8	7	7	7
Personnel Security Branch.....	47	33	21	19
Preauthorizing Funding.....	41	40	42	37
Retirement Processor/Web Application.....	7	6	7	6
TARGET Center.....	15	16	16	14
USDA 1994 Program.....	8	7	9	8
Virtual University.....	22	22	22	20
Total, Departmental Shared Cost Programs.....	373	359	376	338

OFFICE OF THE CHIEF INFORMATION OFFICER

	2015	2016	2017	2018
	<u>Actual</u>	<u>Actual</u>	<u>Estimate</u>	<u>President's Budget</u>
<b>E-Gov:</b>				
Budget Formulation and Execution Line of Business.....	1	1	1	1
Enterprise Human Resources Integration.....	23	21	22	22
E-Rulemaking.....	9	-	-	-
E-Training.....	30	31	-	-
Financial Management Line of Business.....	2	1	1	1
Geospatial Line of Business.....	-	8	12	12
Human Resources Line of Business.....	3	3	3	3
Integrated Acquisition Environment.....	28	14	-	-
Total, E-Gov.....	<u>96</u>	<u>79</u>	<u>39</u>	<u>39</u>
Agency Total.....	<u>41,096</u>	<u>46,415</u>	<u>38,065</u>	<u>38,647</u>

## OFFICE OF THE CHIEF INFORMATION OFFICER

### Status of Programs

The Clinger-Cohen Act of 1996 required the establishment of a Chief Information Officer (CIO) for all major Federal agencies. The Act 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 (EAR), capital planning investment tools, and Enterprise IT Solutions.

OCIO will continue to modernize the eAuthentication shared service (eAuth) and focus on further expanding the enforcement of Personal Identity Verification (PIV) credentials for logical access. OCIO will build upon the modernized eAuthentication platform through the implementation of a secure and easy to use multi-factor authentication capability for public citizens. This enhancement will improve both the security and user experience of accessing citizen-facing services online. OCIO will also expand the authentication and authorization capabilities of the eAuth Service to Application Programming Interfaces, the building blocks of modern applications, and mobile apps. OCIO continues to focus on expanding enforcement of PIV credentials through execution of the Department's PIV strategy. Key highlights of the strategy include expanding the use of Derived PIV credentials for mobile devices, reducing the average time to issue PIV credentials to new employees, and leveraging the CDM Phase 2 tools to expand PIV compatibility to additional systems and devices.

USDA Participation in E-Government Initiatives: USDA participates in 10 E-Government Presidential Initiatives and Lines of Business (LoB). 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.

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

Enterprise Architecture: Enterprise Architecture (EA) is the planning and management process of translating business vision and strategy into effective enterprise business and technology changes through the analysis of the as-is enterprise information and the design of future state key enterprise segments. The purpose of USDA's EA Program is to define the "corporate" or enterprise-wide view and frameworks for the USDA business capabilities, system inventory, data catalog, and technology standards. The USDA EA Program coordinates, aligns, and leverages the USDA Agency/Staff Office EA Programs to ensure that USDA IT investments are business driven, interoperable, and cost effective. The Enterprise Architecture Division (EAD) provides current insights into EA best

## OFFICE OF THE CHIEF INFORMATION OFFICER

practices, coordinates federated Agency/Staff Office EA approaches, and conducts enterprise-level EA analyses to improve the enterprise architecture planning and decision making processes across the USDA.

Capital Planning and Investment Control (CPIC) and IT Governance: The Capital Planning and IT Governance primary mission is the planning, educating, IT management, analysis and governance of USDA's IT investment portfolio worth over \$3 billion dollars and currently comprises of 56 major IT investments and 176 non-major IT investments.

We engage in ongoing efforts to establish and maintain business relationships that support effective IT portfolio management processes and a decision-making environment. Consequently, ensuring the establishment and implementation of IT Governance through strategic initiatives, sound structure, oversight, regulatory compliance, accountability, transparency, and the fiscal responsibility of IT decisions. This environment consists of four key components:

- Executive decision-making;
- Creating repeatable IT Governance and Portfolio Management processes;
- Integrated partnership through regular customer engagements with the business and IT; and,
- Supporting portfolio management tools.

CPIC and IT Governance are supported and reinforced by both the Clinger-Cohen Act of 1996 and the Federal Information Technology Acquisition Reform Act (FITARA) that requires Federal 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 IT investments and USDA strategic priorities throughout the investment life cycle. Investment reporting is done through monthly, quarterly and annual reports to the Office of Management and Budget (OMB) known as but not limited to monthly CIO Evaluations, quarterly Integrated Data Collections and quarterly PortfolioStats along with adhoc TechStats and an annual FedStat review with the USDA Senior Leaders.

The OCIO Capital Planning and IT Governance Division 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.

Information Management: Information management 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.

Policy and IT Strategic Planning: OCIO manages the Departmental Directives System, provides assistance to policy developers, and conducts reviews of draft IT related and non-IT Departmental Directives which include Regulations, Manuals, Notices, and other guidance. There are currently 41 new and revised IT directives and over 35 non-IT directives in development to address key policy gaps, audit recommendations, and management priorities. Based on a policy program assessment and roadmap conducted in 2014 by Gartner Consulting and a Workflow Tool Assessment conducted by DKW Communications in 2015, OCIO is completing the identification of the best tool to automate the directives workflow process. OCIO is building on the foundation of the Lean Six Sigma (LSS) project completed in 2012 and working to identify additional opportunities to streamline the policy process. The average formal clearance time for all Departmental directives was reduced by 25.2 percent in 2016.

OCIO is also in the process of updating policy guidance and best practices documentation and is continuing the development of new policy training modules. In 2016, OCIO revised the *USDA Information Technology Strategic Plan*, which was approved in November 2016. OCIO has also developed a *Policy and Planning Strategic Plan*,

## OFFICE OF THE CHIEF INFORMATION OFFICER

which has been submitted for approval. OCIO also manages the Departmental Forms System and provides reviews and approvals of new and revised Departmental Forms for publication.

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 (PII) about individuals that is maintained in systems of record by Federal agencies. In 2016, the Privacy Office in collaboration with the Office of the Secretary began revision of its review and approval process for Privacy Impact Assessments, System of Record Notices and Computer Matching Agreements in its automated Enterprise Content Management System. These improvements will ensure that an adequate workflow is established and that all review parties can sign and approve. In addition, the Privacy Office made the following improvements; 1) The Senior Agency Official for Privacy designation was elevated from the USDA CIO to the USDA Assistant Secretary for Administration; 2) A new Chief Privacy Officer was also designated during the reporting period; 3) The USDA Privacy Council was selected as a working group under the USDA's CIO Council; 4) The DIB completed two computer matching reviews in FY 2016, and will report those systems as soon as all USDA executive signatures have been captured; and 5) USDA enrolled its privacy act/privacy officers and staff in the Office of Management and Budget's Regulatory Information Service Center and Office of Information and Regulatory Affairs Consolidated Information System Regulations Review Module to ensure that USDA privacy documents are going through the formal OMB regulatory review process.

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 2016, the Department processed 23,134 FOIAs, a 3,575 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 an increase in the overall number of requests processed, decreased processing times, and resulted in a 50 percent decrease in PE&F's 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 and the FOIA Training Subcommittee, continued development of its extended FOIA training module for USDA's FOIA professionals. Lessons 1-8 were published in the Department's training repository in early January. However due to the recent passage of the 2016 FOIA Amendments, Lessons 7 and 8 were recently pulled and revised along with the remaining content not previously posted. These along with the remaining lessons for module two titled *Exemption Application* are now scheduled for publication by the close of the current fiscal year.

Protecting Networks and Information - Prevent Malicious Cyber Activity: The Office of Information Security (OIS) is actively monitoring a rapidly growing volume of IT threat vector data for USDA. In 2016, OIS detected and opened tickets on 2,828 cyber incidents. This is about a 14 percent increase from the previous year. The OIS continues to evolve the capabilities of the tools used to detect cyber incidents.

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. In 2016, additional hardware was purchased and used to upgrade the tool cluster and it is now processing 100,000 events per second. Most of this processing is performed using open source technologies and code generated by SOC employees. Continuing to upgrade the solution and increasing data storage capacity, processing power capability

## OFFICE OF THE CHIEF INFORMATION OFFICER

and analysis skills will continue to provide actionable intelligence the OIS needs to proactively improve IT security and agency program operations without service interruption.

OIS 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.

In 2016, the USDA became the first Department to formally test an Incident Response Exercise using a Major Incident. The OIS has increased its Incident Response capability by adding staff to obtain full 24x7 Incident Monitoring and Response coverage. Additionally, the OIS updated its Service Desk Incident ticketing/tracking system using the latest guidance from DHS US-CERT on Threat Vectors. The OIS 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 detection;
- Network behavior analysis;
- Malware detection and prevention; and,
- Network packet analysis.

The OIS provides system and service resources in support of the federally mandated Continuous Diagnostics and Mitigation 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 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 2017, if approved, OCIO will continue the cyber security policy remediation process to update aged cyber security policies and align them with FISMA, OMB, and NIST requirements.

In 2016, OIS addressed one and began addressing five of the remaining 17 NIST SP 800-53 control families that need new or updated policies. Additional work on five other cyber security policies in 2016 addresses specific IT topics needed by an agency IT program and gaps in the USDA IT security program identified by the OIG and the CISO. In 2017, if approved, OIS 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.

## OFFICE OF THE CHIEF INFORMATION OFFICER

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:

- Windows 2003 - consolidation of support services. As of October 1 there were 14 remaining servers under support. This is down from the almost 400 servers when the project started;
- AutoDesk; and
- FOIA system (FOIAXpress) system upgrade.

Contracting Agreements/Strategic Sourcing/Category Management: 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 are valued at over \$72 million and 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.

New contracts under evaluation:

- Anti-Malware software;
- Laptop / desktop contract;
- Consulting services;
- Adobe Connect (contract consolidation);
- IBM Software (contract consolidation); and
- Tableau.

### Selected Examples of Recent Progress:

Enterprise Architecture Division: The 2016 accomplishments include:

- Developed and established the Agriculture Data Domain for inclusion in the National Information Exchange Model (NEIM) community;
- Developed and published an EA Departmental Regulation (DR) and made significant progress towards completion of the EA Departmental Manual (DM);
- Updated USDA standards profile and created standards forecast based on the USDA standards profile;
- Led the OCIO integrated project to develop requirement and alternative analysis for a common, centralized, and authoritative solution to access consolidated system, application and investment information;
- Developed a new EA Governance structure and created an EA Executive Steering Committee;
- Completed 100 percent Departmental Integrated Data calls on time; and
- Collaborated with multiple civilian agencies Chief Architects and the Federal Chief Architect to share best practices and lessons learned.

### Policy and IT Strategic Planning:

OCIO provided 226 reviews on 46 Departmental Directives which include Regulations, Manuals, Notices, and other guidance. In addition, OCIO processed 52-non-IT related Departmental Regulations, Manuals, Notices, and other guidance. There were over 50 new and revised IT directives in development to address key policy gaps, audit recommendations, and OCIO management priorities at the end of 2016. Based on a policy program assessment and roadmap conducted in 2014, OCIO's policy division completed two projects in 2016. 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 continued the development of new policy training modules. OCIO developed a revision to the *USDA Information Technology Strategic Plan* and a new *Policy and Planning Strategic Plan*, both of which were submitted for approval in 2016. OCIO reviewed and approved 21 Departmental forms for publication.

OFFICE OF THE CHIEF INFORMATION OFFICER

<b>OCIO Departmental Directives and Forms Activities</b>	<b>FY2015</b>	<b>FY2016</b>
OCIO Reviews of IT Departmental Directives	193	226
OCIO Processed IT Departmental Directives	40	46
OCIO Processed Non-IT Departmental Directives	35	52
Total OCIO Processed Departmental Directives	75	98
IT Departmental Directives in Development to Address Policy Gaps, Audit Recommendations, and Management Priorities	49	50
Departmental Forms Approved and Published	16	21

Cyber Security:

ASOC performs annual penetration testing of all agency/office environments and identifies vulnerabilities to provide actionable intelligence that supports timely remediation.

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 oversaw 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.

In 2016, ASOC implemented additional systems to increase cyber incident detection capabilities resulting in an increased detection rate of attacks. Additionally, the capabilities the SOC has implemented are mostly leveraging open source code which reduces the total cost of ownership. The ASOC also matured several processes that allowed it to maintain compliance with the DHS US-CERT 1 hour incident notification Service Level Agreement.

In 2016, ASOC continued the deployment of CDM Phase 1 solutions to increase USDA-wide visibility and management capabilities of hardware and software assets connected to the USDA network.

Enterprise Project Management Services (EPMS): EPMS serves as USDA's primary resource for expertise on enterprise program management and provisions integration and support for project management of IT enterprise initiatives, including project planning, risk analysis, and project reporting; implements continuous improvements across the OCIO spectrum of activities, and by extension, across the Department;

The 2016 accomplishments include:

- The conversion to Office 365. Under this contract option, USDA will have an unlimited archive in Both the MS and Proof Point Archives which will result in a cost avoidance of over \$8M in the next two years. In addition, the USDA will have access to many additional features some of which include:
  - Agencies no longer have to maintain Office, Exchange CALs, and SharePoint CALs on their EA Enrollments. This offering provides USL dual rights which allows USDA hybrid capabilities to deploy Exchange, Office, SharePoint and Lync on-premise and/or in O365;
  - Office will be able to be installed 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; and
  - Hosted Voice Mail.

## OFFICE OF THE CHIEF INFORMATION OFFICER

- Home Use Program (HUP) – A modification was made to the contract to allow USDA employees’ access to the existing HUP. The HUP program allows users to become proficient in the software while working on their home systems.
- 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 that have been supported.
- Provided Project Management Support for FOIAXpress and the Public Access Link (PAL):
  - Coordinated all matters associated with continued use of the FOIAXpress system, including planned software upgrades by AINS, SSL certificate renewals, A&A continuous monitoring, annual assessment of distributed licensing costs, and advanced troubleshooting for users experiencing Document Management issues;
  - Created Correspondence Templates as requested by agency users; and
  - Moderated monthly calls with Departmental FOIA Officers and AINS to discuss FOIAXpress/PAL implementation progress and issues.

### 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. The 2016 accomplishments include:

- EPMS participates in GSA strategic sourcing initiatives and has discussed the Microsoft contracts. Based on GSA feedback and a recent evaluation for a Strategic Sourcing vendor, USDA is best in Government for pricing on these contracts. This holds true even against agencies that purchase 10 times the amount of software.
- Establishment of and Adobe Acrobat Enterprise agreement.
- New email archiving contract.

## OFFICE OF THE CHIEF INFORMATION OFFICER

### Summary of Budget and Performance

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.

The Department will be revising the USDA Strategic Plan later in the spring and expects to release it with the FY 2019 President's Budget.

#### Key Performance Measures

Percentage of USDA electronic documents that are 508 compliant and accessible.							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	N/A	1%	1%	45%	45%
Dollars (in thousands)	\$4,358	\$4,494	\$5,591	\$4,494	\$4,494	\$4,494	\$4,494

#### Selected Past Accomplishments toward Achievement of the Key Outcome:

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 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 developed a governance framework that 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.

The OCIO has also developed a comprehensive IT governance process that incorporates an integrated governance framework that allows for the Information Management Division (IMD), Section 508 to provide the executive teams with a process for reviewing Section 508 language and law within investments and providing guidance to investment managers throughout a project's Agriculture System Development Life Cycle (AgSDLCL).

#### Selected Accomplishments Expected at the FY 2018 Proposed Resource Level:

- 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, Agency Administrators, the CIO Council, Capital Planning and Investment Control (CPIC) administrators, Program and Project Managers, Enterprise Architecture community, and agency and staff office CIOs on the Enterprise IT governance process and framework;
- Fully implement the Enterprise IT governance process and framework;

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.

OFFICE OF THE CHIEF INFORMATION OFFICER

Key Performance Measures

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.							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	N/A	N/A	99%	95%	95%

Decrease in one day of overdue Plans of Actions and Milestones (POAM) for remediation and vulnerabilities.							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	N/A	41%	37%	31%	26%

Percent of incidents closed within 30 days.							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	N/A	85%	85%	86%	89%

Cybersecurity Assessment and Management Tool (CSAM).							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	35%	65%	75%	85%	90%
Dollars (in thousands)	\$25,861	\$26,160	\$26,802	\$27,496	\$27,585	\$28,000	\$44,000

Selected Past Accomplishments toward Achievement of the Key Outcome:

The USDA Office of Information Security (OIS), formerly the Agriculture Security Operations Center, provides Federal Information Security Modernization Act (FISMA) mandated oversight and enforcement to ensure compliance with federally cyber security regulations and initiatives and requirements from the Office of Management & Budget (OMB) and National Institute of Standards in Technology (NIST), and operational directives from the Dept. of Homeland Security (DHS). OIS works toward improving departmental cyber security risk management, cyber security policy, continuous monitoring, and overall strengthening information assurance and security throughout the Department.

- Active monitoring of a rapidly growing volume of IT threat vector data for USDA. OIS continued 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 to increase knowledge of our adversaries and their targets;
- Improved Incident Handling and Incident Response capabilities within USDA, including 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 resulting in a 72% compliance with the DHS SLA of 1-hour notification;
- Improved the availability of the security solution to 99.9% availability. The security solution provides the foundation for USDA enterprise-wide security monitoring, detection, and protection. The security solution performs a mix of critical security functions in near-real-time including: (a) Intrusion detection and prevention; (b) Network data loss detection; (c) Network behavior analysis; (d) Malware detection and prevention; and (e) Network packet analysis;

## OFFICE OF THE CHIEF INFORMATION OFFICER

- Streamlined and updated the cyber security policy development and publications by establishing a dedicated policy development team, consolidating and reducing the number of cyber security policies subject for review and updating, and ensuring compliance with FISMA while adapting policies to evolving cybersecurity threats and risk and the latest IT solutions;
- Enhanced USDA's cyber security compliance and enforcement framework that streamlined and improved the quality and effectiveness of assessments and oversight;
- Implemented Departmental cyber security scorecards that highlights agencies' performance in a variety of security-related areas. The scorecards are also used in CIO performance evaluations and to approve IT acquisition requests;
- Assigned security analysts to agencies to provide expert knowledge and guidance to the agencies and offices in addressing their weaknesses as identified in Plans of Action and Milestones (POA&Ms);
- Closed over 800 POA&Ms through FY16 and 17, 400 of which were related to longstanding IT Material Weaknesses;
- Updated our IT system repository and systems to NIST SP 800-53 Revision 4;
- Continued implementation, integration and support of the Continuous Diagnostics Mitigation (CDM) Phase 1 solution; and
- Developed Department level Cybersecurity and ISCM Strategies.

### Selected Accomplishments Expected at the FY 2018 Proposed Resource Level:

- Streamline the development process for Departmental cyber security policies and procedures to ensure alignment with FISMA, OMB, and NIST requirements and timely publication of new policies;
- Integrate compliance and enforcement tools with operational toolsets for increased capabilities in CDM and continuous monitoring requirements;
- Strategically enhance Department level compliance, oversight and enforcement program to provide streamlined 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;
- Advanced planning for Departmental continuous monitoring and ongoing A&A activities leveraging CDM Phase 1 capabilities and tools automation;
- Complete deployment of CDM Phase 1 solutions through full operational sustainment and maturation of capabilities, including governance, refinement and/or development of new processes, Department level training and program oversight. Data collected and reported by CDM Phase 1 solutions enables USDA security and IT management and technical staff to quickly and continuously identify, prioritize, and remediate risks in near real-time;
- Address and mitigate 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; and (d) Configuration Management;
- Comprehensive reviews of security topics critical to the Department, including security of emerging technology and practices;
- Tighter integration of cyber security compliance requirements and security operations to support external reporting (FISMA, OMB, OIG, GAO, A-123, etc.);
- Expand Big Data technologies and capabilities to better collect and process massive amounts of security related information from an increasing number of USDA agencies for the purposes of detecting cyber incidents;
- Upgrade the existing Intrusion Detection/Protection solution, increase data storage capacity, processing power capability and analysis skills to gather and analyze actionable intelligence in order to improve IT security and agency program operations without service interruption;
- Upgrade the existing cryptographic devices and continue support 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;
- Development and full operationalization of post-detection activities (Analyze; Respond; Recover) is expected as well on an enterprise-wide basis; and
- Complete penetration testing and operational security assessments of USDA agencies, which is essential to

OFFICE OF THE CHIEF INFORMATION OFFICER

identifying department-wide cybersecurity vulnerabilities and risks and enables USDA agencies to identify, prioritize, and remediate vulnerabilities and risks in a timely manner, improve their security posture, and strengthen the protection USDA information and associated assets overall.

Key Performance Measures

Eliminate duplicative IT investments.							
	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Target	2018 Target
Units	N/A	N/A	N/A	N/A	Est. Baseline	1%	1%
Dollars (in thousands)	\$13,778	\$9,797	\$11,638	\$13,055	\$12,312	\$11,959	\$10,456

Selected Past Accomplishments toward Achievement of the Key Outcome:

The Capital Planning & IT Governance has developed a comprehensive IT governance process that incorporates an Integrated and incremental 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, 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, fleets, hardware, software, and personnel (federal and contractor) that are associated with those IT investments.

The Capital Planning and IT Governance Division (CPITGD) continues to ensure alignment of IT investments with mission and business priorities through iterative governance processes and sound portfolio management. Embedded in the approach is the adherence to the Clinger-Cohen Act of 1996, the Federal Information Technology Acquisition Reform Act (FITARA) and the OMB Circular A-11 and OMB Circular A-123.

CPITGD aligns IT capabilities and resources with strategic business objectives that affords the business and IT to invest in the right initiatives at the right time, ultimately ensuring IT investments achieve expected outcomes, provide transparency into IT spending decisions, create opportunities for cost savings/avoidance, and streamline and offer shared capabilities that cut across multiple areas.

Capital Planning and IT Governance purview includes OMB required monthly and annual Investment submissions, CIO standing reporting frequency of scoring and reviews of investments, Acquisition Approval Requests (AARs), Detailed Life Cycle Costs (DLCCs) updates, monthly and ad hoc required Earned Value Management reviews and updates, Re-baseline Performance Changes, IT Governance Decision Gates reviews, Departmental TechStats, OMB led PortfolioStats, quarterly OMB Integrated Data Collection, Annual OMB FedStats, Program and Project Managers Certifications and the CIO’s Annual Portfolio Reviews of Agencies and Staff Offices. In addition, we have a portfolio management tool, AgMAX, to automate and enhance capital planning investment control and portfolio management practices.

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.

- 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 million in annual spending) and identified key levers to achieve cost avoidance and savings including Best Price Evaluation, Volume Concentration, Product Specification Improvement and

## OFFICE OF THE CHIEF INFORMATION OFFICER

Demand Management. The SOPG selected six IT categories after performing initial spend analysis using recent Fiscal Year spending data, and assessing opportunity attractiveness. 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. (As a Note: SOPG was replaced by Category Management under the OMB directives: Category leads for Hardware (OMB Memo M-16-02) and IT Software (OMB Memo M-16-12). The goals of SOPG have been incorporated and continued in Category Management for 2017 and going forward.)

### Selected Accomplishments Expected at the FY 2018 Proposed Resource Level:

- Continue refining standards, conduct system mapping, and start building out system specific standards profile;
- Analyze annual Agency Portfolio Reviews to identify areas and opportunities for improvement (engineering, consolidation, de-commissioning, etc.);
- Identify and consolidate duplicative IT commodity services to identify opportunities for enterprise solutions;
- Develop framework for measuring cost savings and associated re-investments;
- Assess investments through the CPIC and IT Governance portfolio management 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;
- Perform formal governance gate reviews of new concepts propose to be investments and existing major IT investments to determine the optimum path forward and the health of the investment;
- Complete a comprehensive redesign of the Enterprise Architecture Repository (EAR) to provide near real-time information on USDA's IT Portfolio. In addition, the EA organization will continue to successfully work with Agencies, Staff Offices, and across OCIO to ensure IT asset information is accurate and up to date. These efforts support the Federal Enterprise Architecture Framework, OMB reporting requirements, and most importantly are critical to a having a data driven environment for better IT investment decision making in USDA.
- Continue creating repeatable and incremental IT Governance and Portfolio Management processes.
- Continue the integrated partnership through regular customer engagements with the business and IT communities in order to capitalize on shared service opportunities, increase cost savings and avoidance, increase innovation and decrease legacy systems which ultimately decreases the cost of operating and maintain unsupported systems.
- Continue to engage the CIO Council chartered Investment Management Interest Group (IMI) known as Portfolio and Investment Management (PIM) Council in order to implement and provide best practices, incremental governance and processes and development and reduce "shadow IT" across USDA;
- Continue to train 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;
- Coordinate monthly IAB and E-Board meeting with the USDA leadership to make key decisions on IT investments;
- Continue to 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 oversee, analyze, measure performance and report outcomes in order to aide and turn around challenged investments as well as lessons learned to leverage of those successful investments.
- 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;
- Review and certify qualified applicants FAC-PPM levels 1-3;
- Lead and coordinate the quarterly PortfolioStat and Integrated Data Collection (IDC) required by OMB;
- Lead the CIO annual Portfolio Reviews with USDA Agencies and staff offices
- Coordinate in collaboration with OBPA the requirements of the OMB led FedStat for the CIO and Deputy Secretary;
- Lead and coordinate the USDA TechStat review process in coordination with the CXO teams; and
- Continue to implement and execute FITARA in partnership with the CXOs and agencies/staff offices.