Office of the Chief Information Officer

STATE OF IOWA

Terry E. Branstad, Governor
Kim Reynolds, Lt. Governor

Robert von Wolffradt
Chief Information Officer

Return on Investment Program

FY 12 Project Status Report
1/1/16

The Office of the Chief Information Officer is required to report on projects funded through the Return on Investment Program (ROI). The ROI program has been funded through an appropriation from the Technology Reinvestment Fund. The Technology Reinvestment Fund was created during the 2006 legislative session, and the first appropriations from this fund were for FY 2006-2007. The first report related to that fiscal year and was delivered to the legislature by January 1, 2008. This current report updates projects from fiscal year 12 and is the final report. Following is the section of the Code for the report excerpted from 8.57C:

> *Annually, on or before January 15 of each year, a state agency that received an appropriation from this fund shall report to the legislative services agency and the department of management the status of all projects completed or in progress. The report shall include a description of the project, the progress of work completed, the total estimated cost of the project, a list of all revenue sources being used to fund the project, the amount of funds expended, the amount of funds obligated, and the date the project was completed or an estimated completion date of the project, where applicable.*

Each project that received funding through the ROI program for the fiscal years contained in this report completed the following items. Where applicable, the ROI records for each project were used to complete items from Budget Offer and I/3 budget information.

- Project Name and Description
- All Revenue Sources for Funding
- Agency Submitting Request
- Percent of Completed Work
- Total Estimated Project Cost
- All Revenue Sources for Funding
- Expended Funds
- Obligated Funds
- Estimated Completion Date

OCIO collected these data items for all applicable ROI projects and sent the completed report to the following parties on January 15, 2016 before the filing deadline of January 15, 2016:

Legislative Services Agency
Department of Management

This table includes ROI reimbursements processed through DAS Finance, as of June 30, 2015.

Table A: FY 12 ROI Project Expenditures

Project Name	Agency	% Complete	Original Request	Adjusted Request	Expenditures to-date	Obligated Funds	Estimated Complete Date
Continuous Vulnerability Management	Chief Information Officer	100%	$ 585,000	$ 585,000	$ 585,000	$ 0	**Complete**
Personnel Skills Assessment*	Chief Information Officer	N/A	$ 400,000	$ 400,000	$ 0	$ 0	N/A
EVMS Refresh & Upgrade	Chief Information Officer	100%	$ 0	$ 0	$ 219,811	$ 0	**Complete**
FireEye Anti-Malware Protection	Chief Information Officer	100%	$ 0	$ 0	$ 180,189	$ 0	**Complete**
Gateway & Enterprise E-Mail Encryption Services, Phase 2*	Chief Information Officer	N/A	$ 300,000	$ 300,000	$ 0	$ 0	N/A
Statewide Address Geocoding, Phase 2	Natural Resources	100%	$ 550,000	$ 194,000	$ 194,000	$ 0	**Complete**
Critical Response Notification System	Veterans' Home	100%	$ 98,000	$ 98,000	$ 98,000	$ 0	**Complete**
Customer Portal*	Human Services	100%	$ 185,000	$ 66,728	$ 0	$ 0	**Returned**
Web Application Firewall, Phase 2	Chief Information Officer	100%	$ 0	$ 0	$ 41,728	$ 0	**Complete**
Web Application Firewall, Phase 3	Chief Information Officer	100%	$ 0	$ 0	$ 10,835	$ 0	**Complete**
Gforge Update	Chief Information Officer	100%	$ 0	$ 0	$ 3,759	$ 0	**Complete**
Enterprise A&A Enhancement	Chief Information Officer	100%	$ 0	$ 0	$ 10,406	$ 0	**Complete**
Core Infrastructure & Security Architecture Upgrades	Chief Information Officer	100%			$ 300,000	$ 0	**Complete**
TOTALS			$ 2,118,000	$ 1,643,728	$ 1,643,728	$ 0	

FY 12 appropriation within the Technology Reinvestment Fund to the Department of Administrative Services for technology improvement projects was $1,643,728.00

NOTE: Funds for the Gateway & Enterprise E-Mail Encryption Services project were reallocated to fund the Core Infrastructure & Security Architecture Upgrades project.
Funds for the Personnel Skills Assessment project were used to fund EVMS Upgrade and FireEye Anti-Malware projects.
Returned funds for the DHS Customer Portal project were used to fund Web Application Firewall, Gforge and Enterprise A&A projects.

FY 12 ROI funds reverted on June 30, 2015

Table B. FY 12 ROI Project Descriptions and Funding Sources

1. **Security: Continuous Vulnerability Management**

   Administrative Services project for the enterprise to fund phase two of the effort. In this phase of the security project, vulnerability-scanning devices will be deployed to all state agencies. This project includes vendor installation, hardware, software, project management, training, and technical consulting. The main outcome of the system is that all executive branch agencies receive timely and continuous automated IT audits for software vulnerabilities and for configuration management.

   Funding Sources: HSEMD funding is augmenting this initiative and is being used to bring the same service to cities, counties and schools.

2. **IT Personnel Skills Assessment**

   Administrative Services project for the enterprise to inventory and assess state personnel conducting IT functions. The scope includes skills such as programming, system design, system development, and other functions associated with IT staff. The goal of this assessment is to gather information to support the information technology redesign efforts by identifying the means to train and develop our IT professionals, as well as future needs of IT skills.

   Funding Sources: ROI Program funds from this project were used to fund other IT projects.

3. **EVMS Refresh & Upgrade**

   Chief Information Officer project by the ISO to provide additional IT security. Government entities are under persistent cyber-attacks from hackers. These attacks exploit applications, misconfigured IT systems, and cost billions of dollars every year. To ensure states operate in a secure manner and we protect our IT infrastructure, the government has mandated controls be implemented. Organizations are required to follow regulations such as FISMA, IRS Pub 1075, HIPPA, Red Flag Rules and others. To reduce this risk and meet the federal requirements we propose to continue the implementation of an enhanced vulnerability management reporting and Anti-Malware software security tools. The Tripwire Enterprise Vulnerability Management System (EVMS) currently supports 46 Iowa Counties, 47 State Agencies, 7 Iowa Cities and 17 Iowa School districts.   This very successful program has been in existence for over four years now and has helped in supporting State of Iowa, County, Cities and Schools in their vulnerability management and system patching.   The current systems (device profilers) hosted by the supported entities have come to their “end of life” support by the vendor.   The purchase of newly supported device profilers will allow this highly successful and important security program to continue for additional years to come.

   Funding Sources: Remaining ROI funds from other ROI project were expended for this project.

4. **FireEye Anti-Malware Protection**

   Chief Information Officer project by the ISO for additional IT security. The FireEye Network Threat Prevention Platform identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help the State of Iowa scale their advanced threat defenses. FireEye Network uses a signature-less FireEye MVX engine which executes suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments that track vulnerability exploitation, memory corruption, and other malicious actions. The FireEye Network Threat Prevention Platform will be deployed in a fashion that will support for a selected number or State Agencies, Counties and schools in Iowa.

   Funding Sources: Remaining ROI funds from other ROI project were expended for this project.

5. **Security: Gateway & Enterprise E-Mail Encryption Services, Phase 2**
   Administrative Services project for the enterprise to further improve gateway and e-mail encryption services. This security project will benefit the enterprise at large and will raise the security level of messaging to a level that would comply with the enterprise standards and defend against current cyber threats. Expected results include enhanced e-mail encryption, spam control and other related services.

   Funding Sources: ROI Program funds from this project were used to fund other IT projects.

6. **Statewide Address Geocoding, Phase 2**

   Phase 2 of the JCIO and Natural Resources project continues production of driveway addresses points and building points to be used in a statewide geocoding and address service. Phase 1 covered most of western Iowa, with Phase 2 working on south-central and northeast Iowa. As of December 1, 2012: 50 Phase 1 counties completed, 20 Phase 2 counties in progress. Phase 2 funding will be expended by 6/30/2013. Additional funding is needed to complete the state. All current Phase 2 funding obligated.
   Funding Sources: Pooled Technology Fund: $550,000 requested to complete eastern part of state, $194,000 awarded.

7. **Critical Response Notification System**

   Iowa Veterans Home project for a critical response notification system for unified campus wide communication during an emergency or time sensitive event. The project will fill the gap between IVH's Disaster Recovery plan and State of Iowa communications and DR efforts including COOP/COG.

   Funding Sources: Direct funding for this project provided entirely by the FY 12 ROI program.

8. **DHS Customer Portal**

   Human Services project to build on two DHS projects (OASIS and the Medicaid Portal), and will join additional DHS projects, specifically DHS's Electronic Case File. OASIS is DHS's web-based intake system for Iowans to begin the application process for several DHS programs. The Medicaid Portal was developed to support Medicaid providers, members and workers to web-enable the interactions each has with the Iowa Medicaid Enterprise. The unified Customer Portal will enable DHS customers across program boundaries to be able to securely interact with DHS workers and program staff.

   Funding Sources: The total of $66,728 was returned by DHS to be used for other technology projects of benefit to the enterprise. The DHS Portal project is complete, and the project was completed without the need for the additional ROI funds.

9. **OCIO Web Application Firewall, Phases 2 & 3**
   Chief Information Officer project to utilize remaining ROI project funds. The main benefit of the Web Application Firewall (WAF) will be to protect production web applications from external attacks and close vulnerabilities found during web security penetration scanning (example: SQL-Injection, Cross-Site-Scripting and DDOS attacks). Once vulnerabilities are found in applications, the ISO can then blacklist the results using the WAF. This will help remediate vulnerable applications until coding or other means can be used to correct them or the application can be replaced if out of support and funding is found. With the large number web application hosted by the OCIO, having the WAF will help in the protection of vital applications that intake, store and display very sensitive data collected by the State of Iowa thus reducing the risk of a data breach.
   Funding Sources: Remaining ROI funds from other ROI project were expended for this project.

10. **OCIO Gforge Upgrade**

    Chief Information Officer project to use remaining ROI funds from another a completed project. This OCIO project proposal is a request ROI funds to upgrade our instance of GForge, which is a tool used for storing and managing application code, tracking defects and enhancements, and storing technical project documentation. Currently, GForge supports more than 1,200 users representing approximately 200 organizations across state agencies, cities, counties and vendor communities. There are over

1,000 code commits per month on 40-60 projects. In the near future, the OCIO intends to rollout GForge to other agencies such as DNR and ICN; however, the current version has some performance and functionality concerns at the application, database and server levels that need to be addressed before moving forward. There is also an intention to utilize funds for purchasing web enabled Smart HDTVs to be utilized for displaying dashboard monitors and metrics across the department.
Funding Sources: Remaining ROI funds from other ROI project were expended for this project.

11. **OCIO Enterprise A&A Enhancement**

    Chief Information Officer project to use remaining ROI funds from another a completed project. This OCIO project proposal is a request ROI funds to upgrade the Enterprise Authentication & Authorization (ENTAA) enhancement project. The intent of the enhancement is to enable our ENTAA application to be mobile responsive – meaning the size of the screen will adjust to different devices such as tablets or smartphones. This enhancement will have a positive impact to approximately 200 applications across the state enterprise that utilize the ENTAA functionality.
    Funding Sources: Remaining ROI funds from other ROI project were expended for this project.

12. **OCIO Core Infrastructure & Security Architecture Upgrades**

    Chief Information Officer project to obtain equipment to provide the ability for ISO and Networking to simultaneously monitor data interfaces at new, higher speeds, with equipment designed to handle the throughput. Key benefits of the project were creation of a core data monitoring fabric parallel to the new core network. This improved the ability to analyze traffic for performance and capacity concerns, and improved data security by providing more thorough, comprehensive and non-disruptive monitoring for data security threats.
    Funding Sources: Remaining ROI funds from other ROI project were expended for this project.