



## Assistant Secretary for Resources and Technology: HHS Information Technology (IT) Security

### A. Funding Table

(Dollars in Millions)

	<b>Total Appropriated</b>	<b>Planned Obligations FY 2009</b>	<b>Planned Obligations FY 2010</b>
HHS Information Technology Security	\$50.0	\$31.9	\$18.1
<b>Total</b>	50.0	31.9	18.1

### B. Objectives

HHS is taking immediate action to improve the security of its computer systems, and this Recovery Act funding will accelerate these efforts. HHS computer systems and networks include sensitive data regarding public health, Medicare and programs that serve millions of children and families across the country.

Recent compromises of Federal government computer systems and data require concerted and coordinated actions across HHS that are commensurate with the sustained level of sophisticated cyber attacks targeting Federal government computer systems, including HHS computer systems. Department and Operating Division (OPDIV) security leadership embarked in early FY2009 on multiple discussions to define the requirements, scope, and desired security capabilities that would substantially improve the IT security posture of HHS as a whole. This spending plan reflects agency-wide collaboration. The initiatives identified here supplement the resources and funds already being spent by the OPDIVs.

A primary objective of the HHS efforts is to provide the ability to rapidly determine the enterprise security risk posture of operational IT systems and computer networks throughout the Department. This will require significant enhancements to our key information assurance capabilities in order to more effectively detect, defend, and mitigate attacks against HHS systems. Current capabilities vary across HHS organizational components. With interconnected computer systems, a weakness in any Operating Division potentially introduces security risks for all Operating Divisions. Reviews by the Office of the Inspector General (OIG) and the Government Accountability Office (GAO) identified a number of HHS computer systems security capabilities that were recommended for enhancement in order to better protect the Department's computer systems and data. This HHS IT security Recovery Act spend plan is intended to specifically address the issues and recommendations arising from forensics and audit reports.

IT security is a critical issue throughout the Federal government, as nation states, commercial competitors, identity thieves, and computer hackers have significantly ramped up their efforts to attack and penetrate U.S. government computer systems. HHS' ability to continue to fulfill our national health related mission and functions as



our budget grows to support economic recovery depends on our ability to maximize the secure use of the powerful computing resources that are available to us today.

### **C. Activities**

Recovery Act funds will be used to purchase hardware, software and IT security related services. The plan encompasses the following initiatives:

- **Security Incident Response & Coordination:** Funds will be used to significantly expand the capabilities of the recently established HHS Computer Security Incident Response Center (CSIRC), which is co-located with the CDC Security Operations Center in Atlanta. The CSIRC will expand to support 24 X 7 operations that will coordinate all Department and OPDIV actions to monitor, detect, react, and mitigate (or prevent) attacks against HHS and OPDIV systems. This will include the centralized reporting of security incidents to the U.S. Computer Emergency Response Team (CERT), which is operated by DHS. Nominal start-up activities were initiated for the CSIRC in September 2008, and included funding for one government FTE at the CDC in Atlanta, Georgia to manage the HHS CSIRC.
- **OPDIV Security Engineering and Technical Staff Support:** One of the highest priority requirements identified by each of the OPDIVs was the need for additional security technical staffing support. Funds will help alleviate the current security workload backlog of OPDIV security staffs. The backlog is identified in the remediation work associated with the Federal Information Security Management Act (FISMA) Plan of Action and Milestones (POAMs) that are in place at each of the OPDIVs. HHS has also been challenged to keep up with the weekly assignments and tasks generated by the US Computer Emergency Readiness Team (CERT). OPDIV reviews of security audit logs from firewalls, IDS systems, operating system logs, etc...require improvements. Automated tools can assist, but ultimately security technical staff must make a final determination for each of the alarms generated from system audit log data. The funding will assist each OPDIV in being able to respond in a more timely manner to US CERT tasks, and also begin more timely reviews of system audit logs, and reduce the POAM backlog.
- **Enterprise-wide Security Situational Awareness:** Funds will provide enhanced Department-wide computer systems intrusion detection capabilities, security information event management systems, and network forensics capabilities. This includes capabilities to collect and analyze the large set of security audit log data that is collected by HHS computer systems.
- **Endpoint (Desktop Computer) Protection, Internet Content Web Security Filtering, and Data Loss Prevention:** Federal government computers are being compromised by malicious software (malware) and other computer viruses and worms that are introduced into government computing environments when users unknowingly visit infected web sites. The malware takes advantage of any weak security controls that may be implemented in government computer systems. Funds will provide all OPDIVs with a number of advanced security tools to strengthen end user computer defense mechanisms against malware attacks, and also prevent sensitive data from being extracted from the Department's computer systems and databases.
- **Enhanced OPDIV Security Architecture, Engineering and Implementation:**



Utilizing an HHS contract managed by the Department CISO, this initiative develops or updates OPDIV plans for securely architecting our computing environments into secure enclaves. Provides a number of security solutions specifically for OS and IHS, enhancing the protection of sensitive data, and also provides for secure remote access, firewall upgrades, multi-factor authentication, network access control, and enhanced security of the domain name system (DNS).

#### **D. Characteristics**

Contracts will be competitively awarded utilizing Fixed Price with Economic Price Adjustment (EPA) provisions. Targeted recipients will be hardware and software vendors and contracted service providers.

HHS and the OPDIVs will leverage existing competitive contracts for efficiency purposes as much as possible. In the cases where an existing contract will be modified, HHS will ensure that such contract actions are publicized, justified, and reported accordingly. If new contracts are required, HHS will use competitive processes and publicize such opportunities as required, and report the resulting awards.

Implementation plan characteristics by investment are detailed below. HHS will be procuring a software tool to manage enterprise and internet web content filtering and a data loss prevention upgrade as a part of the \$5.0M Endpoint Protection and Data Loss Prevention initiative. An additional investment within the Endpoint Protection and Data Loss Prevention initiative is a \$2.06M software tool to enhance HHS IT security with an enterprise file and e-mail encryption capability. The Enhanced OPDIV Security Architecture Engineering and Implementation initiative is comprised of the \$1.675M enhanced security architecture analysis and roadmap development investment.

OPDIV Security Engineering and Technical Staff Support is a \$7.747M initiative which provides increased security engineering and technical staffing at the OPDIV level for the remainder of FY2009 and FY2010. In most cases, HHS will provide the funds to the OPDIVs to support the hiring of additional government FTEs to fulfill this initiative. HHS will also pursue contractor support for some of the advanced, highly technical security skills that are required.

Indian Health Service (IHS) will receive a transfer of funds, totaling \$1.628M to support several investments that fall within the Enhanced OPDIV Security Architecture Engineering and Implementation and Enterprise-wide Security Situational Awareness initiatives.

The HHS Information Technology Office (ITO) will receive a transfer of funds, totaling \$7.055M, to support several investments that fall within the Enhanced OPDIV Security Architecture Engineering and Implementation, OPDIV Security Engineering and Technical Staff Support, Security Incident Response & Coordination, and Enterprise-wide Security Situational Awareness initiatives.



Department of Health and Human Services  
 American Recovery and Reinvestment Act  
 Improving Accountability and Information Technology Security



The Centers for Disease Control (CDC) will receive a transfer of funds, totaling \$3.416M to support investments that fall within the OPDIV Security Engineering and Technical Staff Support initiative.

At CDC, the Cyber Security Incident Response Center (CSIRC) will receive \$21.419M to finance several investments that address the Security Incident Response & Coordination and Enterprise-wide Security Situational Awareness initiatives.

All contracts funded with Recovery Act allocations will be new contracts. In a small number of instances, new task orders may also be placed against contracts that were previously awarded via competitive procurements. Implementation plan characteristics by contract and investment are also included in the table below:

<b>Contract</b>	<b>Initiative</b>	<b>Total Value (\$M) – incl. contracting fee</b>	<b>Type (in accordance with FAR Part 16)</b>
Enterprise Filtering, Internet Web Filtering, and Data Loss Prevention Upgrade	Endpoint Protection and Data Loss Prevention	\$5.000	FP - EPA: Fixed Price w/ Economic Price Adj.
Enterprise File and E-mail Encryption Capability	Endpoint Protection and Data Loss Prevention	\$2.060	FP - EPA: Fixed Price w/ Economic Price Adj.
Enhanced Security Architecture Analysis and Roadmap Development	Enhanced OPDIV Security Architecture Engineering and Implementation	\$1.675	Enhanced OPDIV Security Architecture Engineering and Implementation
OPDIV Security Engineering and Technical Staff Support	OPDIV Security Engineering and Technical Staff Support	\$7.747	\$ FP - EPA: Fixed Price w/ Economic Price Adj.
IHS Investment	Enhanced OPDIV Security Architecture Engineering and Implementation; Enterprise-wide Security Situational Awareness	\$1.628	FP - EPA: Fixed Price w/ Economic Price Adj.
ITO Investment	Enhanced OPDIV Security Architecture Engineering and Implementation; OPDIV Security Engineering and Technical Staff Support; Security Incident Response & Coordination; Enterprise-wide Security Situational Awareness	\$7.055	FP - EPA: Fixed Price w/ Economic Price Adj.
CDC Investment	OPDIV Security Engineering and Technical Staff Support	\$3.416	FP - EPA: Fixed Price w/ Economic Price Adj.



<b>Contract</b>	<b>Initiative</b>	<b>Total Value (\$M) – incl. contracting fee</b>	<b>Type (in accordance with FAR Part 16)</b>
CSIRC Investment	Security Incident Response & Coordination; Enterprise-wide Security Situational Awareness	\$21.419	FP - EPA: Fixed Price w/ Economic Price Adj.

## E. Delivery Schedule

HHS goal is to get the majority of planned IT security contract awards in place by the end of FY2009. Each of the initiatives will be pursued concurrently. A detailed project management plan will be used to manage the overall efforts. There are a variety of deliverables that are associated with each initiative, but the primary deliverables are the new or enhanced security capabilities that will be provided with each initiative. Once the capability is established, (such as the HHS CSIRC, or the procurement and fielding of endpoint security solutions), the initiative will not necessarily be “complete”, as there will be continuing license renewal costs to sustain the capabilities in the outyears.

Following is a preliminary delivery schedule by initiative:

### June 2009

- OPDIV Security Engineering Technical Staff Support: Acquisition paperwork will be processed and completed by June 2009, at which time funds will be transferred to OPDIVs to support this task. OPDIVs will be required to report periodically to HHS on the status of the investment progress throughout the performance period, ending September 30, 2010.

### July 2009

- Endpoint (Desktop Computer) Protection, Internet Content Web Security Filtering, and Data Loss Prevention: Phase 1 incorporates the acquisition process for the Enterprise-wide software licenses. Currently, this process is estimated to be complete by July, 2009. Phase 2 is software deployment, which is planned to begin July 2009 and be complete by December 30, 2009. Maintenance and outyear support, phase 3, covers the remaining period of performance for Recovery Act funding, through September 30, 2010.
- Enhanced OPDIV Security Architecture, Engineering and Implementation: Preliminary planning and schedules for security architecture reviews should be complete in July 2009. This investment will have a staggered rollout as the Security Architecture and Roadmap Development team visits and reviews each OPDIV and proceeds to deliver findings and recommendations. For larger OPDIVs, this process is expected to take approximately four months each. Smaller OPDIVs are expected to be reviewed together over a period lasting approximately four months. Implementation support will be provided after reports have been presented to OPDIVs, and this support will remain in effect until September 30, 2010.

### August 2009



- **Security Incident Response & Coordination:** Funding obligations to OPDIVs to cover OPDIV level investments should be complete by August, 2009. OPDIVs will be required to comply with periodic reporting requirements for the duration of the performance period, through September 30, 2010. Qualified security support staff will be in place by September 2009. The required Security Incident Response software and hardware will be procured by September 30, 2009 with installation of the products by January 2010. Testing and training of the Security Incident Response System will be completed by April 2010 with support continuing through September 2010.
- **Enterprise-wide Security Situational Awareness:** Funding obligations to OPDIVs to cover OPDIV level investments should be complete by August, 2009. OPDIVs will be required to comply with periodic reporting requirements for the duration of the performance period, through September 30, 2010. Qualified security support staff will be in place by September 2009. The required Security Situational Awareness software and hardware will be procured by September 30, 2009 with installation of the products by January 2010. Testing and training of the Security Situational Awareness System will be completed by April 2010 with support continuing through September 2010.

## **F. Environmental Review Compliance**

For all IT security initiatives, HHS will comply with E.O. 13423 regarding the purchase of energy efficient hardware and related equipment and products. Annually, 95% of electronic products purchased will meet Electronic Product Environmental Assessment Tool standards, and HHS will enable Energy Star® features on 100% of computers and monitors. In addition, HHS will reuse, donate, sell, or recycle 100% of electronic products using environmentally sound management practices. Additionally, it is not anticipated that any of the IT security initiatives will introduce extraordinary circumstances or construction projects necessary to support IT infrastructure improvements.

Therefore, this activity qualifies for a Categorical Exclusion under the HHS General Administration Manual (GAM) 30-20-40 Category 2 –Functional Exclusion 2.c. An Environmental Assessment (EA) will not be required in support of the IT security initiatives. A memorandum documenting this exclusion will be entered into the record and the activity is subject to the HHS Section 1609(c) reporting

## **G. Measures**

The Federal Information Security Management Act (FISMA) has identified a number of security performance measures that HHS and all OPDIVs are already using to monitor the effectiveness of the security controls in HHS enterprise applications and network systems, and also the effectiveness of OPDIV applications and network systems. The existing Department FISMA program reporting processes will be used to monitor for improvements in the security performance of the Department as a result of Recovery Act funds expenditures. The Department FISMA program reporting processes include quarterly and annual formal reporting to the Office of Management and Budget (OMB), and are annually reviewed by the OIG. The HHS Chief Information Officer (CIO) Council and Information Technology Investment Review Board (ITIRB) will also play a role in ensuring accountability.



Specific output performance measures will be used to track the results of Recovery Act funding and will help to enhance and improve the security of HHS computer systems:

- Percentage of HHS laptops and desktops secured with encryption.
- Percentage of HHS enterprise network infrastructure monitored by the CSIRC with automated intrusion detection systems.
- Percentage of HHS IT systems protected with advanced Internet content filtering and anti-malware solutions.
- Percentage of HHS critical IT systems audit logs analyzed by the CSIRC and OPDIV staffs for intrusions and security attacks.
- Percentage of system security weaknesses completed on schedule, in accordance with updated FISMA system plans of actions and milestones (POA&Ms).

To ensure that OPDIVs understand and can meet the objectives, outcomes and accountability expectations associated with the allocation of Recovery Act funds to OPDIV IT security programs, the HHS Chief Information Security Officer (CISO) will provide additional guidance to the OPDIVs to support the enhanced monitoring and reporting required for Recovery Act funds. All contracts will incorporate the reporting requirements of Section 1512, thereby increasing the level of transparency and accountability on the part of the contractors.

## **H. Monitoring and Evaluation**

All Recovery Act programs will be assessed for risk and to ensure that appropriate internal controls are in place throughout the entire funding cycle. These assessments will be done consistent with the statutory requirements of the Federal Manager's Financial Integrity Act and the Improper Payments Information Act, as well as OMB's circular A-123 "Management's Responsibility for Internal Control."

Internal HHS investment review boards, the HHS Recovery Act Oversight Committee, and the HHS Assistant Secretary of Resources and Technology Office of the Chief Information Officer (ASRT/OCIO) staff will all be involved in the management and/or oversight of Recovery Act HHS IT Security investments and their associated performance measures and risks. Periodic reviews on at least a monthly basis of the program's progress will be performed by the HHS CIO Council and the ITIRB.

The ASRT/OCIO will provide oversight and management for the spend plan. Each OPDIV will also be responsible to ASRT/OCIO for carrying out activities, for providing funds control, and satisfying Recovery Act reporting requirements.

The ASRT/OCIO will conduct program reviews for each initiative, and will require formal OPDIV reporting to account for Recovery Act funds expenditures.



## **I. Transparency**

HHS will be open and transparent in all of its contracting and grant competitions and regulations depending on what is appropriate for your program activities that involve spending of Recovery Act funding consistent with statutory and OMB guidance.

HHS will ensure that recipient reporting required by Section 1512 of the Recovery Act and OMB guidance is made available to the public on Recovery.gov by October 10, 2009. HHS will inform recipients of their reporting obligation through standard terms and conditions, contract solicitations, and other program guidance. HHS will provide technical assistance to contractors and fully utilize Project Officers to ensure compliance with reporting requirements.

## **J. Accountability**

To ensure that managers are held to high standards of accountability in achieving program goals under the Recovery Act, HHS will build on and strengthen existing processes. Senior IT security program officials will meet regularly with senior Department officials to ensure that projects are meeting their program goals, assessing and mitigating risks, ensuring transparency, and incorporating corrective actions. The personnel performance appraisal system will also incorporate Recovery Act program stewardship responsibilities for program and business function managers.

## **K. Barriers to Effective Implementation**

The potential for contracting and award date delays is considerable due to acquisition lifecycle risks. Acquisition life cycle risks, such as scheduling delays, are significant due to the level of effort required in developing approved statements of work and acquisition plans. Acquisition risk is present within the request for proposal (RFP) process and could include delays in the release of acquisition paperwork to the public for bids, a lack of adequate response to the RFP, or vendor cost proposals higher than the budgeted amount expected by the Government. Acquisition lifecycle risks also include the large volume of Recovery Act contracts which need to be set in place across the federal government, contracting offices (e.g., PSC, NIH etc) being overburdened, and the significant effort required to develop acquisition documents including acquisition plans and SOWs.

A second barrier to effective implementation will be the significant level of effort required to coordinate and oversee OPDIV Recovery Act activities. To mitigate this risk, the ASRT/OCIO will follow a centralized reporting and evaluation model for the spend plan investments. Each OPDIV will be responsible to ASRT/OCIO for carrying out activities, for providing funds control, and satisfying Recovery Act reporting requirements. The ASRT/OCIO will conduct program reviews for each initiative, and will require formal OPDIV reporting to account for Recovery Act funds expenditures.

## **L. Federal Infrastructure**

In support of government-wide sustainable infrastructure efforts, all IT security initiatives will also comply with E.O. 13423 regarding the purchase of energy efficient hardware and related equipment and products. HHS will comply with requirements



Department of Health and Human Services  
American Recovery and Reinvestment Act  
Improving Accountability and Information Technology Security



to extend the lifecycle replacement timeframes of desktops, laptops, and other IT equipment, by requiring the use of the most energy efficient devices available. Annually, 95% of electronic products purchased will meet Electronic Product Environmental Assessment Tool standards, and HHS will enable Energy Star® features on 100% of computers and monitors. In addition, HHS will reuse, donate, sell, or recycle 100% of electronic products using environmentally sound management practices.