HHS Information Technology (IT) Security

A. Funding Table

(Dollars in millions)

Program/ Project/Activity	Total Appropriated	FY 2009 Actual Obligations	FY 2010 Estimated Obligations
HHS Information Technology Security	$50.00	$6.148	$43.852

B. Objectives

Recovery Act funding will accelerate HHS efforts to improve the security of its computer systems, which must protect the sensitive information held by the agencies many health, social, and research programs.

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 FY 2009 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. The initiatives identified here reflect agency-wide collaboration.

A primary objective of HHS IT security efforts is to have the ability to rapidly determine the enterprise security risk posture of operational IT systems and computer networks throughout the Department. Significant enhancements to our key information assurance capabilities will be required 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 OPDIV potentially introduces security risks for all OPDIVs. Reviews by the Office of the Inspector General (OIG) and the Government Accountability Office (GAO) recommended a number of HHS computer systems security capabilities for enhancement. This HHS IT security Recovery Act spend plan addresses 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 four initiatives, which streamline the original five developed at the start of the program. The new initiatives reorganize program activities in a more logical and efficient manner:

- **Security Incident Response & Situational Awareness; (CSIRC):** Expand capabilities of the HHS Computer Security Incident Response Center (CSIRC), which is co-located with the CDC Security Operations Center in Atlanta, GA. Provide enhanced Department-wide computer systems intrusion detection capabilities, security information event management systems, and network forensics capabilities.
- **Federal Information Security Management Act (FISMA) - Security Engineering and Technical Staff Support:** Alleviate the current security workload backlog of OPDIV security staffs, allowing OPDIVs to respond in a more timely manner to FISMA program tasks, begin more timely reviews of system audit logs, and reduce the Plan of Action and Milestones (POA&M) backlog.
- **Computing Infrastructure Security Redesign Projects:** Develop or update OPDIV plans for securely architecting our computing environments into secure enclaves; implements a number of network security enhancements at several OPDIVs.
- **Endpoint Protection Security Tools:** Provide OPDIVs with advanced security tools to strengthen end user computer defense mechanisms against malware attacks, and help prevent sensitive data from being extracted from the HHS computer systems and databases.

D. Characteristics

Contracts will be competitively awarded as Fixed-Price (FP) or Firm-Fixed-Price (FFP). 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 OPDIV are detailed below.

OS (HHS CSIRC): $25.586M to address risks/vulnerabilities associated with the inability to detect and effectively respond to security incidents in HHS/OPDIV systems. Contracts include labor support, a portion of which will assist OPDIVs in installation of the CSIRC security product deployments. Major contracts include CSIRC IT infrastructure, network forensic solutions, intrusion detection/prevention solutions, and security information and event management solutions. Additional forensics and malware analysis tools will also be purchased.

OS (ITO): $7.055M to strengthen vulnerabilities in security infrastructure and augment endpoint protection. Over 25 projects have been identified including efforts to improve identity management, firewall applications, and network forensics.

OS (OCIO IT Security Program - Secure One): $5.918M to fund staffing support for FISMA compliance, security vulnerability weakness remediation, solutions for endpoint protection, and security architecture planning. Two key contracts include the Enterprise File and E-Mail Encryption Capability Project and the Enhanced Security Architecture Analysis procurement. Additionally, OCIO IT Security will add eight FTE to aid program support.

IHS: $2.240M for security infrastructure and endpoint protection vulnerability projects. Projects include efforts to support multi-factor authentication, vulnerability management, and intrusion detection systems.

CDC: $6.328M for security infrastructure and endpoint protection vulnerability projects. Two contracts include firewall upgrades and software/hardware redundancy, and security engineering support. Funding will also be used for network security upgrade project planning and encryption project, and to procure Department-wide licenses for security solutions for Internet content filtering, malware detection, and data loss prevention.

CMS: $1.187M to fund four FTE for FISMA compliance and security vulnerability weakness remediation support.

FDA: $.679M to fund five FTE for FISMA compliance and security vulnerability weakness remediation support.

HRSA: $.335M to fund two FTE for FISMA compliance and security vulnerability weakness remediation support.

OIG: $.671M to fund two FTE for FISMA compliance and security vulnerability weakness remediation.

The majority of contracts funded with Recovery Act resources 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 included in the table below:

OPDIV	Initiative	Total Value ($M)	Type (in accordance with FAR Part 16)
OS (HHS CSIRC)	FISMA - Security Engineering and Technical Staff Support Security Incident Response & Situational Awareness; (CSIRC)	25.586	Fixed-Price (FP) / Firm-Fixed-Price (FFP)
OS (ITO)	Computing Infrastructure Security Redesign Projects	7.055	Fixed-Price (FP) / Firm-Fixed-Price (FFP)
CDC	FISMA - Security Engineering and Technical Staff Support Security Incident Response & Situational Awareness; (CSIRC) Computing Infrastructure Security Redesign Projects Endpoint Protection Security Tools	6.328	Fixed-Price (FP) / Firm-Fixed-Price (FFP)
OS (OCIO)	FISMA - Security Engineering and Technical Staff Support Endpoint Protection Security Tools	5.918	Fixed-Price (FP) / Firm-Fixed-Price (FFP); Government, Full Time Equivalent Hire
IHS	FISMA - Security Engineering and Technical Staff Support Computing Infrastructure Security Redesign Projects	2.240	Fixed-Price (FP) / Firm-Fixed-Price (FFP)
CMS	FISMA - Security Engineering and Technical Staff Support	1.187	Fixed-Price (FP) / Firm-Fixed-Price (FFP); Government, Full Time Equivalent Hire
FDA	FISMA - Security Engineering and Technical Staff Support	0.679	Government, Full Time Equivalent Hire
OIG	FISMA - Security Engineering and Technical Staff Support	0.671	Government, Full Time Equivalent Hire
HRSA	FISMA - Security Engineering and Technical Staff Support	0.335	Government, Full Time Equivalent Hire

E. Delivery Schedule

The delivery schedule for IT Security ARRA investments is organized by initiative. All four initiatives will be pursued concurrently. Although there are a variety of deliverables and performance measures associated with each, the primary deliverables are the new or enhanced security capabilities that will be provided. 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. HHS will award all IT security contracts by the end of FY 2010.

- **Security Incident Response & Situational Awareness; (CSIRC):** Begin obligations in Q4 FY 2009, complete obligations in Q3 FY 2010, and full operational capability by end of FY 2011.
- **FISMA - Security Engineering and Technical Staff Support:** Begin obligations in Q4 FY 2009, complete obligations by Q4 FY 2010, and contracted support complete by Q4 FY 2011.
- **Computing Infrastructure Security Redesign Projects:** Begin obligations in Q4 FY 2009, complete obligations by Q3 FY 2010, and redesign projects complete by end of FY 2011.
- **Endpoint Protection Security Tools:** Begin obligations in Q1 FY 2009, complete obligations in Q4 FY 2010, partial implementation in Q4 FY 2010 with full tool deployment complete by the end of calendar year (CY) FY 2011.

F. Environmental Review Compliance

HHS does not anticipate 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:

Outcome/ Achievement	Frequency	Type	Units	Type	9/30/09	12/31/09	3/31/10	6/30/10	9/30/10	12/31/10	3/31/11	6/30/11	9/30/11	Program End
Percentage of HHS laptops and desktops with sensitive information secured with encryption capabilities.	Quarterly	Output	Percent	TARGET	40	40	40	40	55	65	75	85	100	100
				ACTUAL	40	40	40							
Percentage of HHS enterprise network infrastructure monitored by the CSIRC with automated intrusion detection systems.	Quarterly	Outcome	Percent	TARGET	55	55	55	55	60	70	80	90	90	90
				ACTUAL	55	55	55							
Percentage of HHS IT systems protected with advanced Internet content filtering and anti-malware solutions.	Quarterly	Output	Percent	TARGET	60	60	60	60	60	85	85	85	95	95
				ACTUAL	60	60	60							
Percentage of HHS critical IT systems audit logs analyzed by the CSIRC and OPDIV staffs for intrusions and security attacks	Quarterly	Outcome	Percent	TARGET	60	60	60	60	60	75	80	85	90	90
				ACTUAL	55	55	55							

Currently, the fourth measure, 'Percentage of HHS critical IT systems audit logs analyzed by the CSIRC and OPDIV staffs for intrusions and security attacks', is 5% behind target. This is due to a delayed support contract which has resulted in a delay in acquiring the necessary staff to analyze the audit logs. The HHS IT Security program is working with the Program Support Center (PSC) to ensure the support contract begins as soon as possible, and by Q4 FY 2010. 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/Evaluation

All Recovery Act programs are assessed for risk to ensure that appropriate internal controls are in place throughout the entire lifecycle of the program. These assessments are 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."

The risk management process fits within the overall governance structure established at HHS to address Recovery Act program risks. The HHS Risk Management and Financial Oversight Board provides executive leadership and establishes accountability for the risk assessment process related to internal controls over financial reporting, and the HHS Senior Assessment Team ensures that risk assessment objectives are clearly communicated throughout the Department. The OCIO Senior Assessment Team carries out comprehensive annual assessments of its Recovery Act program(s) to identify risks and develop strategies to address them, including those associated with selecting recipients, awarding and overseeing funds, and achieving program goals. It meets monthly to monitor and assess the effectiveness of mitigation strategies and identify emerging risks.

In addition, the CISO has presented its high level risks to the Recovery Act Implementation Team. Chaired by the Deputy Secretary and comprised of senior policy officials from throughout the Department, the Implementation Team convenes monthly to monitor progress in carrying out Recovery Act programs and address the obstacles and risks that could impact on their success.

Internal HHS investment review boards, the HHS Recovery Act Oversight Committee, and the HHS Office of the Chief Information Officer (OCIO) staff under the Assistant Secretary for Administration 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 OCIO will provide oversight and management for the spend plan. Each OPDIV will also be responsible to OCIO for carrying out activities, for providing funds control, and satisfying Recovery Act reporting requirements.

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

I. Transparency

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

HHS ensures that recipient reports required by Section 1512 of the Recovery Act are submitted and reviewed for material omissions and significant errors that would mislead or confuse the public. HHS informs recipients of their reporting obligation through

standard terms and conditions, grant announcements, contract solicitations, and other program guidance. In addition, HHS provides key award information to recipients and other technical assistance to grantees and contractors and fully utilizes 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 has built upon and strengthened existing processes. Senior IT security program officials 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 also incorporates 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, which result in part from the level of effort required in developing approved statements of work and acquisition plans. For instance, the request for proposal (RFP) process 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 are also increased by the large volume of Recovery Act contracts that need to be set in place across the federal government, and overburdened contracting offices (e.g., PSC, NIH etc).

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 OCIO will follow a centralized reporting and evaluation model for the spend plan investments. Each OPDIV will be responsible to OCIO for carrying out activities, for providing funds control, and satisfying Recovery Act reporting requirements. The OCIO will conduct program reviews for each initiative, and will require formal OPDIV reporting to account for Recovery Act funds expenditures.

L. Federal Infrastructure Investments

For all IT security initiatives, HHS will comply with E.O. 13423 and E.O. 13514 regarding the purchase of energy efficient hardware and related equipment and products and the operation of Data Centers. 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. HHS is developing implementation plans to meet technology energy consumption goals in its data center operations.

Summary of Significant Changes:

- The funding table now reflects actual obligations for FY 2009 and an updated estimate for FY2010 obligations. The program is still on target to obligate all funds by the end of FY10.
- The Activities section is organized using four initiatives, which streamline the original five from the original plan. The initiatives reorganize program activities in a more logical and efficient manner.
- The Characteristics section is reorganized based on OPDIV obligations, rather than initiatives. This better reflects how the program is managed via Intra Departmental Delegations of Authority (IDDAs) and how obligations are tracked.
- The Delivery Schedule, which is organized by initiative, is updated based on actual obligations and projections for the remainder of the fiscal year.
- The number of performance measures was streamlined from five to four. The Measures section now includes target and actual metrics for each measure.