



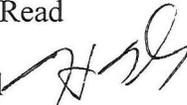
United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

AUG 11 2011

MEMORANDUM

TO: A/LM/AQM – Cathy J. Read

FROM: OIG – Harold W. Geisel 

SUBJECT: Report on *Audit of the Department of State Tools To Guard Against and Track Cyber Attacks Program Funded by the American Recovery and Reinvestment Act*

The subject report is attached for your review and action. As the action office for the report's one recommendation, please provide your response to the report and information on actions taken or planned for the recommendation within 30 days of the date of this memorandum. Actions taken or planned are subject to follow-up and reporting in accordance with the attached compliance response information.

The Office of Inspector General (OIG) incorporated your comments as appropriate within the body of the report and included them in their entirety as Appendix C.

OIG appreciates the cooperation and assistance provided by your staff during this audit. If you have any questions, please contact Evelyn R. Klemstine, Assistant Inspector General for Audits, at (202) 663-0372 or Richard Astor, Division Director, at (703) 284-2601 or by email at astorr@state.gov.

Attachment: As stated.

cc: INR/EX/B&F – (b) (6) 
M/PRI – (b) (6) 
IRM/BMP/SPO/SPD – (b) (6) 

UNCLASSIFIED

**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Office of Audits

**Audit of the
Department of State
Tools To Guard Against and Track
Cyber Attacks Program
Funded by the
American Recovery and Reinvestment Act**

**AUD/CG-11-38
August 2011**

~~Important Notice~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. § 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

UNCLASSIFIED



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report is being transmitted pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

This report addresses the Department of State's (Department) compliance with Federal, Department, and American Recovery and Reinvestment Act of 2009 (Recovery Act) acquisition management practices as related to the Department's Tools To Guard Against and Track Cyber Attacks program. The report is based on interviews with Department employees and officials, direct observation, and a review of applicable documents.

OIG contracted with the independent public accountant Clarke Leiper, PLLC, to perform this audit. The contract required that Clarke Leiper perform its audit in accordance with guidance contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. Clarke Leiper's report is included.

Clarke Leiper identified three areas in which improvements could be made: transparency of award notifications posted on the Federal Business Opportunities Web site (FedBizOpps.gov), compliance with certain requirements established by the Office of Management and Budget, and accuracy of reporting by award recipients.

OIG evaluated the nature, extent, and timing of Clarke Leiper's work; monitored progress throughout the audit; reviewed Clarke Leiper's supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with Clarke Leiper's findings. The recommendation contained in the report was developed on the basis of the best knowledge available and was discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendation has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of the individuals who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel", written in a cursive style.

Harold W. Geisel
Deputy Inspector General

UNCLASSIFIED

CLARKE LEIPER PLLC

CERTIFIED PUBLIC ACCOUNTANTS

6265 FRANCONIA ROAD

ALEXANDRIA, VA 22310-2510

703-922-7622

FAX: 703-922-8256

DORA M. CLARKE
LESLIE A. LEIPER

Audit of Department of State Tools To Guard Against and Track Cyber Attacks Program Funded by the American Recovery and Reinvestment Act

Office of Inspector General
U.S. Department of State
Washington, D.C.

Clarke Leiper, PLLC (referred to as “we” in this letter), has performed an audit of the Department of State’s (Department) Tools To Guard Against and Track Cyber Attacks program funded by the American Recovery and Reinvestment Act of 2009 (Recovery Act). We evaluated the program’s planned activities, contracts awarded with Recovery Act funds, and compliance with reporting requirements established by the Recovery Act. This performance audit, performed under Contract No. SAQMPD04D0033, was designed to meet the objective in the report section titled “Objective” and further defined in Appendix A, “Scope and Methodology,” of the report.

We conducted this performance audit from April through November 2010 in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our performance audit and the related findings and recommendation to the Department of State Office of Inspector General.

We appreciate the cooperation provided by personnel in Department offices during the audit.

Clarke Leiper PLLC

Clarke Leiper, PLLC
July 2011

UNCLASSIFIED

Acronyms

Cyber Attacks program	Tools To Guard Against and Track Cyber Attacks program
Department	Department of State
DS	Bureau of Diplomatic Security
FAR	<i>Federal Acquisition Regulation</i>
FedBizOpps.gov	Federal Business Opportunities Web site
FPDS.gov	Federal Procurement Data System Web site
GFMS	Global Financial Management System
INR	Bureau of Intelligence and Research
IRM	Bureau of Information Resource Management
IRM/EA	Office of Enterprise Architecture
IRM/ENM	Office of Enterprise Network Management
IRM/IA	Office of Information Assurance
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
Recovery Act	American Recovery and Reinvestment Act of 2009
TAS	Treasury Account Symbol
VOIP	Voice Over Internet Protocol

UNCLASSIFIED

TABLE OF CONTENTS

Executive Summary 1

Background 2

Objective 3

Results of Audit 3

 A. Program Objectives Are Being Accomplished 4

 B. Program Is Generally in Compliance With Recovery Act Requirements 6

Appendices

 A. Scope and Methodology 10

 B. Capital Investment Fund 13

 C. Bureau of Administration Response 14

UNCLASSIFIED

Executive Summary

The American Recovery and Reinvestment Act of 2009 (Recovery Act)¹ provided approximately \$64.2 million to fund the Tools To Guard Against and Track Cyber Attacks (Cyber Attacks) program to produce a more secure information technology (IT) infrastructure to protect the Department of State's (Department) physical and logical information and assets. By implementing a state-of-the-art secure IT infrastructure, the Department will enhance its ability to execute its diplomatic mission, serve the U.S. public, and strengthen its infrastructure from cyber security threats.

The objective of our audit was to determine whether the Department adequately implemented Cyber Attacks program plans, achieved stated program outcomes, and complied with the reporting requirements of the Recovery Act.

We found that program managers in the Bureaus of Information Resource Management (IRM), Diplomatic Security (DS), and Intelligence and Research (INR) have planned for and integrated the Cyber Attacks program into the Department's existing cyber security initiatives. Because the objectives of the Cyber Attacks program are part of an already existing IT Strategic Plan, much of the initial planning has already been approved. The plan includes appropriate focus on accountability and other requirements of Recovery Act funds. In addition, the Department's plans were thorough and well thought out. There were no deviations or major delays in execution of the plan.

The Department has taken appropriate actions in establishing guidelines intended to ensure compliance with Office of Management and Budget (OMB) requirements for the Recovery Act. Contracts were awarded in accordance with the *Federal Acquisition Regulation* (FAR) and OMB memoranda.² Procedures related to data transparency and reporting requirements were established and implemented. While procedures related to data transparency and reporting requirements were established and implemented, a few minor issues of noncompliance were identified for the Cyber Attacks program. Recovery Act transparency requirements identifying the purpose, nature, and corresponding program for contract awards were not met prior to posting or publicizing information. Also, some Recovery Act award information was not reported accurately.

We recommended that the Bureau of Administration, Office of Logistics Management, Office of Acquisitions Management (A/LM/AQM), enhance its contract oversight efforts to ensure more complete and accurate reporting of award information.

In its response to the draft report (see Appendix C), AQM concurred with the recommendation. Based on the response, OIG considers the recommendation resolved, and it

¹ Pub. L. No. 111-5, 123 stat. 115 (2009).

² Memoranda M-09-10, *Initial Implementing Guidance for the American Recovery and Reinvestment Act of 2009*, and M-09-15, *Updated Implementing Guidance for the American Recovery and Reinvestment Act of 2009*.

UNCLASSIFIED

will be closed pending review and acceptance of documentation for the actions OIG specified. The response and OIG’s analysis are presented after the recommendation.

Background

The American Recovery and Reinvestment Act of 2009 was signed into law as a direct response to the recent economic crisis in an effort to jumpstart the economy and invest in long-term growth by creating or saving jobs and putting a down payment on addressing long-neglected challenges. The Department received \$602 million of Recovery Act funds to create and save jobs, repair and modernize domestic infrastructure crucial to the safety of American citizens, enhance energy independence, and expand consular services offered to American taxpayers. The Recovery Act also established an unprecedented level of accountability and transparency in U.S. Government spending. Agencies and contractors were subject to new reporting requirements set forth by OMB that allow the general public to view Recovery Act spending in a direct and timely manner. A summary of the Department’s projects and a breakdown of proposed spending of funds are shown in Table 1.

Table 1. Department Projects and Proposed Spending of Recovery Act Funds

Department of State – Account / Project	Funds (in 000s)
Diplomatic and Consular Programs	\$90,000
- Hard Skills Training Center	70,000
- Consular Affairs Passport Facilities	15,000
- National Foreign Affairs Training Center	5,000
Capital Investment Fund	\$290,000
- Data Center	120,000
- IT Platform	33,500
Diplomatic Facility Telephone System Replacement	10,000
Replacement of Aging Desktop Computers	13,000
Mobile Computing	10,500
- Cyber Security	98,500
Tools To Guard Against and Track Cyber Attacks	64,205
Strengthen Computer Hardware Security Testing and Forensic Investigations	4,000
Safeguarding Citizens – Computer Security Systems	25,366
Expanded Cyber Education	4,929
- Transfer to U.S. Agency for International Development	38,000
Office of Inspector General	\$ 2,000
International Boundary and Water Commission Construction	\$ 220,000
TOTAL	\$ 602,000

Source: Department of State.

The nature of the Department’s mission makes it a target for cyber terrorists and hackers. The Department serves the American public through the execution of its diplomatic mission and the issuance of passports and visas to American citizens and foreign guests. A secure and modern IT infrastructure is essential to the execution of those duties. Of the total \$602 million in

UNCLASSIFIED

Recovery Act funds provided to the Department, funds of approximately \$64.2 million are designated to the Cyber Attacks program to produce a more secure IT infrastructure to protect the Department's physical and logical information and assets. By implementing a state-of-the-art secure IT infrastructure, the Department will both enhance its ability to execute its diplomatic mission and serve the U.S. public and strengthen its infrastructure from cyber security threats.

The objectives of the Cyber Attacks program are key components of an existing cyber security initiative that is part of the Department's long-term IT Strategic Plan. The Recovery Act funds provided the Department the opportunity to supplement its existing efforts to accomplish some of the key objectives of the cyber security initiative. These objectives are as follows:

- Produce a more secure infrastructure that protects the IT assets of the Department and maintains the capability to expand support to its partners in the U.S. foreign affairs community.
- Expand the capability to monitor, guard against, track, and respond to cyber attacks.
- Enhance the protection of personally identifiable information of U.S. citizens receiving services from the Department.
- Modernize, standardize, and centralize the Department's domestic IT network.
- Fully integrate the Department's domestic and overseas IT networks through reengineering, standardization, and deployment of a world-class, enterprise-wide network and network security architecture.
- Provide technological improvements to, and enhance security for, the Department's mobile computing platform.

Objective

The objective of our audit was to determine whether the Department adequately implemented Cyber Attacks program plans, achieved stated program outcomes, and complied with the reporting requirements of the Recovery Act.

Results of Audit

The Department has made progress in accomplishing Cyber Attacks program objectives and milestones. The success of the Cyber Attacks program was the result of collaboration among IRM, DS, and INR personnel, as well as other Department personnel and contractor staff. The bureaus planned and integrated the Cyber Attacks program into the Department's existing cyber security initiative.

As of September 30, 2010, almost 100 percent of the \$64.2 million in program funds had been obligated, and about half of the funds had been expended for contracts to support six major subprojects: Hardening Department of State Infrastructure and Improved Defensive Sensors; Security Architecture, Support, and Oversight; Data Loss Prevention; Improved Defensive Sensors, Hardening Infrastructure and Classified Systems Assessments; Sensitive

UNCLASSIFIED

Compartmented Information Network Security; and Mobile Communications, Voice Over Internet Protocol (VOIP), Web Development, and Network Enhancements.

Overall, IRM program managers have complied with management and financial oversight requirements of OMB. Also, funds were awarded and distributed in a prompt, fair, and reasonable manner. However, we noted several areas in which Recovery Act procedures were not followed and contract data was not reported accurately.

Finding A. Program Objectives Are Being Accomplished

Based on our inquiries of project management, review of supporting documentation, and tests for propriety of contract obligation and expenditure transactions, we determined that satisfactory progress is being made on meeting program objectives. Recovery Act funds are appropriately accounted for and being used in accordance with approved program plans. The objectives of the Cyber Attacks program do not encompass complete and discrete plans for the Department's existing cyber security initiative and IT Strategic Plan. These Recovery Act-funded activities are only partial components of broader Department plans. Therefore, the Cyber Attacks program is meant primarily to supplement the Department's current efforts by funding certain activities within those plans. We found no significant delays or funding issues in the Cyber Attacks program with regard to activities funded by the Recovery Act. To complete all components of the cyber security initiative as they relate to the Cyber Attacks program, additional funding and resources will be required in FY 2011 and beyond. IRM officials project that operation and maintenance costs to operate and manage the new infrastructure will be about \$300,000 each year. This additional cost will cover the increased maintenance requirements. When cyber security projects are completed with a secure infrastructure serving all foreign affairs agencies, IRM officials stated that they believe they will realize savings because standard, more secure systems and networks are less expensive to operate.

The Cyber Attacks program has resulted in collaboration among personnel of several Department bureaus, as well as Department personnel and contractor staff. The overall responsibility and accountability of the program were managed by IRM's Office of Enterprise Network Management (ENM). IRM's Offices of Enterprise Architecture (EA) and Information Assurance (IA) are also involved in the Cyber Attacks program. DS and INR supported IRM and were responsible for designated parts of the program. These bureaus provided IRM with weekly updates for consolidated reporting purposes. The Cyber Attacks program comprises six subprojects. The subprojects and respective responsible bureaus are shown in Table 2, and major contracts are in Table 3.

UNCLASSIFIED

Table 2. Cyber Attacks Program Subprojects and Responsible Bureaus

Subprojects – Tools To Guard Against and Track Cyber Attacks		Bureau	Obligated	Expended
1	Hardening Department Infrastructure and Improved Defensive Sensors <i>a. Network Access Controls & Perimeter Security</i> <i>b. End-to-End Configuration Management</i> <i>c. Centralized Patch Management</i> <i>d. Domestic Network Modernization</i>	IRM	\$ 39,713,695.55	\$ 18,398,856.68
2	Security Architecture, Support, and Oversight	IRM	5,404,679.51	3,107,444.62
3	Data Loss Prevention	IRM	4,297,218.60	1,988,797.14
4	Improved Defensive Sensors, Hardening Infrastructure, Classified Systems Assessments	DS	6,754,501.33	4,532,709.22
5	Sensitive Compartmented Information Network Security	DS	2,260,497.04	1,092,647.17
6	Mobile Communications, VOIP, Web Development, Network Enhancements	INR	5,773,226.73	3,130,396.04
TOTAL			\$ 64,203,818.76	\$ 32,250,850.87

Source: Department of State.

Table 3. Cyber Attacks Program Major Contracts

	Award #	Vendor	Awarded	Services
1	SAQMPD07F0777	Northrop Grumman Information Technology, Inc.	\$20,898,670.20	Labor contract for project management and implementation of Functional Task 8, which encompasses IRM/ENM initiative for Hardening Infrastructure and Improving Defensive Sensors.
2	SAQMMA09L0369	Allied Technology Group, Inc.	\$1,836,196.92	Acquire services to support the Chief Information Officer's planning organization in the IT Capital Planning and Investment Control and Infrastructure Optimization Initiative Line of Business processes for the Department, and support the Department in tracking and evaluating current and emergent technologies.
2	SAQMMA09L0943	Deloitte Consulting LLP	\$2,599,953.19	Acquire services to document, evaluate, and develop architecture and transition strategy.
2	SAQMMA10F0997	W I N S	\$228,019.20	Acquire services for enterprise-wide software monitoring and testing.
3	SAQMMA09L0757	SRA	\$173,157.04	Develop new privacy policies related to the Data Loss Prevention program.
3	SAQMMA10L0391	Booz Allen Hamilton Inc.	\$162,199.52	Acquire program management, enterprise risk, and data analysis services to support IRM/IA's collaborative Data Loss Prevention initiative.

UNCLASSIFIED

3	SAQMMA10L1038	Booz Allen Hamilton Inc.	\$2,880,476.95	Network Continuous Certification and Accreditation Support Services. Initiation and development of a new continuous certification and accreditation process to increase the use of automation and monitoring in certification and accreditation activities.
4	SAQMMA08L3182	SRA	\$4,374,806.47	IT infrastructure security support and program management.
5	SAQMMA08L1558	Mantech Information Systems	\$2,238,113.35	Evaluate existing systems and processes related to network security.
6	SAQMMA09F2886	W I N S	\$239,986.18	VOIP engineer to design/implement VOIP infrastructure.
6	SAQMMA09F3054	W I N S	\$864,122.20	Systems engineers for network enhancements/ modernization.
6	SAQMMA09F3062	W I N S	\$749,163.20	Web site developers.

Source: Department of State.

Finding B. Program Is Generally in Compliance With Recovery Act Requirements

IRM program managers adequately planned for and managed the funds provided for the Cyber Attacks program. Recovery Act funds were used for their intended purposes, and overall, the Department complied with OMB requirements. We found funds were awarded and distributed in a prompt, fair, and reasonable manner. Contractors and other fund recipients met eligibility requirements and complied with award requirements. For example, fixed-price contracts were awarded to American companies for hardware, software, and circuits in support of American high-technology companies. As required by the Recovery Act, separate Treasury Account Symbols (TAS) were established for the Cyber Attacks program. As reported through the Department’s Capital Investment Fund, we verified that program funds had proper approvals and that the monitoring of subprojects and contracts was adequate, as shown in Appendix B, “Capital Investment Fund.” We noted, however, some minor instances in which Recovery Act procedures were not followed and contract data was not reported accurately.

Notifications on the Federal Business Opportunities Web Site

For the 25 contracts reviewed, we found that the majority of the FedBizOpps.gov notifications did not provide adequate transparency or a clear understanding to the general public of the purpose, nature, and corresponding program of the procurements. The Department has publicized both its program plans and its contracts awarded with Recovery Act funds. However, 19 award notifications did not reference specific program plans or objectives, making it difficult to determine which awards were made pursuant to the Department’s Recovery Act programs. In addition, 17 award notifications did not include descriptions of the products or services that could be readily understood by the general public.

UNCLASSIFIED

In that regard, OMB Memorandum M-09-15³ states:

Agencies should ensure that their descriptions of procurements use language appropriate for a more general audience, avoiding industry-specific terms and acronyms without plain language explanations. Taxpayers, the media, and others are using our business systems to gain insight on how Recovery Act funds are being spent.

Transparency and accountability of Recovery Act funds are major requirements of the act. However, almost all program funds have been obligated. Therefore, we are not making any recommendations for IRM to improve transparency for future procurements notifications reported through FedBizOpps.gov. Nevertheless, this deficiency prevented the general public from being able to identify procurements made pursuant to the Cyber Attacks program, since descriptions within award notifications did not contain references or mention corresponding programs.

Recipient-Reported Data on Award Information

For the quarterly reporting period ended June 30, 2010, we identified the following awards in which recipient-reported data did not agree with source documentation:

- Recovery Act funds of \$14,366,103 awarded prior to the quarter ended June 30, 2010, were not reported by recipients. This amount was based on four different awards. The majority of this amount, \$12,148,674, was attributable to a modification of an existing award that was not reported by a recipient as of the end of the reporting period.
- For one award, duplicate reporting of a modification of \$149,803 was included within the contractor's report.

The FAR⁴ establishes reporting requirements for contractors receiving awards funded by the Recovery Act. The information to be reported includes data such as cumulative amounts awarded, cumulative amounts spent, descriptions of goods and services, assessment of contractor progress toward completion, and any subcontracting activity. Contractors receiving awards under the Recovery Act are required to report quarterly on award information and activities using the online reporting Web site FederalReporting.gov. This information is then uploaded from FederalReporting.gov to the Recovery.gov Web site for publicizing to the general public. Department personnel are required to review recipient-reported information every quarter to ensure consistency with Department records. Therefore, as noted, recipient-reported data for the Cyber Attacks program showed \$14,366,102 as underreported and \$149,803 as overreported.

Recommendation 1. We recommend that the Bureau of Administration's Office of Logistics Management, Office of Acquisitions Management, ensure that contractors that

³ OMB Memorandum M-09-15, pt. 6.2., p. 57 (April 3, 2009).

⁴ FAR 52.204-11, "American Recovery and Reinvestment Act-Reporting Requirements." (March 2009)

UNCLASSIFIED

received awards from the American Recovery and Reinvestment Act for the Tools To Guard Against and Track Cyber Attacks program provide accurate award information and that the inaccurate award information identified in this report is corrected.

Management Response: AQM concurred with the recommendation, stating that the bureau will research reported inaccuracies and provide OIG with an action plan to resolve any discrepancies.

OIG Analysis: On the basis of the response, OIG considers the recommendation resolved. OIG will consider the recommendation closed pending review and acceptance of AQM's action plan.

Instances of Noncompliance With Certain Office of Management and Budget Requirements

IRM generally followed OMB requirements for contracts supporting the Cyber Attacks program. However, we identified instances of agency noncompliance with OMB Memorandum M-09-15 concerning performance requirements in awarding contracts to contractors. Specifically, for the 25 contracts reviewed, we noted the following instances of noncompliance:

- The clause in the FAR (FAR 52.204-11)⁵ that specifies recipient reporting requirements was not included in the award documents for one award.
- Pre-solicitation and award notifications were not published on FedBizOpps.gov for three awards. According to the FAR,⁶ agencies should publish both pre-solicitation and award notifications on FedBizOpps.gov for the procurement of all goods and services using Recovery Act funds.
- On the Federal Procurement Data System Web site (FPDS.gov), five awards were not identified as Recovery Act initiatives. According to the FAR,⁷ in addition to publicizing contract and award actions on FPDS.gov, agencies should identify any action funded in whole or in part by the Recovery Act in accordance with the instruction at <https://www.fpds.gov>.
- One contract had been awarded on a noncompetitive basis, which was not disclosed in the special reporting section on the Web site Recovery.gov. The FAR⁸ requires awards that are made on a noncompetitive and/or a non-fixed-price basis to be disclosed in a special reporting section on Recovery.gov.

⁵ Ibid.

⁶ FAR 5.704, "Publicizing Pre-award," and FAR 5.705, "Publicizing Post-award," respectively.

⁷ FAR 4.605, "Contract Reporting - Procedures."

⁸ FAR 5.705(b).

UNCLASSIFIED

Since almost all program funds have been obligated and the noncompliance instances cited are primarily isolated, we are not making any recommendations in this area.

Scope and Methodology

The Department of State (Department), Office of Inspector General (OIG), contracted with Clarke Leiper, PLLC, independent public accountant, to audit the Department's Tools To Guard Against and Track Cyber Attacks (Cyber Attacks) program.

The purpose of this audit was to evaluate the Cyber Attacks program and assess the Department's planning and use of funds from the American Recovery and Reinvestment Act of 2009 (Recovery Act) to meet program objectives, to ensure that Recovery Act funds were used for their intended purpose, and to determine whether the Department complied with Office of Management and Budget requirements. To ensure the adequacy of program plans and to ensure that the Department used Recovery Act funds appropriately, we performed audit procedures to determine whether

- Funds were awarded and distributed in a prompt, fair, and reasonable manner.
- Recipients and uses of all funds were transparent to the public and the public benefits of the funds were reported clearly and accurately and in a timely manner.
- Risks associated with the project receiving Recovery Act funding have been identified and communicated to the Department.
- Funds were used for authorized purposes.
- The program has taken action to identify and mitigate instances of fraud, waste, error, and abuse.
- Established schedules were monitored and delays were properly justified.
- Cost overruns and unnecessary delays were avoided and lessons learned were identified to prevent recurrences.
- Program goals were achieved and specific program outcomes were realized.
- Contractors and other fund recipients met eligibility requirements and complied with award requirements.
- Adequate planning was conducted for potential future project phases.

We conducted the audit work from April through October 2010. This work was conducted in accordance with generally accepted government auditing standards. Those standards require that the auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We and OIG believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

In our audit of the Department's Cyber Attacks program, we interviewed project managers and officials at the Bureaus of Information Resource Management, Diplomatic Security, and Intelligence and Research and evaluated documentation supporting planned activities and milestones, risk assessments, and other relevant documents in support of major accomplishments or decisions. For compliance with Recovery Act requirements, we reviewed

UNCLASSIFIED

contract files, award documentation, and information published on the Web sites Recovery.gov, FPDS.gov, and FedBizOpps.gov. In determining the proper use of Recovery Act funds, we tested sample transactions and reviewed related source documents, including purchase orders, contracts, vendor invoices, and payment and approval vouchers.

In the draft report, we addressed the report's one recommendation to the Bureau of Information Resource Management (IRM). However, IRM officials suggested that the Bureau of Administration, Office of Logistics Management, Office of Acquisitions Management (A/LM/AQM), would be the more appropriate office to take action on this recommendation. Therefore, we redirected the recommendation in this final report to AQM, whose response is presented in Appendix C.

Work Related to Internal Controls

To assess the adequacy of internal controls related to the weekly activity reports, the accountability of Recovery Act funds, and the monitoring of projects to avoid cost overruns and delays, we performed the following actions:

- Obtained an understanding of the processes and procedures.
- Reviewed source documentation and other types of evidence in order to confirm the adequacy of stated controls.
- Compared weekly report balances with details and reconciled differences in the Global Financial Management System (GFMS).
- Reviewed internal reports related to the compilation of balances and amounts for reporting to the public.
- Compared reported progress with information in the planning documents and progress schedules.
- Determined that separate Treasury Account Symbols were established for Recovery Act programs.
- Verified proper approval over transactions involving Recovery Act funds.
- Discussed with program managers issues regarding cost overruns and delays and subsequently compared responses with expenditure details and program schedules to assess the reasonableness of responses.

Data Reliability

We selected a sample and performed the following procedures in assessing data reliability and quality:

- Reviewed contract files to determine whether contracts were competitively awarded and at fixed cost.
- Tested, if a contract was determined to have been awarded noncompetitively or at a non-fixed cost, whether those contracts were disclosed and listed in a separate section on Recovery.gov.

UNCLASSIFIED

- Reviewed, for each contract, corresponding notifications and award information published on FedBizOpps.gov and FPDS.gov to determine whether all required Recovery Act disclosures and identifying information were reported.
- Reviewed, for each contract, the vendors' reported data from Recovery.gov to ensure that all required information was included. We also compared vendor-reported amounts with those within GFMS.
- Compared weekly financial report balances with underlying schedules and GFMS details.

Use of Computer-Processed Data

We used computer-processed data from GFMS to select sample items for testing contracts and obligation and/or expenditure transactions. We also used GFMS details and reconciling schedules to compare the accuracy of balances reported within the Recovery Act weekly financial reports posted by the Department. We determined that the GFMS data and schedules were reliable based on our selected sample and our testing of internal controls involving the weekly reporting process.

Capital Investment Fund

Funding from the Recovery and Reinvestment Act of 2009 (Recovery Act) for the Department of State (Department) is allocated among four separate Treasury Account Symbols (TAS), or funds. These funds were created to comply with the Recovery Act requirement of tracking and accounting for Recovery Act funds separately from other agency funds. All TASs and related activities are included within the Department’s weekly financial reports. The Department obligated nearly 100 percent of the amount available for the Tools to Guard Against and Track Cyber Attacks program.

The Department’s Capital Investment Fund (TAS 1119) is broken down into three sections—the data center, cyber security, and IT platform initiatives, as shown in Table 1. The Cyber Attacks program is tracked and recorded under the cyber security portion of the fund (TAS 1119.0002), as shown in Table 2.

Table 1. Department of State Capital Investment Fund

Department of State – Capital Investment Fund (TAS 1119)	Fund Code	Planned Budgeted	Actual Obligations
- Data Center	1119.0001	120,000,000	119,972,941
- Cyber Security	1119.0002	98,500,000	98,502,834
- IT Platform	1119.0003	33,500,000	33,499,148
Transfer to U.S. Agency for International Development (USAID)	-	38,000,000	38,000,000
TOTAL		\$ 290,000,000	\$ 289,974,923

Source: Department of State.

Table 2. Cyber Security Portion of Capital Investment Fund

Cyber Security (TAS 1119.0002)	Planned	Obligations as of 9-30-2010
Tools To Guard Against and Track Cyber Attacks	\$64,205,000	\$ 64,203,789
Strengthen Computer Hardware Security Testing and Forensic Investigations	4,000,000	3,998,790
Safeguarding Citizens – Computer Security Systems	25,366,000	25,365,911
Expanded Cyber Education	4,929,000	4,934,344
TOTAL	\$ 98,500,000	\$ 98,502,834

Source: Department of State.



United States Department of State

Washington, D.C. 20520

July 19, 2011

UNCLASSIFIED
MEMORANDUM

TO: OIG/AUD – Mark Taylor

FROM: Cathy Read  A/LM/AQM

SUBJECT: Draft Report on Audit of the Department of State Tools To Guard Against and Track Cyber Attacks Program Funded by the American Recovery and Reinvestment Act

Recommendation 1: We recommend that the Bureau of Information Resource Management, Office of Enterprise Network Management, ensure that contractors that received awards from the American Recovery and Reinvestment Act for the **Tools To Guard Against and Track Cyber Attacks program** provide accurate award information and that the inaccurate award information identified in this report be corrected.

A/LM/AQM response:

A/LM/AQM will work with the OIG regarding the identified contracts/task orders and will research each reported inaccuracy. Once all procurement-related actions have been researched and verified, A/LM/AQM will provide OIG with an action plan to resolve any discrepancies.

UNCLASSIFIED

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
<http://oig.state.gov>

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.