



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 Department of State Safeguarding Citizens – Computer Security Systems 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
Safeguarding Citizens –
Computer Security Systems Program
Funded by the
American Recovery and Reinvestment Act**

AUD/CG-11-36

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 (Recovery Act) acquisition management practices as related to the Department's Safeguarding Citizens – Computer Security Systems 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 Web site FedBizOpps, 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, and the recommendations contained in the report were developed on the basis of the best knowledge available and were discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations 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. 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 the Department of State Safeguarding Citizens – Computer Security Systems 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 (Department) Safeguarding Citizens – Computer Security Systems program funded by the American Recovery and Reinvestment Act (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 identified in the report section titled “Objective” and further defined in Appendix A, “Scope and Methodology,” of this report.

We conducted this performance audit from April through October 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 recommendations to the U.S. Department of State Office of Inspector General.

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



Clarke Leiper, PLLC
July 2011

UNCLASSIFIED

UNCLASSIFIED

ACRONYMS

A/LM/AQM	Bureau of Administration, Office of Logistics Management, Office of Acquisitions Management
Department	Department of State
DS	Bureau of Diplomatic Security
FAR	Federal Acquisition Regulation
FBO	Federal Business Opportunities (FedBizOpps)
FPDS	Federal Procurement Data System
GFMS	Global Financial Management System
IRM	Bureau of Information Resource Management
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

UNCLASSIFIED

TABLE OF CONTENTS

Executive Summary1

Background.....2

Objective3

Results of Audit3

 A. Program Objectives Are Being Accomplished4

 B. Program Is Generally in Compliance With Recovery Act Requirements5

Appendices

 A. Scope and Methodology7

 B. Capital Investment Fund.....10

 C. Bureau of Administration Response11

UNCLASSIFIED

Executive Summary

The American Recovery and Reinvestment Act of 2009 (Recovery Act)¹ provided approximately \$25.4 million to fund the Safeguarding Citizens – Computer Security Systems (Safeguarding Citizens) program to deploy state-of-the-art computer security systems to the Department of State (Department) headquarters building and embassies worldwide.

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

We found that program managers in the Bureau of Information Resource Management (IRM) have planned for and integrated the Safeguarding Citizens program into the Department's existing information technology (IT) initiatives. Because the objectives of the Safeguarding Citizens 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, we determined that the Department's plans were thorough and well thought out. Delays in scheduled progress have been justified and were considered to be reasonable.

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 instances of noncompliance were identified for the program. Recovery Act transparency requirements identifying the purpose, nature, and corresponding program for contract awards were not met prior to the awards being posted or publicized. 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 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.

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

² Memorandums 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

Background

The Recovery Act 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 downpayment on addressing long-neglected challenges. The Department was provided \$602 million in 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 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. The Department's projects and a breakdown of proposed spending of Recovery Act funds are summarized in Table 1.

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

Department of State – Account / Project	Funds (in 000s)
Diplomatic & 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 (GITM)	13,000
Mobile Computing	10,500
- Cyber Security	98,500
Tools to Guard Against & Track Cyber Attacks	64,205
Strengthen Computer H/W Security Testing & Forensic Investigations	4,000
Safeguarding Citizens – Computer Security Systems	\$25,366
Expanded Cyber Education	4,929
Transfer to U.S. Agency for International Development (USAID)	38,000
Office of Inspector General	\$2,000
International Boundary and Water Commission Construction	\$ 220,000
TOTAL	\$ 602,000

Source: Department of State.

Of the total \$602 million the Department received in Recovery Act funds, \$25,366,000 was designated for the Safeguarding Citizens program. This program involves deploying state-of-the-art computer security systems to the Department headquarters building and at U.S. Embassies worldwide.

The Department of State's unique relationships with the Departments of Homeland Security, Justice, and Defense and with private-sector partners make the Department of State's information a major target of hostile intelligence services and terrorist organizations. This threat to the Department's information systems must be addressed to protect American interests and

UNCLASSIFIED

citizens both domestic and overseas. The critical systems that process passports and visas, support foreign policy negotiations, and synchronize U.S. evacuations are under constant attack. The Department requires cutting-edge security solutions that incorporate comprehensive and modern protections to enhance National security and address the challenges of constantly changing cyber threats. To address these issues, the Safeguarding Citizens program has three main projects:

1. Public Key Infrastructure (PKI – Smart ID badges) – This program allows all domestic Department employees and contractors to gain physical access to Department facilities and logical access to information systems through the issuance of a single Smart identification (ID) badge, which is in contrast to the current “two-card” system. Recovery Act funds will be used to assist current Department efforts in procuring and implementing these Smart cards and card readers.
2. Secure Voice Phones (SV) –The Department’s current secure telephones use technologies that were developed in the late 1980s and 1990s. The end of life of this Government-developed system and the change of the global telephone infrastructure to Voice over Internet Protocol (VoIP) are making the current telephones unreliable and encouraging the Department to accelerate its migration to the next generation telephone, which uses VoIP technologies. Recovery Act funds will be used to supplement current Department efforts by funding the procurement of secure telephones.
3. Anti-Virus (AV) – The AV Program implements and manages Department-wide countermeasures to stop malicious code, such as computer viruses, SPAM, adware, phishing, spyware, and other cyber threats. Recovery Act funds will be used to extend current anti-virus capabilities to allow for the following centrally managed and configured processes:
 - a. Prevent the use of any unauthorized devices (for example, USB thumb drives) on any system within the Department while allowing authorized devices to be used at any location enterprise-wide.
 - b. Prevent unauthorized software from running or log, based on security requirements of the system, attempts to run unauthorized software.
 - c. Prevent any system not meeting current security profiles (such as patch status) from connecting to the network and offer remedial action options for network control centers.

Objective

The objective of our audit was to determine whether the Department adequately implemented Safeguarding Citizens 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 its Safeguarding Citizens program objectives and milestones. The success of the program was the result of collaboration between several Department bureaus and other Department personnel and contractor staff.

UNCLASSIFIED

As of September 30, 2010, almost 100 percent of the \$25,366,000 in program funds had been obligated for contracts to support three major subprojects: Public Key Infrastructure (PKI – Smart ID badges), Secure Voice Phones, and Anti-Virus Countermeasures.

Overall, program managers in IRM have complied with OMB management and financial oversight requirements. 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 Safeguarding Citizens program do not encompass complete and discrete plans for the Department’s existing Safeguarding Citizens and Information Technology (IT) Strategic Plan. These Recovery Act-funded activities are only partial components of broader Department plans. Therefore, the Safeguarding Citizens program is intended primarily to supplement the Department’s current efforts by funding certain activities within those plans. We found that the Safeguarding Citizens program did not experience any significant delays or funding issues with regard to those activities funded by the Recovery Act.

As of September 30, 2010, almost 100 percent of the \$25,366,000 in program funds had been obligated for contracts to support three major subprojects: Public Key Infrastructure (PKI – Smart ID badges), Secure Voice Phones, and Anti-Virus Countermeasures.

Major contracts awarded using Recovery Act funds under the Safeguarding Citizens program are shown in Table 2.

Table 2. Safeguarding Citizens Program Major Contracts Awarded

			(As of September 30, 2010)		
	VENDOR	AWARD NUMBER	OBLIGATIONS	EXPENDITURES	GOODS / SERVICES
PKI	Precise Biometrics	SAQMMA09C0175	\$5,875,000	\$5,875,000	Biometric readers and equipment
PKI	Siemens Govt Services	SAQMMPD05D1115	\$5,273,774	\$2,094,002	Installation of card readers for building access
PKI	Agtech, LLC	SAQMMA07F1066	\$3,967,527	\$1,474,551	Third-party independent support to conduct Federal PKI cross-certification audits
SV	National Security Agency	(Federal Vendor) Not an award	\$4,999,400	\$4,999,400	Procurement of 1,720 vIPer secure telephones
AV	Carahsoft Technology Group	SAQMMA10F2459	\$3,049,803	\$2,604,200	Anti-virus software and support
		TOTAL	\$23,165,504	\$17,047,153	

Source: Department of State.

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

IRM program managers adequately planned for and managed funds provided for the Safeguarding Citizens program. Recovery Act funds were used for their intended purposes, and overall, the Department complied with OMB requirements. Funds were awarded and distributed in a prompt, fair, and reasonable manner. Also, contractors and other fund recipients met eligibility requirements and complied with award requirements. For example, fixed-price contracts were made 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 Safeguarding Citizens 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 detailed in Appendix B, "Capital Investment Fund." We did note, 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 15 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, 12 award notifications did not reference specific program plans or objectives, which made it difficult to determine which awards were made with respect 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.

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, 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. Since almost all program funds have been obligated, however, we are not making any recommendations for IRM to take actions to improve transparency for future procurement notifications reported through FebBusOpps.gov. Nevertheless, this deficiency prevented the general public from having the ability to identify procurements made pursuant to the Safeguarding Citizens program, since descriptions within award notifications did not contain references or mention corresponding programs.

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

UNCLASSIFIED

Recommendation 1. We recommend that the Bureau of Administration, Office of Logistics Management, Office of Acquisitions Management, ensure, through more effective oversight of the quarterly review of recipient-reported data, that contractors that receive awards from the American Recovery and Reinvestment Act for the Safeguarding Citizens – Computer Security Systems 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 Safeguarding Citizens program. However, we identified minor instances of agency noncompliance with OMB Memorandum M-09-15⁴ concerning performance requirements in awarding contracts. Specifically, for the 15 contracts reviewed, we noted the following instances of noncompliance:

- The clause in the FAR (part 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 two awards. According to the FAR,⁶ agencies should publish both presolicitation and award notifications on FedBizOpps for the procurement of all goods and services using Recovery Act funds.
- On the Federal Procurement Data System Web site (FPDS.gov), one award was not identified as a Recovery Act initiative. According to the FAR,⁷ in addition to publicizing contract and award actions on FPDS.gov, agencies should label all awards that are Recovery Act related.

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.

⁴ Ibid.

⁵ FAR 52.204-11, "American Recovery and Reinvestment Act – Reporting Requirements." (March 2009)

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

⁷ FAR 4.605, "Contract Reporting - Procedures."

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 Safeguarding Citizens – Computer Security Systems (Safeguarding Citizens) program.

The purposes of this audit were to evaluate the Safeguarding Citizens program and assess the Department's planning and use of Recovery and Reinvestment Act (Recovery Act) funds in order to meet program objectives, to ensure that Recovery Act funds were used for their intended purposes, and to determine whether the Department complied with Office of Management and Budget (OMB) 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 their findings and conclusions based on audit objectives. We and OIG believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

In our audit of the Department's Safeguarding Citizens program, we interviewed project managers and officials at the Bureaus of Information Resource Management (IRM) and Diplomatic Security (DS). We also evaluated documentation that supported 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 contract files, award documentation, and information published on the Web sites Recovery.gov,

UNCLASSIFIED

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 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 the contract was disclosed and listed in a separate section on Recovery.gov.
- 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.

UNCLASSIFIED

- 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 compared GFMS details and reconciling schedules with information 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 for the Department of State (Department) Recovery and Reinvestment Act (Recovery Act) is allocated between 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. Each TAS and related activities are included within the Department’s weekly financial reports.

As shown in Table 1, the Department’s Capital Investment Fund (TAS 1119) is broken down into three sections: Data Center, Cyber Security, and IT Platform initiatives. Safeguarding Citizens is tracked and recorded under the Cyber Security portion of the fund (TAS 1119.0002).

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	-	38,000,000	38,000,000
TOTAL		\$ 290,000,000	\$ 289,974,923

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 Reports on Audit of the Department of State Safeguarding Citizens – Computer Security Systems 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, through more effective oversight of the quarterly review of recipient-reported data, that contractors that receive awards from the American Recovery and Reinvestment Act for the **Safeguarding Citizens – Computer Security Systems program** provide accurate award information and that the inaccurate award information identified in this report is 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.