National Science Foundation • 4201 Wilson Boulevard • Arlington, Virginia 22230
Office of Inspector General

MEMORANDUM

DATE: February 15, 2011

TO: Dr. Subra Suresh, Director, National Science Foundation

FROM: Allison Lerner
Inspector General

SUBJECT: Federal Information Security Management Act FY 2011 Independent Evaluation Report – OIG Report Number 12-2-004

Attached is the Federal Information Security Management Act of 2002 (FISMA) FY 2011 Independent Evaluation Report. In accordance with Office of Management and Budget (OMB) Memorandum M 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* we previously provided the Inspector General Section of NSF's FY 2011 FISMA Report, which was submitted through the OMB automated reporting tool on November 15, 2011.

Clifton Gunderson's Independent Evaluation Report includes one new finding as follows:

- NSF needs to correct the United States Antarctic Program's (USAP) Certification and Accreditation documentation process to include required elements.

The report also includes four previous findings, as follows:

- The USAP "Advanced Revelation" suite of applications needs to be replaced.
- USAP needs to develop, document, and implement a disaster recovery plan for its Antarctica Operations at its Denver data center.
- NSF needs to remove timely the information technology accounts for separated employees and contractors.
- NSF needs to improve the security of its network topology as the present design poses a potential security weakness.

The Independent Evaluation was performed in conjunction with the annual financial statement audit. A draft of the Independent Evaluation Report was previously submitted to your staff and their comments are included as an attachment to the report.

In accordance with OMB Circular A-50, on Audit Follow-Up, we request that NSF submit a written corrective action plan to our office within 60 days of the date of this memorandum to address the recommendations in the Independent Evaluation. This corrective action plan should identify specific actions your office has taken or plans to take to address each recommendation along with the associated milestone date. We are available to work with your staff to ensure the submission of a mutually agreeable corrective action plan.

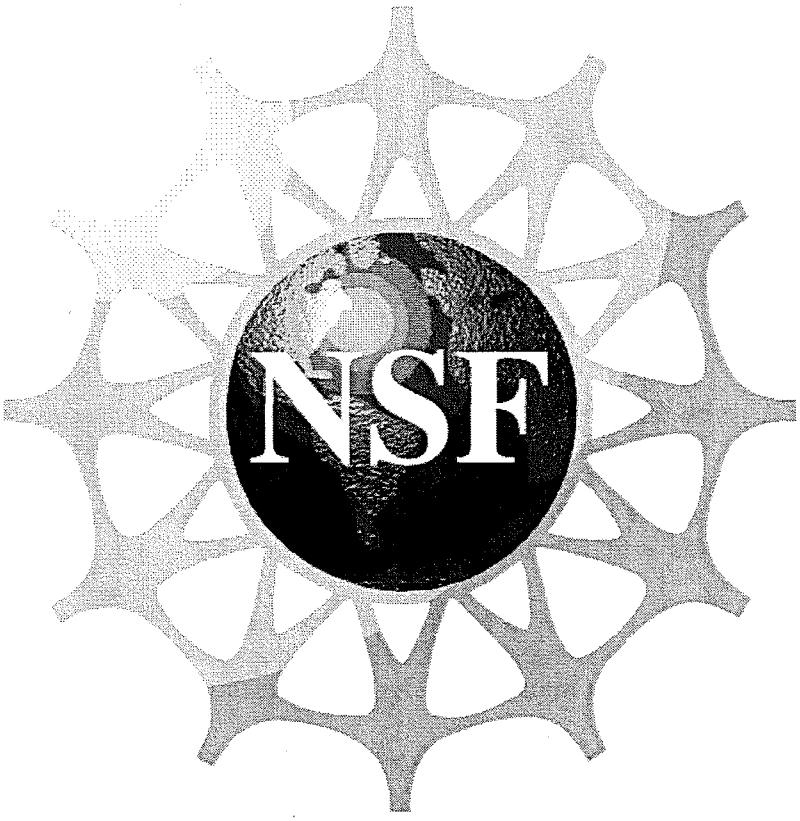
We appreciate the courtesies and cooperation extended to Clifton Gunderson LLP during the evaluation.

If you or your staff has any questions, please contact Brett M. Baker, Assistant Inspector General for Audit, or me at (703) 292-7100.

Attachment

cc: Cora B. Marrett, Deputy Director, Acting, OD
Kathryn Sullivan, Senior Advisor, OD
Karl A. Erb, Director, OPP
Martha Rubenstein, Director and CFO, BFA
Amy Northcutt, Chief Information Officer
Eugene Hubbard, Director, OIRM

FINAL



NATIONAL SCIENCE FOUNDATION

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

2011 INDEPENDENT EVALUATION REPORT

November 10, 2011

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Ms. Allison Lerner
Inspector General
National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

Dear Ms. Lerner:

We are pleased to provide the Fiscal Year (FY) 2011 Office of Inspector General (OIG) response to Office of Management and Budget (OMB) Memorandum M-11-33, "*FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*" and FY 2011 FISMA Independent Evaluation Report, detailing the results of our review of NSF's information security program.

FISMA requires Inspectors General to conduct annual evaluations of their agency's security programs and practices, and to report to OMB on the results of their evaluations. OMB Memorandum M-11-33 provides instructions for meeting the FISMA reporting requirements.

We completed our response to OMB Memorandum M-11-33 based on our independent evaluation as of September 30, 2011, subsequent review through the date of this report of documentation supporting the security program performance statistics reported by NSF management, and review of Plans of Action and Milestones. In preparing our responses, we collaborated with NSF management and appreciate their cooperation in this effort.

NSF management has provided us with a response (dated February 10, 2012) to this FISMA 2011 Independent Evaluation Report. Management accepts our findings and recommendations and intends to develop an action plan to address these findings.

We appreciate the opportunity to assist your office with these reports. Should you have any questions please call George Fallon at (301) 931-2050.

Clifton Gunderson LLP

Calverton, Maryland
November 10, 2011

11710 Beltsville Drive, Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law No. 104-347), also called the Federal Information Security Management Act (FISMA), requires agencies to adopt a risk-based, life cycle approach to improving computer security that includes annual security program reviews, independent evaluations by Inspector General (IG), and reporting to the Office of Management and Budget (OMB) and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

Based on the results of our Fiscal Year (FY) 2011 independent evaluation, we determined that the National Science Foundation (NSF) has an established information security program and has been proactive in reviewing security controls and identifying areas to strengthen this program.

The FY 2010 Independent Evaluation Report included seven findings – two of the findings were from prior years and remain open. These two findings relate to NSF's United States Antarctic Program (USAP) operating environment and disaster recovery plans. NSF plans to correct these weaknesses after the results of the Antarctic Support Contract re-competition have been determined. Three of the five findings found in 2010 are closed. They relate to (1) the annual review of the USAP security plans, (2) maintenance of access authorization documentation and (3) the Security Assessment Report (SAR) for one of NSF's systems. Two of the findings related to NSF's prompt revocation of access, and the security of NSF's network topology remain open.

We are reporting one new finding in FY 2011 relating the USAP Enterprise Business (EBS) Security Assessment Report (SAR).

II. BACKGROUND

NSF is an independent Agency established by the National Science Foundation Act of 1950 to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense. NSF is the funding source for approximately 20 percent of all federally supported basic research conducted by America's colleges and universities. In many fields such as mathematics, computer science, and the social sciences, NSF is the major source of Federal funding. NSF also funds national research centers, state-of-the-art research facilities, and the USAP.

NSF does not operate its own laboratories or research facilities but rather acts as a catalyst providing state-of-the-art tools and facilities and identifying the most capable people and allowing them to pursue innovation.

One of NSF's major programs is the USAP. The Office of Polar Programs (OPP) manages and initiates NSF funding for basic research and operational support for the USAP. NSF has become increasingly dependent on computerized information systems to execute its scientific research and operations and to process, maintain, and report essential information. As a result, the reliability of computerized data and of the systems that process, maintain, and report this data is a major priority for NSF. While the increase in computer interconnectivity has changed the way the government does business, it has also increased the risk of loss and misuse of information by unauthorized or malicious users. Protecting information systems continues to be one of the most important challenges facing government organizations today.

Through FISMA, the U.S. Congress showed its intention to enhance the management and promotion of electronic government services and processes. Its goals are to achieve more efficient government performance, increase access to government information, and increase citizen participation in government. FISMA also provides a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

NSF operates an open and distributed computing environment to facilitate collaboration and knowledge sharing, and support its mission of promoting science, engineering research and education. It faces the challenging task of maintaining this environment, while protecting its critical information assets against malicious use and intrusion.

The NSF Office of Inspector General (OIG) contracted with us to conduct NSF's FY 2011 FISMA Independent Evaluation. We performed this evaluation in conjunction with our review of information security controls required as part of the annual financial statement audit issued on November 11, 2011.

III. OBJECTIVES

The purposes of this evaluation were to assess the effectiveness of NSF's information security program and practices and to determine compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

IV. SCOPE & METHODOLOGY

To perform our review of NSF's security program, we followed a work plan based on the National Institute of Standards and Technology (NIST)'s *Recommended Security Controls for Federal Information Systems – Special Publication (SP) 800-53* for specification of security controls; NIST Special Publications 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems* and 800-*53A Guide for Assessing the Security Controls in Federal Information Systems* for the assessment of security control effectiveness; the Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual (FISCAM: GAO-09-232G);* and our general controls review methodology. The combination of these methodologies allowed us to meet the requirements of both FISMA and the Chief Financial Officer (CFO)'s Act.

Our procedures included following-up on recommendations made in the FY 2010 Independent Evaluation Report; performing internal and external security reviews of NSF's information technology (IT) infrastructure; reviewing agency Plans of Action and Milestones (POA&Ms); and evaluating the following subset of NSF's major systems:

- Financial Accounting System (FAS)
- FastLane
- Awards System (Awards)
- Electronic Jacket (e-Jacket)
- NSF Website
- NSF Network LAN
- USAP Enterprise Business System Application (EBS)
- Central Computer Facility

We performed procedures to test (1) NSF's implementation of an entity-wide security plan, and (2) operational and technical controls specific to each application such as service continuity, logical access, and change controls. We also performed targeted tests of controls over financial and grant processing applications and processes. We performed our review from May 2, 2011 to November 10, 2011 at NSF's headquarters in Arlington, Virginia. We also performed testing of the USAP Enterprise Business System (EBS) in June 2011 in Denver, Colorado.

NSF management and staff were very helpful and accommodating throughout this review and assisted us in refining the recommendations. This independent evaluation was prepared based on information available as of September 30, 2011.

V. DETAILS OF RESULTS

A. Prior Year Results

The FY 2010 Independent Evaluation Report identified seven (7) findings, reported as other weaknesses (i.e., not significant enough to be reported as a significant deficiency in accordance with OMB classification guidelines). The following table summarizes the findings reported in FY 2010 and their current status:

#	Finding Number	Title	Current Status
1	06-01	The USAP "Advanced Revelation" Suite of Applications Needs to be Replaced.	Reissued
2	06-02	USAP Needs to Develop, Document and Implement a Disaster Recovery Plan for its Antarctica Operations.	Reissued
3	10-01	The Security Assessment Report (SAR) for the E-Jacket system needed to include more information.	Closed
4	10-02	The Office of Polar Programs' (OPP) Enterprise Operations System (EOS) System Security Plan (SSP) needs to be reviewed annually as prescribed by NSF policies.	Closed
5	10-03	Office of Polar Programs (OPP) needs to have documentation of authorized access for all Enterprise Operation System (EOS) users.	Closed
6	10-04	NSF needs to remove timely the information technology (IT) accounts for separated employees and contractors.	Reissued
7	10-05	NSF's need to improve security of its network topology as the present design poses a potential security weakness.	Reissued

B. Current Year Results

NSF has been proactive in reviewing security controls and identifying areas to continuously enhance the program. As part of its ongoing security program, NSF periodically performs network scanning and annually re-certifies and re-accredits a select number of major systems consistent with NIST's guidance including Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37), Standards for Security Categorization of Federal Information and Information Systems (FIPS 199), and Recommended Security Controls for Federal Information Systems (SP 800-53 Rev.3).

The following table summarizes the findings that remain open as of September 30, 2011:

Finding Number	Title	Status
06-01	The USAP "Advanced Revelation" Suite of Applications Needs to be Replaced.	Re-issued
06-02	USAP Needs to Develop, Document and Implement a Disaster Recovery Plan for its Antarctica Operations.	Re-issued
10-04	NSF needs to remove timely the information technology (IT) accounts for separated employees and contractors.	Re-issued
10-05	NSF's need to improve security of its network topology as the present design poses a potential security weakness.	Re-issued
11-01	NSF needs to correct the USAP C&A documentation process to include required elements	New

The details of our findings and recommendations follow.

VI. FINDINGS AND RECOMMENDATIONS

06-01 The USAP "Advanced Revelation" Suite of Applications Needs to be Replaced. (Re-Issued)

Operational support of scientific research in Antarctica is the principal responsibility of OPP and Raytheon Polar Services Company (RPSC). To provide this support, OPP depends on a complex array of network systems and applications spread across nine operating sites.

In FY 2006, we reported that the Advanced Revelation application (AREV) was outdated and had inherent security weaknesses. USAP uses Disk Operating System (DOS)-based AREV on Microsoft Windows platforms to process transactions on various applications including: (a) the Personnel Tracking System (PTS) that manages USAP business processes involving Personally Identifiable Information (PII), including hiring records, social security numbers (SSNs), and medical processing checklists; (b) Cargo Tracking System (CTS) for tracking inventory to and from Antarctica; (c) MAPCON, which provides inventory management and equipment maintenance records; and (d) Power 1000, a procurement and receiving subsystem.

AREV was developed using a programming language that is now outdated, and is becoming increasingly difficult to interface with newer systems and platforms. Revelation Software has ceased development and maintenance of AREV. As a result, AREV is difficult to maintain and may not function with newer technologies, which may reduce efficiency in NSF carrying out its mission.

Federal guidelines provided in NIST Special Publication 800-23 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products (SP 800-23) provides advice to Federal organizations on acquisition and use of security-related Information Technology (IT) products. NIST's advice is provided in the context of larger recommendations regarding security assurance. Sp 800-23 states that "Federal Departments and agencies should be aware of how assurance in the acquired products support security...Assurance in individual product components contributes to overall system security assurance. Moreover; performance includes dependability and reliability and hence is directly impacted by security considerations."

An inadequate and antiquated processing environment may expose system resources to intentional and unintentional loss or impairment, destruction, or malicious damage. Security in this DOS-based environment is weak as a user with access privileges on one application in this suite can access several other applications which he does not need access to in the execution of his duties. Continuity of operations cannot be ensured in the face of forced hardware and LAN operating system upgrades. Securing trained personnel/vendors with the requisite expertise to support these antiquated systems will be increasingly difficult.

In FY 2010, OPP and USAP management analyzed the USAP production environment and risks regarding the operation of the AREV application. USAP has completed planning to replace the AREV system with completion scheduled for the fourth quarter of FY 2014. NSF is awaiting the completion of the USAP contract re-competition to allow the selected contractor to determine the best solution for replacing AREV.

Recommendation (06-01)

We repeat our FY 2006 – 2010 recommendation that the Office of Polar Programs replace the AREV suite of applications with a scalable, vendor-supported database management system.

06-02 USAP Needs to Develop, Document, and Implement a Disaster Recovery Plan for its Antarctica Operations. (Re-Issued)

Contingency planning and disaster recovery refers to measures to recover IT services following an emergency or system disruption. Interim measures may include 1) relocation of IT systems and operations to an alternate site, 2) recovery of IT functions using alternate equipment, and 3) performance of IT functions using manual methods.

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorist actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions, as part of the organization's risk management effort, it is virtually impossible to completely eliminate all risks. Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

In FYs 2006 - 2010 we reported that:

- USAP did not have alternate wide area network links or an alternate network security perimeter location to continue mission network communications and general support systems if the Denver operating location became unavailable.
- There was no alternate-site redundancy in key mission support information systems to ensure failsafe recovery in the event of an extended interruption at the central Denver data center.

OPP management completed strategic planning in FY 2009 to mitigate the potential risk of interruption to USAP program operations. Implementation of the disaster recovery plan will occur after the selection of a contractor for the re-competed USAP contract.

NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems states that major disruptions with long-term effects may be rare, but should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

- a dedicated site that is owned or operated by the organization;
- a reciprocal agreement or memorandum of agreement with an internal or external entity; and
- a commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan.

NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, states "...the alternate site should be in a geographic area that is unlikely to be negatively affected by the same disaster event [e.g., weather-related impacts or power grid failure] as the organization's primary site."

There is a risk that an extended outage of the Antarctic network and communications would occur if a natural or man-made disaster caused severe damage to the wide area network communications centrally housed in the USAP Denver operating location.

Unavailability of the network support infrastructure could result in loss of dedicated network communications. Scientific grantees in the Antarctic already backup and store the results of their scientific experiments on physical media, as there is no guarantee of network infrastructure service. This means that the availability of scientific results could be delayed, if critical systems are no longer operational. Because of the lack of a disaster recovery plan, there is a risk that if USAP suffers a disaster it may not recover timely, or in full, which could restrict USAP from carrying out its mission.

Recommendation (06-02)

We repeat our FY 2006 – 2010 recommendation that OPP continue its initiative to create alternate network connectivity in the event of an emergency. This connectivity should be in a geographic area that is unlikely to be negatively affected by the same disaster event as the organization's primary site. In making this decision, NSF should consider other USAP operating locations already in use, in addition to established commercial providers of alternative site services (co-located facilities, data center hosting facilities, restoration network services, etc.).

10-04 NSF needs to remove timely information technology (IT) accounts for separated employees.

In FY 2010, in our sample of 45 separated employees and contractors, we found that the information technology (IT) accounts for three users were not timely removed or deleted upon the termination of the users' employment at NSF. Two employee accounts were removed 34 days and one 30 days after separation. This reflects a continuation of a prior year issue. Therefore, we are repeating this finding for FY11.

NIST 800 -53 – Recommended Security Controls for Federal Information Systems and Organizations stipulates that:

"the organization, upon termination of individual employment:

- Terminate information system access;
- Retrieve all security-related organizational information system-related property; and
- Retain access to organizational information and information systems formerly controlled by terminated individual."

The Division of Information System (DIS) was not notified of employee and contractor separations on time.

A separated employee or contractor who retains access privileges has the opportunity to make malicious changes resulting in potential loss of confidentiality, integrity, and availability of NSF IT resources.

Recommendation (10-04)

We recommend that NSF develop and implement a policy that clearly defines responsibilities for notifying DIS of upcoming departures and the subsequent removal of physical and logical access for all separated employees and contractors within 48 hours of separation.

10-05 NSF needs to improve security of its network topology as the present design poses a security risk. (Modified Repeat)

NSF needs to improve security of its network topology as the present design poses a security risk. NSF has added a perimeter firewall to offer protection for the external facing services and devices, thus creating the "demilitarized zone" or DMZ. However, the external firewall provides little application layer inspection and filtering of any harmful content that may be considered an attack on the external facing services. The outside firewall device only provides limited source host filtering. The network design does not offer isolation of publicly available computer assets via physically separate subnets with managed interfaces to other portions of the network.

Based on NIST Special Publication 800-45 *Guidelines on Electronic Mail Security*, a Single Firewall approach does not offer protection against most network protocol attacks (POP, IMAP) and does not protect against application layer attacks.

Based on NIST Special Publication 800-46 Rev1 *Guide to Enterprise Telework and Remote Access Security,* if the remote access server is a different device than the firewall, then the best location for the remote access server is the DMZ to offer separation from the trusted internal network.

Based on NIST Special Publication 800-44 *Guidelines on Security Public Web Servers* a DMZ offers a design compromise solution that offers the most benefits with the least amount of risk for provided access to public web servers.

Based on NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems:*

> as part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

There is a risk to NSF's unprotected assets in the event of single system compromise of a publicly accessible system, which could result in loss of availability, integrity and confidentiality of computer systems and data. There remains risk associated with filtering limited to source IP address capability. Application specific attack identification and response remain absent from the current configuration, which could result in system compromise and lead to loss of availability, integrity, and confidentiality of systems and data.

Recommendation (10-05)

We recommend that NSF develop protocol and application specific filters to protect publicly available services.

***11-01 NSF* needs to correct the USAP C&A documentation process to include required elements.**

We noted in our review of the Security Assessment Report (SAR) for the Enterprise Business System (EBS) that the SAR was not prepared in accordance with NIST SP 800-37 guidance. Specifically, the results of Information Security Assessment (ISA) testing were not incorporated into the SAR. The ISA with the completed and analyzed results provides a step toward identifying remaining potential weaknesses.

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, states that:

> Security control assessment results obtained during system development are brought forward in an interim report and included in the final security assessment report. This supports the concept that the security assessment report is an evolving document that includes assessment results from all relevant phases of the system development life cycle including the results generated during continuous monitoring.

Recommendation (11-01)

We recommend that NSF enhance the C&A documentation process to include required elements including the results of the Information Security Assessment (ISA) testing or other continuous monitoring reports into the SAR.

VII. OTHER INFORMATION COMMUNICATED TO MANAGEMENT

We conducted internal and external vulnerability assessments and penetration testing on NSF systems located in Arlington, Virginia, in accordance with the rules of engagement agreed upon with NSF. We performed this testing to identify possible weaknesses in NSF's logical security controls and to attempt to exploit discovered vulnerabilities and to determine the degree of control an attacker could achieve after a successful penetration. During our assessment, we discovered live hosts residing on external and internal NSF networks and conducted overt and covert vulnerability assessments on IP addresses in use. We obtained approval prior to exploiting discovered vulnerabilities. We gained access to the teleconferencing video system during our testing. We then advised management in a separate document on corrective actions to further strengthen its environment.

Office of Chief Information Officer

MEMORANDUM

Date: FEB 10 2012

To: Ms. Allison C. Lerner
Office of the Inspector General

From: Amy Northcutt
Chief Information Officer

Subject: Response to the "Federal Information Security Management Act (FISMA) 2011 Independent Evaluation Report"

Thank you for the opportunity to review the subject report, which presents the results of CliftonLarsonAllen's review of NSF's information security program.

We will provide an updated action plan to address the five findings detailed in the report.

We appreciate your recognition of NSF's information security program and the efforts of the OIG staff and audit team throughout this review. We will incorporate information gained and lessons learned from this review as we continue to make improvements in our program.

cc:
Subra Suresh/OD
Cora B. Marrett/OD
Kathryn Sullivan/OIA
Karl A. Erb/OPP
Amy Northcutt/CIO
Gene Hubbard/OIRM
Dorothy Aronson/OIRM
Dan Hofherr/OIRM
Martha Rubenstein/BFA
Sal Ercolano/CliftonLarsonAllen
George Fallon/CliftonLarsonAllen