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

DATE: February 18, 2014

TO: Dr. Cora Marrett,
Director (Acting), National Science Foundation

FROM: Dr. Brett M. Baker
Assistant Inspector General for Audit

SUBJECT: *Federal Information Security Management Act FY 2013 Independent Evaluation Report*, Report Number 14-2-003

This memorandum transmits CliftonLarsonAllen LLP's (CLA) Federal Information Security Management Act of 2002 (FISMA) FY 2013 Independent Evaluation Report. In accordance with Office of Management and Budget (OMB) Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, we previously provided the Inspector General Section of NSF's FY 2013 FISMA Report, which was submitted through the OMB automated reporting tool on December 2, 2013.

CliftonLarsonAllen's Independent Evaluation Report includes eight new findings as follows:

- USAP needs to improve controls over policies and procedures.
- USAP needs to improve configuration management controls.
- USAP needs to complete MOUs/ISAs General Support System Local-Area Network (GSS LAN) and Enterprise Business System (EBS) interconnections.
- USAP needs to improve timeliness of system remediation based on scan results.
- USAP needs to improve account management controls.
- USAP needs to improve assessment and authorization controls.
- NSF Security Assessment Reports (SARs) need to identify consistently all assessed risks.
- NSF needs to address weaknesses in role-based IT security awareness and training.

The report also includes 11 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.
- USAP needs to review its System Security Plan for consistency with NIST requirements.
- USAP needs to enforce NSF's password and account management policies at USAP.

- NSF needs to address weaknesses in its IT accreditation packages.
- NSF needs to address weaknesses in its IT identification and authorization controls.
- NSF needs to address weaknesses in its IT configuration management controls over baseline conformance.
- NSF needs to address weaknesses in its IT configuration management controls over ACM$ Change Management.
- NSF needs to address weaknesses in the NSF and USAP Incident Response program.
- NSF needs to improve controls over IT account management.

Please note that this year's Independent Evaluation Report includes summarized versions of findings reported in a separate IT Management Letter (dated December 12, 2013) prepared in conjunction with CLA's audit of NSF's FY 2013 financial statements, and being transmitted under separate cover. CLA considers the management letter findings relevant to the FISMA report since the specific conditions identified for NSF's financial systems are also covered by FISMA.

The Independent Evaluation was performed in conjunction with the annual audit of NSF's financial statements. A draft of the Independent Evaluation Report was previously submitted to your staff and their comments were considered in preparing this final 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 CliftonLarsonAllen LLP during the evaluation. If you or your staff has any questions, please contact Tom Moschetto, Director, Financial and IT Audits at (703) 292-7398, or me at (703) 292-2985.

Attachment

cc: Dan Arvizu, Chair, National Science Board
G.P. Peterson, Chair, Audit and Oversight Committee
Kathryn Sullivan, Senior Advisor, OD
Eugene Hubbard, Director, OIRM
Amy Northcutt, Chief Information Officer
Roger Wakimoto, Assistant Director, GEO
Kelly K. Falkner, Director, PLR
Martha Rubenstein, Director and CFO, BFA
Susanne LaFratta, Senior Advisor, PLR

NATIONAL SCIENCE FOUNDATION

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

2013 INDEPENDENT EVALUATION REPORT

December 12, 2013

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.claconnect.com

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

Dear Ms. Lerner:

We are pleased to provide the FY 2013 FISMA Independent Evaluation Report. The report details the results of our review of National Science Foundation (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. The Office of Management and Budget (OMB) Memorandum M-14-04 ("*FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"*) provides this year's instructions for meeting the FISMA reporting requirements.

We separately provided the Fiscal Year (FY) 2013 Office of Inspector General (OIG) response to Memorandum M-14-04, based on our independent evaluation as of September 30, 2013 and subsequent review through the date of the report of documentation supporting the security program performance statistics reported by NSF management, and review of the Foundation's Plans of Action and Milestones (POA&Ms). In preparing our responses, we collaborated closely with NSF management and appreciate their cooperation throughout this effort.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we 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 believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

NSF management has provided us with a response to this 2013 FISMA Independent Evaluation Report, which is presented in Exhibit A. We did not audit management's response and, accordingly, do not provide any conclusion on it.

This report is issued for the restricted use of the Office of Inspector General, the management of NSF, the National Science Board and its Audit & Oversight Committee, and the Office of Management and Budget, and is marked Sensitive But Unclassified.

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

CliftonLarsonAllen LLP

Calverton, Maryland
December 12, 2013

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 Inspectors 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) 2013 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 2012 Independent Evaluation Report included eight findings – four of the findings were from FY 2010 and earlier, and three of these remain open. Two of these three findings relate to NSF's United States Antarctic Program (USAP) operating environment and disaster recovery plans. NSF continues to develop plans to correct these weaknesses now that the new Antarctic Support Contractor has completed the transition to replace its predecessor. The remaining reissued prior year finding relates to the need for NSF to ensure prompt revocation of user access upon termination. The finding related to the risks to security associated with NSF's overall network topology has been closed.

The other four findings in the FY 2012 report include two that have been closed related to patch management and the need to include required elements in C&A documentation. The two that are being reissued as repeat findings, both for USAP, include the need to update System Security Plans to be consistent with National Institute of Standards and Technology (NIST) requirements, and to enforce NSF password and account management policies more consistently at USAP.

We are reporting eight new FISMA-related findings in FY 2013, six for USAP and two for NSF:

- 13-01: USAP - Policies/procedures documentation (availability, completeness, accuracy)
- 13-02: USAP - Configuration management (change management)
- 13-03: USAP - Assessment and authorization (MOUs/ISAs)
- 13-04: USAP - Risk assessment (scanning procedures)
- 13-05: USAP - Access controls (account management)
- 13-06: USAP - Assessment and authorization (risk understanding and acceptance)
- 13-07: NSF - Assessment and authorization (Security Assessment Reports)
- 13-08: NSF - Weaknesses in NSF Role-based IT Security Awareness and Training (Note: Finding 13-08 is drawn from our Management Letter)

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% 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 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 USAP. The Division of Polar Programs (part of the Directorate for Geosciences, previously the Office of Polar Programs, or OPP) manages and initiates NSF funding for basic research and operational support for USAP under a primary contract with Lockheed Martin Corporation known as the Antarctic Support Contract (ASC). Operating under extreme environmental and logistical conditions in Antarctica creates special challenges for effective execution of USAP's mission supporting scientific research, requiring extensive global support and coordination of communications, personnel and supplies.

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 CLA to conduct NSF's FY 2013 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 December 12, 2013.

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 following guidance:

- National Institute of Standards and Technology (NIST)'s Special Publication (SP) 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* for specification of security controls;
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach;* and SP 800-53A Rev. 1*, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* for the assessment of security control effectiveness;
- Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual (FISCAM: GAO-09-232G);*
- CliftonLarsonAllen's 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 2012 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 as part of our three-year rotation strategy:

- Core Financial System (FAS - Financial Accounting System) components:
  - Standard General Ledger
  - Budget Execution/Funds Management

- Awards/Grants Management System:
  - Electronic Jacket
  - Research.gov (ACM$ module only)

- Non-Financial & General Support Systems:
  - NSF Network (LAN), general controls only (no Vulnerability Assessment with Penetration Testing)

- United States Antarctic Program:
  - USAP Enterprise Business System application (EBS)
  - USAP Enterprise Network General Support System (GSS), including Vulnerability Assessment with Penetration Testing

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 April 2013 to September 30, 2013 at NSF's headquarters in Arlington, Virginia. Finally, we tested the USAP EBS and GSS in July 2013 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, 2013.

V. DETAILS OF RESULTS

A. Prior Year Results

The FY 2012 Independent Evaluation Report identified eight (8) 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 2012 and their current status:

(FY – Finding #)	Description	Current Year Status
06-01	The USAP "Advanced Revelation" suite of applications needs to be replaced.	Reissued
06-02	USAP needs to develop, document and implement a Disaster Recovery Plan for its Antarctica operations.	Reissued
10-04	NSF needs to remove timely the information technology (IT) accounts for separated employees and contractors.	Reissued
10-05	NSF needs to improve security of its network topology as the present design poses a potential security weakness.	Closed
12-01	NSF needs to improve its patch management process for the timely resolution and mitigation of logical security vulnerabilities	Closed
12-02	NSF needs to correct the USAP C&A documentation process to include required elements	Closed
12-03	USAP needs to review its System Security Plans for consistency with NIST requirements	Reissued
12-04	USAP needs to enforce NSF's password and account management policies consistently	Reissued

B. Current Year Results

The following table summarizes both the reissued/repeat and new findings noted as of September 30, 2013. Note that this year's Independent Evaluation Report includes summarized versions of findings reported in a separate IT Management Letter (dated December 12, 2013) prepared in conjunction with the audit of NSF's FY 2013 financial statements. We consider the management letter findings relevant to the FISMA report since the specific conditions identified for NSF's financial systems are also covered by FISMA. Such findings carried forward from the IT management letter (identified as such using the prefix "ML") are distinguished from other security program weaknesses affecting non-financial systems discussed in this report. The status shown for IT ML findings also differs from that of FISMA-only findings in that they may appear as "Repeat" or Modified Repeat":

(FY – Finding #)	Description	Current Year Status
06-01	The USAP "Advanced Revelation" suite of applications needs to be replaced.	Reissued
06-02	USAP needs to develop, document and implement a Disaster Recovery Plan for its Antarctica operations.	Reissued
10-04	NSF needs to remove timely the information technology (IT) accounts for separated employees and contractors.	Reissued
12-03	USAP needs to review its System Security Plans for consistency with NIST requirements	Reissued
12-04	USAP needs to enforce NSF's password and account management policies consistently	Reissued
ML-12-07	NSF needs to address weaknesses in its IT accreditation packages	Repeat
ML-12-09	NSF needs to address weaknesses in its IT identification and authorization controls	Modified Repeat
ML-12-10	NSF needs to address weaknesses in its IT configuration management controls over baseline conformance	Repeat
ML-12-11	NSF needs to address weaknesses in its IT configuration management controls over ACM$ Change Management	Modified Repeat
ML-12-12	NSF needs to address weaknesses in the NSF and USAP Incident Response program	Modified Repeat
ML-12-13	NSF needs to improve controls over IT account management	Repeat
13-01	USAP needs to improve controls over policies and procedures	New
13-02	USAP needs to improve configuration management controls	New

(FY – Finding #)	Description	Current Year Status
13-03	USAP needs to complete MOUs/ISAs General Support System Local-Area Network (GSS LAN) and Enterprise Business System (EBS) interconnections	New
13-04	USAP needs to improve timeliness of system remediation based on scan results	New
13-05	USAP needs to improve account management controls	New
13-06	USAP needs to improve assessment and authorization controls	New
13-07	NSF Security Assessment Reports (SARs) need to identify consistently all assessed risks	New
ML-13-08	NSF needs to address weaknesses in role-based IT security awareness and training	New

We have discussed these comments and suggestions with agency personnel, and we will be pleased to discuss them in further detail at your convenience. We will review the status of these comments during our subsequent year's audit engagement.

VI. FINDINGS AND RECOMMENDATIONS

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

Operational support of scientific research through the United States Antarctic Program (USAP) is the principal responsibility of the Division of Polar Programs (Polar, formerly the Office of Polar Programs) and its contractor, Lockheed Martin Antarctic Support Contract (ASC). Prior to the award of a new support contract on April 1, 2012 Raytheon Polar Services Company (RPSC) was the main contractor. To provide this support, Polar depends on a complex array of network systems and applications provided by the contractor, which are 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 (i.e., native DOS programs, as there is no Windows version) 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.

Security in this DOS-based environment is weak as users with access privileges on one application in this suite can inappropriately or unnecessarily access several other applications. In addition, continuity of operations cannot be ensured when confronted with forced hardware changes and Local Area Network (LAN) operating system upgrades. Securing trained personnel/vendors with the requisite expertise to support these antiquated systems will be increasingly difficult.

In FY 2010, the Office of Polar Programs and USAP management analyzed the USAP production environment and risks regarding the operation of the AREV application. As a result, USAP planned to work on replacing the AREV system by Q4 FY 2014.

In FY 2013, Polar is actively working with its new contractor, Lockheed Martin ASC, to determine the best strategy to replace AREV.

Recommendations (06-01):

We recommend, as we have previously (since FY 2006) that:

- NSF Division 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 and 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.

Beginning in FY 2006, 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 in case the Denver operating location becomes 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.

In FY 2010, OPP management completed strategic planning to mitigate the potential risk of interruption to USAP program operations.

In FY 2013, the Division of Polar Programs is working with its new contractor, Lockheed Martin, to determine the best strategy for contingency planning and disaster recovery. Implementation is to be determined.

Recommendations (06-02)

We recommend, as we have previously (since FY 2006) that:

- NSF Division of Polar Programs implement 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 affected negatively 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 (colocation facilities, data center hosting facilities, restoration network services, etc.).

10-04 NSF needs to remove information technology (IT) accounts for separated employees on a timely basis. (Re-Issued)

We noted the following weaknesses in National Science Foundation (NSF)'s controls of separated employees and contractors:

- Exit Clearance Forms were not appropriately completed for 6 of the 25 employees that we tested. Specifically, we noted the following:
  - 3 of the Exit Forms were not signed by the Authorizing Official (AO) or the Contract Office's Technical Representative (COTR).
  - 3 of the forms were not completed within 2 business days of the employee's termination date in accordance with NSF procedures.
- Identity Management system (IDM) help desk tickets were not opened within 2 business days of the individual's termination date for 6 of the 25 individuals.
- There was one (1) terminated individual identified that still had eJacket access.

Note: NSF formally closed the related POA&M on 7/1/2013. The above individuals terminated before that date; however, some of them did not have their exit clearance process completed until after July 1st, and the eJacket individual cited retained access after that date.

Recommendations (10-04):

We recommend, as we have previously (since FY 2010) that:

- NSF strengthen controls to ensure that clearance forms are properly completed and maintained for terminated employees and contractors.
- NSF ensure the system accounts of terminated users are deactivated timely.

12-03 NSF needs to review USAP System Security Plans for consistency with NIST requirements. (Re-Issued)

We noted the following weaknesses in the accreditation packages for the USAP Enterprise Operations System (EOS), the USAP General Support System (GSS) and the USAP Enterprise Business System (EBS):

The EOS System Security Plan (SSP) was not fully consistent with NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* and SP 800-53 Rev.3 requirements. For example, we noted the following:

- The IA-5 control implementation did not address the server operating systems.
- Control enhancement AC-17(5) was not addressed in the control implementation.
- The CP-9(1) control implementation does not identify the organizationally defined frequency for testing backup information to verify media reliability and information integrity. The controls only state that Backup Exec tests media reliability at the conclusion of any backup job but that does not address the control requirement.
- The RA-5 control implementation does not identify organizationally defined response times for remediating vulnerabilities.

- The USAP GSS System Security Plan (SSP) was not fully consistent with NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* and SP 800-53 Rev.3 requirements. For example, we noted the following:
  - The CP-9(1) control implementation does not identify the organizationally defined frequency for testing backup information to verify media reliability and information integrity. The controls only state that Backup Exec tests media reliability at the conclusion of any backup job but that does not address the control requirement.
  - The RA-5 control implementation does not identify organizationally defined response times for remediating vulnerabilities.
  - Some results from USAP Security Assessments documented in the Security Assessment Management Review (SAMR) workbook were not incorporated into the GSS System Security Plan. For example, the AU-1, MP-1, PS-1, PE-1, PS-1, and AC-6 controls status state that the controls are satisfied; however, there are weaknesses identified in the SAMR workbook for these controls.
  - The GSS SSP indicates credentialed scans do not cover all devices since they are limited to a sample of approximately 100 machines; however, USAP is actually performing credentialed scans on all machines.

- The USAP EBS System Security Plan (SSP) was not fully consistent with NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* and SP 800-53 Rev.3 requirements. For example, we noted the following:
  - The CP-9(1) control implementation does not identify the organizationally defined frequency for testing backup information to verify media reliability and information integrity. The controls only state that Backup Exec tests media reliability at the conclusion of any backup job but that does not address the control requirement.
  - The RA-5 control implementation does not identify organizationally defined response times for remediating vulnerabilities.
  - The IA-5 control enhancements and implementation states that passwords must be a minimum of 12 alphanumeric characters and the system prevents reuse of the previous 24 passwords; however, we found that the password length for POLAR ICE was set to a minimum of 8 instead of 12 alphanumeric characters. Additionally, POLAR ICE password history was set to remember 10 passwords instead of 24.

  - Interconnection Security Agreements (ISAs) have not been completed for the interconnections with HealthLink and UTMB; however, the CA-3 control implementation does not state that the ISAs are not in place.

Recommendations (12-03)

NIST SP 800-53 has been updated and Revision 4 was issued in April 2013. Federal agencies are expected to comply by April 2014. Our recommendations have been updated with this in mind.

We recommend that:

- NSF ensure the USAP EOS SSP is updated to be consistent with NIST SP 800-18 rev.1 and 800-53 rev.4 Requirements.
- NSF ensure the USAP GSS SSP is updated to be consistent with NIST SP 800-18 rev.1 and 800-53 rev.4 Requirements.
- NSF ensure the USAP EBS SSP is updated to be consistent with NIST SP 800-18 rev.1 and 800-53 rev.4 Requirements.

12-04 NSF needs to enforce its password and account management policies at USAP. (Re-Issued)

Password settings for POLAR ICE were not consistent with NSF policy. Specifically, we noted the following:

- Password length was set to a minimum of 8 instead of 12 characters.
- Password history was set to remember 10 instead of 24 passwords.

Recommendations (12-04)

We recommend that:

- NSF ensure the USAP POLAR ICE password settings are consistent with defined NSF password standards

ML-12-07 *(Repeat)*: Weaknesses in NSF IT Accreditation Packages

We noted the following weaknesses in the accreditation packages for NSF systems:

- The NSF Network System Security Plan (SSP) was not fully consistent with NIST SP 800-18 rev.1 and SP 800-53 rev.3 requirements.
- The Research.gov System Security Plan (SSP) was not fully consistent with NIST SP 800-18 rev.1 and SP 800-53 rev.3 requirements.
- The FAS System Security Plan (SSP) was not fully consistent with NIST SP 800-18 rev.1 and SP 800-53 rev.3 requirements.
- The eJacket System Security Plan (SSP) was not fully consistent with NIST SP 800-18 rev.1 and SP 800-53 rev.3 requirements.

NSF started a new streamlined certification and accreditation process (C&A), now Assessment & Authorization (A&A), in FY 2010. The new process was designed to have all the controls documented in the Cybersecurity Assessment and Management system (CSAM), and provide summary documents to authorizing officials for approval. NSF staff first document all of the controls and security testing results in CSAM, and then pull the information into the security plans. When the information is not entered correctly into CSAM, or controls are not adequately addressed, then incomplete and inaccurate information is transferred over to the actual security plans, and may not be detected by plan reviewers, in turn negatively affecting the reliable review of documentation in CSAM.

Weaknesses in A&A documentation increase the risk that appropriate security controls will not be consistently applied. System resources may not be properly protected if risk is not properly assessed and documented. Thus, NSF is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected. If the information contained in the authorization package (i.e., the security plan, and the security assessment report) are not appropriately updated, the authorizing official and the information system owner may not have an up-to-date status of the security state of the information system and authorizing officials may not have all of the information necessary to make an informed risk based authorization decision.

Recommendations (ML-12-07)

NIST SP 800-53 has been updated and Revision 4 was issued in April, 2013. Federal agencies are expected to comply by April 2014. Our recommendations have been updated with this in mind.

We recommend that:

- NSF enhance its review process to ensure the accuracy and completeness of its System Security Plans (SSP).
- NSF update the NSF Network SSP to be consistent with NIST 800-18 rev.1 and 800-53 rev.4 requirements.
- NSF update the FAS SSP to be consistent with NIST 800-18 rev.1 and 800-53 rev.4 requirements.
- NSF update the Research.gov SSP to be consistent with NIST 800-18 rev.1 and 800-53 rev.4 requirements.
- NSF update the eJacket SSP to be consistent with NIST 800-18 rev.1 and 800-53 rev.4 requirements.

ML-12-09 *(Modified Repeat)*: Weaknesses in NSF IT Identification and Authentication Controls

We note the following weaknesses in NSF's identification and authentication controls for information systems:

- Lightweight Directory Access Protocol (LDAP) password settings were not consistent with NSF policy.
- Password Settings for the Sybase database supporting FAS and eJacket were not consistent with NSF policy.
- Research.gov Oracle database password settings were not consistent with NSF policy.

- Password Settings for the Sybase database supporting ACM$ were not consistent with NSF policy.
- During the prior year audit, CLA noted weaknesses in specific password and account lockout settings for the Solaris operating system supporting Research.gov. As a part of our current year audit process, CLA was notified by NSF that corrective actions were still ongoing.

NSF is in the process of updating its baseline configuration requirements for its databases and operating systems that include strong password controls. NSF plans to complete this process in FY 2014.

Weaknesses in identification and authentication controls increase the risk that individuals may obtain unauthorized access to NSF systems; thus putting systems and data at risk of unauthorized disclosure, modification or destruction.

Recommendations (ML-12-09)

We recommend that:

- NSF ensure LDAP password settings are consistent with NSF password requirements.
- NSF ensure password settings for the Sybase database that support FAS and eJacket are consistent with NSF password and account lockout requirements.
- NSF ensure password settings for the research.gov Oracle and Sybase databases (including ACM$, which is implemented as a module within Research.gov using Sybase) and its supporting Solaris operating system are consistent with NSF password and account lockout requirements.

ML-12-10 *(Repeat)*: Weaknesses in NSF IT Configuration Management Controls – Baseline Conformance

We noted the following weaknesses in NSF's configuration management controls:

- The production Sybase database that supports the FAS and eJacket applications was not configured in accordance with the documented Sybase Configuration Checklists.
- The production Sybase database that supports the ACM$ module was not configured in accordance with the documented Sybase Configuration Checklists.

NSF is in the process of updating its baseline configuration requirements for its Sybase databases and implementing the baselines on its financial applications. NSF plans to complete this process in FY 2014.

Weaknesses in configuration management controls increase the risk that system components may not have security settings consistently applied thus putting the information systems and data at risk. NSF may be exposed to increased risk of data modification or deletion. Unauthorized changes could occur and go undetected.

Recommendations (ML-12-10):

We recommend that:

- NSF ensure the production Sybase database supporting the FAS and eJacket applications is configured in accordance with the approved baseline and any deviations are properly authorized and approved.
- NSF ensure the production Sybase database supporting the ACM$ module is configured in accordance with the approved baseline and any deviations are properly authorized and approved.

ML-12-11 *(Modified repeat)*: Weaknesses in NSF IT Configuration Management Controls – ACM$ Change Management

We noted weaknesses in NSFs controls for managing configuration changes to ACM$.

NSF's procedures to implement its change control policies are not adequate, which leads to incomplete documentation of the review and approval process for system changes. NSF uses ClearQuest to document change requests. Approvals are not maintained in the NSF ClearQuest system. NSF informed us that detailed changes were entered into ClearQuest for pending changes to be included in the upcoming release; however, there are no approvals performed at this time. We were informed that a collection of application releases with the selected change requests are reviewed in a single Readiness Review presentation. However, change requests should be approved and scheduled before changes are developed and tested.

Weaknesses in configuration management controls, including documentation of review and approval, increases the risk that unauthorized changes may be implemented without going through the appropriate change control process. Unapproved changes may adversely impact the integrity and/or security of the application, which may lead to unauthorized transactions, or modification or deletion of data.

Recommendations (ML-12-11):

We recommend that:

- NSF ensure change approvals are documented for all changes and that the approvals clearly indicate which changes are being approved.
- NSF ensure all of the appropriate approval signatures are documented for each change.

ML-12-12 *(Modified repeat)*: Weaknesses in NSF and USAP Incident Response

There were weaknesses in the procedures both NSF and USAP followed for handling incidents.

Although NSF has documented its Computer Security Incident Response Plan and Procedures, the requirements were not always followed. As a result, security incidents were not documented, tracked and reported in line with the NSF procedures. The NSF procedures centralize the incident response handling and reporting capability; however in practice, USAP has a level of flexibility in handling and reporting incidents that was not documented within the current NSF procedures.

Weaknesses in incident response controls increase the risk that incidents may not be reported or resolved within NSF's time frames, which may lead to unauthorized access to sensitive information, and/or malicious modification or deletion of data or transactions. NSF may not be able to correlate current incidents to past incidents to identify trends or widespread attacks. Additionally lessons learned may not be incorporated into the incident response process to enable management to improve the process.

Recommendations (ML-12-12):

We recommend that:

- NSF ensure all security incidents are consistently identified as such, and are documented and tracked within its incident tracking system.
- NSF ensure all security incidents are categorized in line with the US CERT Incident Categories.
- NSF ensure all applicable security incidents are reported to US CERT in a timely manner.
- NSF ensure USAP incidents are handled in accordance with the centralized incident handling process or formally document and implement alternative processes for USAP.

ML-12-13 *(Repeat)*: Weaknesses in Account Management

We noted the following weaknesses in NSF's account management controls:

- NSF does not maintain documentation evidencing the authorization and approval of eJacket access permissions.
- There are weaknesses in the NSF process for periodically recertifying access permissions for the Sybase databases supporting its financial applications.
- FAS access permissions were not consistent with the access e-mails for one (1) of the 25 individuals tested.

NSF's current process does not require Administrative Managers to maintain documentation evidencing approvals for granting eJacket access permissions. Also, the recertification process for Sybase databases did not include sending out a list of a database accounts. Individuals requesting FAS access permissions are not always aware of the access that they are requesting; as a result, the system administrators sometimes interpret the intention of requests while granting access.

Weakness in account management controls increases the risk that users may have unauthorized access to NSF systems and data.

Recommendations (ML-12-13):

We recommend that:

- NSF ensure authorization and approval of eJacket access permissions are documented and maintained.
- NSF strengthen controls to ensure that access permissions for the FAS, eJacket, and/or ACM$ Sybase databases are recertified periodically.
- NSF strengthen controls to ensure that the assigned access permissions for the FAS users are consistent with the approval emails that requested the access.

- NSF ensure the individuals responsible for approving FAS access permissions are aware of the meaning of the access permissions that they are requesting.
- NSF ensure administrative Officers (AO) are trained on the various FAS job classes and the actions that they allow an individual to perform. Additionally, system administrators should not interpret unclear access requests, and should instead have the AO resubmit an updated request after working with them to identify the specific access permissions needed.

13-01 USAP needs to improve controls over policies and procedures (New)

We noted weaknesses in USAP's controls over policies and procedures. Specifically,

- Some USAP policies and procedures were not available for review when initially requested, though the missing policies and procedures were eventually provided (between 9/4/2013 and 9/6/2013) after we clarified the need to review documents actually in place during the year vs. those that were being updated and undergoing management review when initially requested in July 2013. Specifically, we noted the following policies and procedures that were not received in time to allow for appropriate testing:
    - Systems and Communications Protection
    - Systems and Information Integrity
    - System and Services Acquisition
    - System Maintenance
    - Media Protection and Sanitization
    - Policies and procedures for granting, removing and periodically reviewing Virtual Private Network (VPN) access for the USAP General Support System Local Area Network (GSS LAN)
    - USAP Policies and procedures for reviewing and disabling inactive accounts.

- There are weaknesses in the USAP Audit and Accountability Policies and Procedures. Specifically, we noted the following:
    - The USAP auditing policy and procedure documents are not finalized or authorized, nor do they have documented management commitment
    - USAP Security Auditing Policy does not facilitate implementation of all audit and accountability controls, including establishing a policy requirement for audit storage capacity and response to audit processing failures
    - The audit and accountability procedure IT-A-9309 QSP-System Auditing has not been reviewed/updated in accordance with the organizational defined frequency, "annually"
    - The list of events USAP information systems must be capable of auditing is not based on a risk assessment. Additionally, the subset of auditable events defined in AU-2 to be audited within the information system is not based on current threat information and ongoing assessment of risk.
    - The USAP policy does not define the frequency of auditing each identified event.

- The NSF *Information Security Handbook* has conflicting requirements for session locks. The Access Control Section of the document requires a session lock after 30 minutes of inactivity while the Security Control Parameters section lists the requirement at 15 minutes.

Recommendations (13-01)

We recommend that:

- NSF ensure USAP policies and procedures for key IT controls are accessible and readily available.
- NSF ensure USAP finalizes, approves, and implements Audit and Accountability Policies and Procedures that adequately address risks in the USAP systems auditing environment. The procedures should address controls such as audit storage capacity and response to audit processing failures, list of auditable events based on risk assessment, and frequency of auditing each identified event.
- NSF update the *Information Security Handbook* to include the appropriate session lock settings.

13-02 USAP needs to improve configuration management controls (New)

We noted the following weaknesses in USAP's configuration management controls:

- USAP does not test and validate some changes to the USAP GSS information system before implementing the changes on the operational system.
- USAP GSS system components (e.g., servers and networking devices with various operating systems) were not consistent with their standard configurations and unauthorized changes to configuration settings were not investigated.

Recommendations (13-02)

We recommend that:

- USAP test and validate all GSS changes to the information system before implementing the changes on the operational system.
- USAP ensure the GSS systems are configured in accordance with the approved standard configurations and any deviations are properly investigated and approved.

13-03 USAP needs to complete MOUs/ISAs General Support System Local-Area Network (GSS LAN) and Enterprise Business System (EBS) interconnections (New)

USAP has not completed the implementation of interconnection security agreements (ISA) and memoranda of understanding (MOU) for all USAP General Support System Local-Area Network (GSS LAN) or Enterprise Business System (EBS) interconnections.

Recommendations (13-03)

We recommend that:

- NSF ensure ISAs and MOUs are documented for all external systems with interconnections to the USAP GSS and EBS systems.

13-04 USAP needs to improve timeliness of system remediation based on scan results (New)

We noted the following weakness in USAP's vulnerability assessment controls:

- Vulnerabilities noted from the scans of the USAP systems are not always remediated timely. For instance the June 2013 USAP IT Security Management Report showed that the corrective actions for resolving 85 moderate vulnerabilities were delayed. CLA scans performed during July 2013 identified 7 hosts with addressable (exploitable) vulnerabilities that could be addressed through timely patching.

Recommendations (13-04)

We recommend that:

- NSF ensure that vulnerabilities from the USAP scans are remediated within organizationally defined time periods.
- USAP consider modifying IS-SOP-9306 to require remediation of vulnerabilities designated 'critical and high' instead of 'high and medium' to align the procedure with current practices.

13-05 USAP needs to improve account management controls (New)

We noted the following weaknesses in USAP's account management controls:

- Access permissions for the SHIELD application's users were not appropriately authorized and approved. A USAP User Service Request form was not completed until 8/29/2013 for 9 of the 10 users that we tested even though they had SHIELD access prior to 7/8/2013. The documentation provided showed 30 SHIELD users who were granted access to the system without having an initial approved user service request.
- Access forms or evidence of recertification was not available for 22 of the 25 POLAR ICE application users that we tested.
- The date that the USAP datacenter visitor logs were reviewed was not documented on the record provided; therefore, we could not establish whether the reviews were actually occurring on a quarterly basis.
- Details of the USAP datacenter access recertification were not provided for review.

Recommendations (13-05)

We recommend that:

- NSF ensure that USAP access permissions for SHIELD users are approved and documented.
- NSF ensure that USAP strengthens controls so access permissions for the POLAR ICE users are recertified and documented periodically.
- USAP document the date of review of data center access logs as part of the evidence to show that the logs are reviewed quarterly.
- USAP ensure that the datacenter access list is reviewed periodically and the details of the review documented.

13-06 USAP needs to improve assessment and authorization controls (New)

We noted the following weaknesses in USAP's Assessment and Authorization controls. Specifically, we noted the following:

- There was no evidence that all weaknesses identified in the USAP Security Assessment Reports, including items from the SAMR (Security Assessment Management Review workbook), are provided to the Authorizing Official (AO) or included in the plan of actions and milestones (POA&M) or in any other updates periodically provided to the AO.
- During the FY2013 audit, we noted that USAP has not completed corrective actions for NFR 12-04. USAP has documented an Acceptance of Residual Risk (AORR) for EOS subsystems that did not meet NSF password requirements and for EOS systems that used shared accounts; however there was no evidence that the AO explicitly accepted the risk.

Recommendations (13-06)

We recommend that:

- NSF ensure that all weaknesses identified in the USAP Security Assessment Reports, (SARs) including items from the SAMR, are provided to the designated NSF Authorizing Official so that he or she can decide which risks to accept.
- USAP ensure that the NSF Authorizing Official is provided with periodic security status reports to demonstrate that the effectiveness of security controls employed within and inherited by the system is monitored and communicated.
- NSF ensure that password settings for USAP EOS components are consistent with NSF password and account lockout requirements. Alternatively, if NSF proceeds with accepting the associated risks for EOS, the Authorizing Official should approve the Acceptance of Residual Risk (AORR) document.
- NSF ensure that individual accounts are used for all USAP EOS users or establish compensating controls to ensure individual accountability for actions performed with shared accounts. Alternatively, if NSF proceeds with accepting the associated risks for EOS, the Authorizing Official should approve the AORR document.

13-07 NSF Security Assessment Reports (SARs) need to identify consistently all assessed risks (New)

We noted the following weaknesses in NSF's Assessment and Authorization controls:

The NSF Network, FAS, Research.gov, and eJacket SARs, which document the risk assessments, did not include all the **risks** that are applicable to the systems. Specifically,

- The SARs did not include 3 NSF open POA&Ms that are due to be closed on 9/30/2013. The open POA&Ms include Finding Nos. 12-07, 12-09, and 12-10.
- The SARs did not include the systemic risks associated with the kinds of vulnerabilities identified over time in weekly NSF vulnerability scans, such as computers with missing patches that have not yet been remediated despite availability of patches to address the vulnerabilities after an extended period of time. While SARs are not expected to be

updated for each and every new vulnerability as found through ongoing scanning, they should identify where such unremediated vulnerabilities continue to be found over time

Recommendations (13-07)

We recommend that:

- NSF ensure the Risk Assessments documented in the Security Assessment Reports for NSF Network, FAS, Research.gov, and eJacket are updated to include all risks applicable to the systems, including those that may be derived from open vulnerabilities noted in POA&Ms and vulnerability scans.
- NSF ensure the Assessment and Authorization process for NSF Network, FAS, Research.gov, and eJacket includes consideration of all open risks noted in the POA&Ms and identified over time through ongoing vulnerability scans.

ML-13-08 *(New)* Weaknesses in NSF Role-based IT Security Awareness and Training

We noted the following weaknesses in NSF's security awareness and role-based training controls:

- Documentation was not available to show that Security Awareness Training was completed and Rules of Behavior were signed for 3 of the 25 individuals that we tested.
- NSF does not provide role-based security training for Authorizing Officials, system owners, security control assessors and IT Security Officers.

NSF is still in the process of implementing controls to strengthen their process for monitoring users to ensure that they complete the annual security awareness training. Additionally, NSF provides role based security training for system administrators; however the role based training program has not been updated to include training requirements for additional individuals with significant IT security responsibilities elsewhere in the security assessment and authorization process, including Authorizing Officials, System Owners, Security Control Assessors, and IT Security Officers.

Weakness in security awareness and role-based training controls increases the risk that users may not be aware of their responsibilities for protecting NSF systems and data. This could result in unauthorized access to NSF systems and data.

Recommendations (ML-13-08):

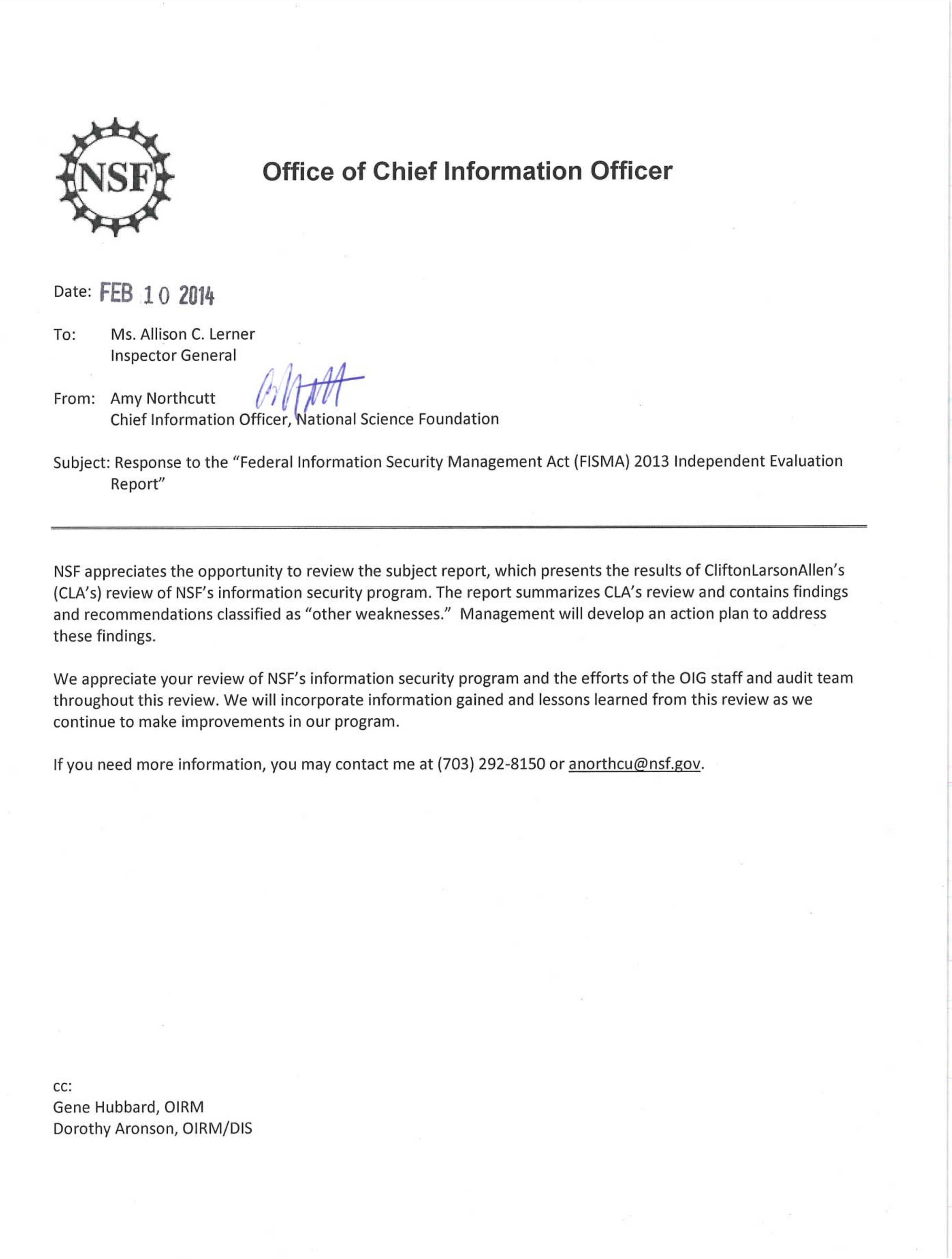
We recommend that:

- NSF strengthen controls to ensure that annual security awareness training is completed and rules of behavior forms are signed and maintained for all employees and contractors before they obtain access to NSF systems.
  NSF ensure Authorizing Officials, System Owners, Security Control Assessors, and IT Security Officers complete appropriate role-based security training.

VII. OTHER INFORMATION COMMUNICATED TO MANAGEMENT

We conducted internal and external vulnerability assessments and penetration testing on USAP systems located in Denver, Colorado in July, 2013, in accordance with formal Rules of Engagement agreed upon with NSF management. We performed this testing to identify possible weaknesses in USAP'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, accessible hosts residing on internal USAP networks and conducted overt and covert vulnerability assessments on IP addresses in use. We sought approval prior to exploiting discovered vulnerabilities, but did not conduct additional testing based on the identified exploitable vulnerabilities. We then advised management in a separate document on corrective actions to strengthen its environment further.

VIII. EXHIBIT A – AGENCY COMMENTS



Office of Chief Information Officer

Date: FEB 10 2014

To: Ms. Allison C. Lerner
Inspector General

From: Amy Northcutt
Chief Information Officer, National Science Foundation

Subject: Response to the "Federal Information Security Management Act (FISMA) 2013 Independent Evaluation Report"

NSF appreciates the opportunity to review the subject report, which presents the results of CliftonLarsonAllen's (CLA's) review of NSF's information security program. The report summarizes CLA's review and contains findings and recommendations classified as "other weaknesses." Management will develop an action plan to address these findings.

We appreciate your review 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.

If you need more information, you may contact me at (703) 292-8150 or anorthcu@nsf.gov.

cc:
Gene Hubbard, OIRM
Dorothy Aronson, OIRM/DIS