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

MEMORANDUM

DATE: January 12, 2013

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

FROM: Allison C. Lerner /s/
Inspector General

SUBJECT: Federal Information Security Management Act FY 2012 Independent Evaluation Report – OIG Report Number 13-2-003

Attached is the Federal Information Security Management Act of 2002 (FISMA) FY 2012 Independent Evaluation Report. In accordance with Office of Management and Budget (OMB) Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, we previously provided the Inspector General Section of NSF's FY 2012 FISMA Report, which was submitted through the OMB automated reporting tool on November 15, 2012.

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

- NSF needs to improve its patch management process for the timely resolution and mitigation of logical security vulnerabilities.
- NSF needs to correct the United States Antarctic Program's (USAP) Certification and Accreditation documentation process to include required elements.
- 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.

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 CliftonLarsonAllen 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
G.P. Peterson, Chair, Audit and Oversight Committee
Kathryn Sullivan, Senior Advisor, OD
Eugene Hubbard, Director, OIRM
Amy Northcutt, Chief Information Officer
Kelly K. Falkner, Acting Director, OD/OPP
Martha Rubenstein, Director and CFO, BFA
Susanne LaFratta, Senior Advisor, OD/OPP

NATIONAL SCIENCE FOUNDATION

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

2012 INDEPENDENT EVALUATION REPORT

January 22, 2013

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

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) 2012 Office of Inspector General (OIG) response to Office of Management and Budget (OMB) Memorandum M-12-20, "*FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*" and FY 2012 FISMA Independent Evaluation Report, detailing 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. OMB Memorandum M-12-20 provides instructions for meeting the FISMA reporting requirements.

We completed our response to OMB Memorandum M-12-20 based on our independent evaluation as of September 30, 2012, 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.

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 (dated January 9, 2013) to this FISMA 2012 Independent Evaluation Report, presented in Exhibit – A. We did not audit management's response, and therefore do not provide any conclusion on it.

We appreciate the opportunity to assist your office with these reports. Should you have any questions, please call [redacted].

CliftonLarsonAllen LLP

Calverton, Maryland
January 22, 2013

TABLE OF CONTENTS

Page

TRANSMITTAL LETTER i

I. EXECUTIVE SUMMARY 2

II. BACKGROUND 2

III. OBJECTIVES 3

IV. SCOPE AND METHODOLOGY 3

V. DETAILS OF RESULTS 4

A. Prior Year Results 4

B. Current Year Results 5

VI. FINDINGS AND RECOMMENDATIONS 5

VII. OTHER INFORMATION COMMUNICATED TO MANAGEMENT 14

VIII. EXHIBIT A – AGENCY COMMENTS 15

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) 2012 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 2011 Independent Evaluation Report included five 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 now that the results of the Antarctic Support Contract re-competition have been determined. Two of the findings related to NSF's prompt revocation of access, and the security of NSF's network topology remain open. One finding, on the NSF Assessment and Authorization (A&A) documentation process, has been closed; however, a new but related issue has been reported in FY 2012.

We are reporting four new findings in FY 2012, one relating to the patch management process, one relating to the USAP A&A documentation process (mentioned above), one relating to the USAP System Security Plan, and one relating to USAP enforcement of NSF's password and account management policies.

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 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 CLA to conduct NSF's FY 2012 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 9, 2012.

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 and Organizations – Special Publication (SP) 800-53, Rev. 3* for specification of security controls; NIST SP 800-37,Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems;* and SP 800-*53A Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations* 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 2011 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)
- Research.gov
- NSF Network LAN
- USAP Enterprise Operations System Application (EOS)
- 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, 2012 to September 30, 2012 at NSF's headquarters in Arlington, Virginia. We also performed testing of the USAP Enterprise Operations System Application (EOS) in July 2012 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, 2012.

V. DETAILS OF RESULTS

A. Prior Year Results

The FY 2011 Independent Evaluation Report identified five (5) 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 2011 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	10-04	NSF needs to remove timely the information technology (IT) accounts for separated employees and contractors.	Reissued
4	10-05	NSF's need to improve security of its network topology as the present design poses a potential security weakness.	Reissued
5	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 in the SAR.	Closed

B. Current Year Results

The following table summarizes the reissued and new findings noted as of September 30, 2012:

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
12-01	NSF needs to improve its patch management process for the timely resolution and mitigation of logical security vulnerabilities.	New
12-02	NSF needs to correct the USAP C&A documentation process to include required elements.	New
12-03	USAP needs to review its System Security Plan for consistency with NIST requirements.	New
12-04	USAP needs to enforce NSF's password and account management policies at USAP.	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 through the United States Antarctic Program (USAP) is the principal responsibility of the Office of Polar Programs (OPP) 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 operational support, OPP 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 to process transactions with 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.

In FY 2010, OPP 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 the fourth quarter of FY 2014. In FY 2012, OPP began working with its new contractor, Lockheed Martin ASC (ASC), to determine the best strategy to replace AREV.

Federal guidelines provided in NIST Special Publication SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products provide 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."

The inadequate and antiquated processing environment may expose system resources to intentional and unintentional loss or impairment, destruction, or malicious damage. Specifically, in this DOS-based environment, a user with access privileges on one application in this suite can access several other applications, which may be outside his/her scope of duties. This may result in unauthorized access to data or unapproved data modification and/or deletion. USAP operations may be adversely impacted as a result. Additionally, 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.

Higher order USAP mission priorities have delayed the development of a new scalable and supportable business solution with the effect that the existing solution and most of its components have become antiquated and difficult to support, which potentially exposes system resources to intentional and unintentional loss or impairment, destruction, or malicious damage.

Recommendation (06-01)

We repeat our FY 2006 – 2011 recommendation that OPP 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.

In FYs 2006, 2007, 2008, 2009, 2010, and 2011 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 the event that 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.

NIST SP 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. The three types of alternate sites may be categorized in terms of their operational readiness. Based on this factor, sites may be identified as cold sites, warm sites, hot sites, mobile sites, and mirrored sites.

NIST SP 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 USAP's Denver operating location.

Unavailability of the network support infrastructure may result in loss of dedicated network communications. Although scientific grantees in the Antarctic backup and store the results of their scientific experiments on physical media, with an extended network disruption, the availability of scientific results could be delayed. Additionally, 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 prevent USAP from carrying out its mission.

In FY 2010, OPP completed its strategic planning to mitigate the potential risk of interruption to USAP program operations. However, implementation of the plan was delayed pending finalization of the contract competition and award to the new vendor. NSF awarded the new contract to ASC in FY 2012. OPP is now working with ASC to refine its strategy and determine modalities for implementation.

Recommendation (06-02)

We repeat our FY 2006 – 2011 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 information technology (IT) accounts for separated employees on a timely basis. (Re-Issued)

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 removed timely or deleted upon the termination of the users' employment at NSF. Two employee accounts were removed 34 days and one 30 days after separation. We noted similar weaknesses in FY 2011 and FY 2012. This reflects a continuation of a prior year issue. Therefore, we are repeating this finding for FY 2012.

NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations,* stipulates the following control:

> The organization, upon termination of individual employment:
> - Terminates information system access;
> - Retrieves all security-related organizational information system-related property; and
> - Retains access to organizational information and information systems formerly controlled by terminated individual.

The Division of Information Systems (DIS) was not notified of employee and contractor separations timely. Additionally, a central repository was not in place for maintaining contractor clearance forms. Finally, the clearance process implemented October 3, 2011, was not consistently followed.

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.

We also recommend that NSF strengthen controls to ensure that clearance forms are properly completed and maintained for terminated employees and contractors.

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 maintains a high-speed research network separate from its main network. Although NSF has implemented management, operational and technical controls to protect its high-speed network, these controls do not provide adequate content filtering, port and service protection from hostile outsiders or the ability to react to brute force attempts to compromise these systems residing on this public facing network.

Based on NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, as part of a defense-in-depth protection strategy, the organization should consider 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 confidentiality integrity and availability of computer systems and data. There remains risk associated with the absence of network filtering which results in limited source IP address protection capability. Application specific attack identification and response remain absent from the current configuration, which could result in system compromise and lead to loss of confidentiality, integrity, and availability of systems and data.

Recommendation (10-05)

While NSF has implemented some security domains to protect much of the publically accessible assets, some network segments designated as High Speed research networks remain generally unprotected. We recommend that NSF develop protocol and application specific filters to protect all publicly available services.

12-01 NSF needs to improve its patch management process for the timely resolution and mitigation of logical security vulnerabilities (NEW)

We performed vulnerability scanning of NSF's network assets to include servers, workstations, appliances, and infrastructure components. Our analysis compared the results of vulnerabilities reported by the scans from FYs 2010 and 2011 to the current year (FY 2012). During our testing, we discovered a measurable increase of reported critical and high severity vulnerabilities compared to past years. While NSF has demonstrated a robust patch management process, this analysis demonstrates a continuing trend of increased growth of detected vulnerabilities within the network. In addition, the quantity of reported medium severity vulnerabilities has increased notably over the same period of time. Our analysis of the scan data has shown an increase in the total vulnerabilities:

- Critical vulnerabilities increased by 5 or nearly 10% from the prior year;
- High vulnerabilities increased by 110 or nearly 129% from the prior year;
- High vulnerabilities increased by 149 or nearly 323% from 2010;
- Medium vulnerabilities increased by 4,616 or nearly 261% from 2011.

Based on NIST SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program:*

> Timely patching of security issues is generally recognized as critical to maintaining the operational confidentiality, integrity and availability of information technology (IT) systems. However, failure to keep operating system and application software patched is one of the most common issues identified by security and IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches and ensure proper deployment in a timely manner. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed before the outbreaks. Indeed, the moment a patch is released, attackers make a concerted effort to reverse engineer the patch swiftly (measured in days or even hours), identify the vulnerability, and develop and release exploit code. Thus, the time immediately after the release of a patch is ironically a particularly vulnerable moment for most organizations due to the time lag in obtaining, testing, and deploying a patch.
>
> To help address this growing problem, it is recommended that all organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches.
>
> NIST recommends that Federal agencies implement the following recommendations to assist in patch and vulnerability management.
>
> - Organizations should create a patch and vulnerability group (PVG) to facilitate the identification and distribution of patches within the organization.
> - Organizations should use automated patch management tools to expedite the distribution of patches to systems.
> - Organizations should deploy enterprise patch management tools using a phased approach.
> - Organizations should assess and mitigate the risks associated with deploying enterprise patch management tools.
> - Organizations should consider using standardized configurations for IT resources.
> - Organizations should consistently measure the effectiveness of their patch and vulnerability management program and apply corrective actions as necessary.

Recommendation (12-01)

NSF should improve its patch management process to eliminate the growth in vulnerabilities requiring vendor patches and updates. As the number of vulnerabilities in the public domain increases, the effort to address and remediate these vulnerabilities should parallel this growth to maintain the current level of accepted risk.

12-02 NSF needs to correct the USAP C&A documentation process to include required elements. (NEW)

NSF implemented a Security Assessment Management Review (SAMR) process to ensure that security assessment results were documented and reported to management. However, there were control deficiencies identified in the Enterprise Operations System (EOS) Authorization Document that did not appear in the Security Assessment Report (SAR) for the system. Additionally, there were control deficiencies identified in the EOS Authorization Document that did not appear in the SAMR workbook.

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 (12-02)

We recommend that NSF enhance the SAMR process to include all control deficiencies in A&A documents: the SAMR, SAR, and Authorization Document to ensure management is provided all information on control risk.

12-03 NSF needs to review its System Security Plan for consistency with NIST requirements. (NEW)

The NSF USAP certification and accreditation (C&A), now Assessment & Authorization (A&A) review process was incomplete and inaccurate. The A&A documentation did not adequately address compliance with the requirements in NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems.* We noted the following weaknesses in the accreditation packages for the NSF USAP EOS system:

- The USAP EOS System Security Plan (SSP) was not fully consistent with NIST SP 800-18 requirements. Specifically, we noted the following:
    - The interconnection table did not identify the following required information:
        - Name of system;
        - Type of interconnection (Internet, Dial-Up, etc.);
        - Authorizations for interconnection (MOU/MOA, ISA);
        - Date of agreement;
        - FIPS 199 Category;
        - Certification and accreditation status of system; and
        - Name and title of authorizing official(s).
    - The security plan does not accurately identify whether controls were implemented. Specifically, we noted that the EOS Authorization Support Document, which supplements the security plan, identified many instances of controls that were other than satisfied; however, the control status in the security plan stated that the controls were satisfied.

- The document was not approved by the authorizing official nor was a designated approval authority identified in the plan.

NIST SP 800-18 states:

> A designated system owner must be identified in the system security plan for each system. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. The assignment of a system owner should be documented in writing and the plan should include the following contact information..."
>
> In this section, for each interconnection between systems that are owned or operated by different organizations, provide the following information concerning the authorization for the connection to other systems or the sharing of information:
> - Name of system;
> - Organization;
> - Type of interconnection (Internet, Dial-Up, etc.);
> - Authorizations for interconnection (MOU/MOA, ISA);
> - Date of agreement;
> - FIPS 199 Category;
> - Certification and accreditation status of system; and
> - Name and title of authorizing official(s).

Recommendation (12-03)

We recommend that NSF update the EOS SSP to be consistent with NIST 800-18 requirements.

12-04 NSF needs to enforce its password and account management policies. (NEW)

We noted the following weaknesses in the USAP EOS system's identification and authentication controls for information systems:

- There were shared user ids and passwords used to access USAP EOS components. Specifically, we noted the following:
  - Five people share the McmAdmin account used to administer the Black Island Telecommunications Facility;
  - Two people share the administrator account for the South Pole Land Mobile Radio;
  - Four people share the administrator login for the McMurdo Pager System; and
  - The root login and the teradm account were shared Linux accounts used to administer the TeraScan system.

- There was one active generic account identified on the EOS system. Specifically, we noted that the built-in administrator account had not been renamed for the McMurdo High Frequency Radio system or the South Pole Land Mobile Radio system. NSF renamed this account before the end of our fieldwork; therefore, we did not issue any related recommendations.

- EOS password settings were not consistent with NSF policy. Specifically, we noted the following:
    - Aeronautical Fixed Telecommunications Network was configured with a minimum password age of zero days instead of one day.
    - Black Island Telecommunication Facility was configured with a minimum password age of zero days instead of one day. Additionally, the password length was set to eight instead of 12 characters.
    - Password settings for South Pole Land Mobile Radio were not consistent with NSF Policy. Specifically, we noted the following:
        - The system was configured with a minimum password age of zero days instead of one day;
        - Passwords were set to expire in 37201 days instead of 60 days;
        - Password length was set to zero instead of 12 characters;
        - Password complexity requirements were disabled;
        - Account lockout controls had not been configured; and
        - The system had not been configured to prevent users from reusing their last 24 passwords.
    - Password settings for McMurdo High Frequency Radio System were not consistent with NSF Policy. Specifically, we noted the following:
        - The system permits blank passwords;
        - Password complexity requirements were disabled;
        - Account lockout controls had not been configured; and
        - The system had not been configured to prevent users from reusing passwords.
    - Password settings for South Pole High Frequency Radio System were not consistent with NSF Policy. Specifically, we noted the following:
        - The system was configured with a minimum password age of zero days instead of one day;
        - Password length was set to zero instead of 12 characters;
        - Password complexity requirements were disabled;
        - Account lockout controls had not been configured; and
        - The system had not been configured to prevent users from reusing their last 24 passwords.
    - The Terascan system had not been configured to prevent users from reusing their last 24 passwords.

USAP's process for reviewing the Assessment & Authorization (A&A) process was not robust enough to note deficiencies in controls and non-compliance with policy.

NSF Bulletin No. 08-04 – NSF Password Policy includes the following:

4.0 Policy:

- The use of a valid and current password is required for access to all NSF automated systems and applications for which user accountability is required.
- Use of two-factor authentication (e.g., a method of access requiring two forms of authentication, such as a pin and SecurID token) is required for remote access to NSF automated systems and email.
- Workstation screensavers with passwords must be used.
- Generic or group passwords must not be used.

- All NSF personnel are responsible for taking appropriate steps to create strong passwords.
- Network passwords must contain at least twelve characters and must not repeat any of the previous 24 passwords.
- Application passwords must contain at least eight characters.

"Network and application passwords:

- Must contain at least three of the following character sets: upper case English; lower case English; numeric characters; and "special characters," which are all non-alphanumeric characters found on a standard keyboard (e.g., # & % ! ? @ (.);
- Must not contain any simple pattern of letters or numbers such as "aaabbbcc" or "qwertyui;"
- Must not be easy to guess (e.g., "my family name");
- Must not be a word in any language, slang, jargon, or found in a dictionary."

Network passwords must be changed every 60 days; you will receive a reminder 14 days prior to network password expiration. Application passwords must be changed every 90 days. Passwords for Personal Digital Assistants must be changed every 180 days.

The National Science Foundation Information Security Handbook states that "...Information systems enforce a limit of five (5) consecutive invalid login attempts by a user; when this limit is met or exceeded, information systems will be unavailable for 15 minutes, after which the user may attempt to login."

Recommendation (12-04)

We recommend that:

- NSF ensure that password settings for EOS components are consistent with NSF password and account lockout requirements.
- NSF ensure that individual accounts are used for all EOS users, or NSF establish compensating controls to ensure individual accountability for actions performed with shared accounts.

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.

VIII. EXHIBIT A

Office of Chief Information Officer

Date: JAN 09 2013

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) 2012 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 eight findings and recommendations classified as "other weaknesses." Management accepts six of the findings and will develop an action plan to address these findings.

We appreciate the collaboration of your office and CLA in performing this year's review; we do though have some concerns about two of the findings as they are described in CLA's report. Specifically:

1. We believe finding 10-05 does not constitute a repeat finding related to NSF's network design and instead should be reissued as a separate finding. When initially issued, finding 10-05 was based on the internal network where externally-facing services (e.g., e-mail, domain name services, and web servers) were protected by a single layer of firewalls. As stated in the FY11 Independent Evaluation Report, NSF added additional layers of firewalls to create a secure demilitarized zone (DMZ) and separate publicly facing services. NSF considers finding 10-05 and its recommendation(s) regarding the internal network addressed and closed.

   The re-issued finding focuses on the High Speed Network, our research network which is physically separate from NSF's internal network. The research network is a limited purpose capability used for Internet2 connectivity to universities and research institutions, with access limited to technical operators and approximately 20 NSF program staff. This network is protected by numerous management and operational security controls, including monitoring services and web content filtering, and it does not store sensitive information. The observations that drove issuance of the finding do not reflect the lack of technical controls to protect services, but are due to configuration management anomalies that have since been corrected. We will develop an action plan to address this finding.

2. NSF believes finding 12-01 on NSF's vulnerability management program does not fully consider the context of NSF's security controls and the mitigating factors used to address potential vulnerabilities. NSF disagrees with CLA's statement that the increase in vulnerabilities indicates NSF's "patch management process is not as

robust as prior years." NSF has a robust, risk-based, proactive and mature vulnerability management program that focuses on comprehensive processes including network scanning, penetration testing, patch management and remediation, as acknowledged in the finding. In fact prior to the review, NSF had already implemented the NIST recommendations for patch and vulnerability management that CLA includes in their finding description.

NSF believes the inclusion of scan data showing an increased number of vulnerabilities does not provide insight into whether the security risk to the Foundation has increased accordingly. These point-in-time numbers do not consider context related to changes in the number of devices, management acceptance of risk, or mitigating controls that would reduce the possibility of a vulnerability being exploited. Most significantly, the raw numbers do not consider false positives – for example, cases where the vulnerabilities do not actually exist for a service (e.g., the service has been turned off). Without detailed analysis of the scan data and consideration of the context described above, there is no evidence that NSF systems could have been compromised as a result of the identified vulnerabilities.

NSF is aware the number of external threats continues to increase at a rapid pace. NSF monitors open source intelligence and government sources to ensure we adequately address threats that pose a real risk to NSF computing infrastructure. NSF continues to strengthen its vulnerability management process and will continue the momentum to ensure that an already robust process becomes better.

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