United States Department of State
and the Broadcasting Board of Governors

Inspector General

NOV 12 2013

SENSITIVE BUT UNCLASSIFIED

TO: Management Control Steering Committee

FROM: OIG – Steve A. Linick

SUBJECT: *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (AUD-IT-14-04)

(U) Attached is an Office of Inspector General (OIG) report discussing significant and recurring weaknesses found by OIG in the Department of State (Department) Information System Security Program over the past three fiscal years (FY 2011-13).

(SBU) Recently, OIG issued its annual report for FY 2013 concerning the Department's compliance with the Federal Information Security Management Act (FISMA). [Redacted] (b)(5) [redacted] Multiple authorities, including FISMA, the Office of Management and Budget (OMB), and the *Foreign Affairs Manual,* require immediate corrective action of any significant deficiency as well as the external reporting of a material weakness pursuant to the FMFIA.

(U) Although OIG identified similar significant deficiencies in its annual FISMA reports for FY 2011 and FY 2012, the Department has yet to report externally on or correct many of the existing significant deficiencies thereby leading to continuing undue risk in the management of information. Recent, highly-publicized cyber security breaches involving highly-sensitive data illustrate the need to better manage the Department's information security risks.

(U) OIG is making three recommendations to Department management, through the Management Control Steering Committee: (1) elevate the existing FISMA significant deficiency designation of the Information System Security Program to an FMFIA material weakness and include the finding in the Department's FY 2013 FMFIA annual statement of assurance; (2) direct the Bureau of Information Resource Management to develop, on a timely basis, a comprehensive corrective action plan to address the existing FISMA significant deficiency designation of the Information System Security Program; and, (3) direct the Office of the Chief Information Officer to employ the services of the National Security Agency to conduct independent penetration testing to further evaluate the Information System Security Program and outline a range of technical and procedural countermeasures to reduce risks.

Address correspondence to: U.S. Department of State, Office of Inspector General, Washington, D.C. 20522-0308

(U) OIG would appreciate a written response to this report from the Management Control Steering Committee and information on actions taken or planned for the report's three recommendations. The response should indicate agreement or disagreement with each recommendation. It is not necessary to provide detailed explanations of implementation efforts at this time.

(U) Comments received within 14 calendar days of the date of this Management Alert will be reprinted as an appendix to the attached report. In addition to the hard-copy response, please provide an electronic copy of the final response to Norman P. Brown, Acting Assistant Inspector General for Audits, at brownnp2@state.gov. The Management Alert and the final report may be posted to the OIG Internet and Intranet Web sites.

(U) If you have any questions, please contact Mr. Brown or Jerry Rainwaters, Information Technology Division Director, at rainwatersj@state.gov.

Attachment: As stated.

cc: D(B) – William J. Burns
C – Heather A. Higginbottom
S – David Wade
M – Patrick F. Kennedy

A – Joyce A. Barr
BP – Barbara Retzlaff
CA – Janice Jacobs
CGFS – James Millette
CGFS/DCFO – Chris Flaggs
CGFS/DCFO/MC – Carole Clay
CGFS/DCFO/MC – Michelle Carter
DGHR – Hans Klemm, Acting
DS – Gregory B. Starr
EAP – Daniel Russel
ECA – Lee Satterfield, Acting
INL – William R. Brownfield
IRM – Steven C. Taylor
L – Richard Visek
OBO – Lydia Muniz
PM – Thomas Kelly, Acting
PRM – Anne Richard

(U) OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program

(U) The Department of State (Department) is entrusted to safeguard sensitive information, which is often the target of terrorist and criminal organizations. Cyber attacks against Government organizations appear to be on the rise,[1] including state-sponsored efforts to exploit U.S. Government information security vulnerabilities.[2] The Department is responsible for preserving and protecting classified information vital to the preservation of national security in high risk environments across the globe.[3] The Department also undertakes significant numbers of financial and other transactions, including, for instance, the daily collection of millions of dollars in consular fees.[4] In addition, the Department maintains records on approximately 192 million current passports,[5] which contain such sensitive personally identifiable information (PII) as dates of birth and social security numbers. To protect this information, the Department must ensure that its Information System Security Program and management control structure are operationally effective.

(SBU) The Federal Information Security Management Act (FISMA)[6] requires the Department's Office of Inspector General (OIG) to conduct annual evaluations of the Department's information security programs. [Redacted] (b)(5) [redacted] Areas of high and most immediate risk have led OIG, as well as the Government Accountability Office (GAO), to issue six reports concerning information security during the period FY 2011 through FY 2013:

- **(U)** *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain* (GAO-11-149, July 2011)
- **(U)** *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, November 2011)
- **(U)** *Audit of Department of State Access Controls for Major Applications* (AUD/IT-12-44, September 2012)
- **(U)** *Audit of Department of State Information Security Program* (AUD-IT-13-03, November 2012)

---

[1] **(U)** "[Department of Energy] data breach came after warnings," *Federal Computer Week: The Business of Federal Technology*, published on Feb. 5, 2013, and accessed on Aug. 20, 2013, http://fcw.com/Articles/2013/02/05/DOE-data-breach.aspx.

[2] **(U)** Tom Vanden Brook, "Cyber attack? What cyber attack?" *USA Today*, published on Aug. 19, 2013, and accessed on Sept. 13, 2013, http://www.usatoday.com/story/nation/2013/08/19/china-cyber-attack-pentagon/2671579/.

[3] **(U)** For instance, in September 2012, a Department compound in Libya was attacked, resulting in the death of the U.S. Ambassador to Libya and other U.S. Government personnel. In August 2013, the Department directed the closure of 22 diplomatic posts in the Middle East and North Africa because of credible terrorist threat.

[4] **(U)** United States Department of State, Fiscal Year 2012 Agency Financial Report: Delivering Results to the American People, Notes to Principal Financial Statements, Earned Revenues, p. 119.

[5] **(U)** *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)* (AUD/IP-08-29, July 2008).

[6] **(U)** Pub. L. No. 107-347, title III.

- **(SBU)** *Inspection of the Bureau of Information Resource Management, Office of Information Assurance* (ISP-I-13-38, July 2013)
- **(U)** *Audit of Department of State Information Security Program* (AUD-IT-14-03, October 2013)[7]

(U) As discussed in more detail below, the reports have found recurring weaknesses in six areas: Authority to Operate (ATO), Baseline Controls, Scanning and Configuration Management Controls, Access Controls, Cyber Security Management, and Risk Management and Continuous Monitoring Strategies.

(U) Because these recurring weaknesses continue to put at significant risk the integrity of the Department's overall information security program, OIG has designated the collective weaknesses as a significant deficiency, as defined by the Office of Management and Budget (OMB) guidance, in FY 2011, FY 2012, and now in FY 2013.

(U) OMB defines a Significant Deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and other agencies must be notified and immediate or near-immediate corrective action must be taken."[8] The foregoing is also consistent with the *Foreign Affairs Manual's* definitions of significant deficiency[9] and material weakness[10] under the Federal Managers Financial Integrity Act[11] (FMFIA), as well as FISMA reporting requirements.[12]

(U) To date, the Department has not externally reported these weaknesses, nor has it remediated the identified vulnerabilities and risks. In its FY 2011 annual FISMA report, OIG concluded that the collective control weaknesses identified in that report represented "a significant deficiency ... to enterprise-wide security including the Department's financial systems." The report further noted that a compounding factor was that "that the Department had not taken corrective action to remediate all of the control weaknesses identified in the FY 2010 FISMA report."[13] The significant deficiency finding should have been reported outside the Department, specifically as a material weakness in the FMFIA statement of assurance. However, the Department, through

---

[7] (U) *Audit of Department of State Information Security Program* (AUD-IT-14-03, Oct. 2013).
[8] (U) OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" at 26 (Sept. 27, 2012), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf.
[9] (U) Per 2 FAM 021.3, "Definitions," a FMFIA significant deficiency is "a deficiency, or combination of deficiencies, that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives."
[10] (U) Per 2 FAM 021.3, "Definitions," a FMFIA material weakness is constituted by "[s]ignificant deficiencies [that] the agency head determines to be significant enough to report outside of the agency."
[11] (U) Pub. L. No. 97-255, Sept. 8, 1982.
[12] (U) Pub. L. No. 107-347, title III.
[13] (U) Evaluation of Department of State Information Security Program (AUD/IT-12-14, November 2011), p. 6, available at http://oig.state.gov/documents/organization/182933.pdf.

the Management Control Steering Committee, disagreed and determined that the FISMA significant deficiency was only an FMFIA "reportable condition,"[14] not an FMFIA material weakness,[15] and therefore not subject to mandatory external reporting.

(U) In its FY 2012 annual FISMA report, OIG again concluded that "[c]ollectively, the control weaknesses identified, along with the weaknesses identified by OIG in the [September, 2012] report *Audit of Department of State Access Controls for Major Applications*,[[16]] represent a significant deficiency to enterprise-wide security, including the Department's financial system." The report also again noted that a compounding factor was "that the Department had not taken corrective action to remediate all of the control weaknesses identified in the FY 2011 FISMA report."[17] In response to this report, the Department again disagreed; the Department's 2012 Agency Financial Report states that the Department acknowledged the weaknesses identified by OIG but did not agree that the findings identified rose to the FMFIA significant deficiency level, which presumably would require external reporting as an FMFIA material weakness.[18]

(U) Based on audit work recently completed,[19] the FY 2013 FISMA report again identified the collective information system security control weaknesses as a FISMA significant deficiency that requires immediate corrective action, as well as external disclosure because OIG continues to regard the deficiency as an FMFIA material weakness.

(U) Recurring Significant Deficiency Findings, FY 2011–2013

(U) OIG's FY 2012 FISMA report identified 14 uncorrected findings from the FY 2011 FISMA report. OIG's FY 2013 FISMA report identifies 20 uncorrected findings identified in the FY 2012 FISMA report. OIG regards the following six areas to be of highest risk.

(U) Absence of Current Authority to Operate in Multiple Information Security Systems

(SBU) [Redacted] (b)(5) [redacted][21] The ATO serves as management's official decision to authorize operation of an information system. It also provides for the implementation of an agreed-upon set of security controls in order to mitigate risk.

---

[14] (U) According to 2 FAM 021.3, the term FMFIA "significant deficiencies" was formerly called "reportable conditions." This change was instituted for the purpose of FMFIA reporting after December 15, 2009, per Office of Management and Budget (OMB) Memorandum 09-33.
[15] (U) Management Control Steering Committee Minutes, Nov. 10, 2011, p. 2.
[16] (U) Available at http://oig.state.gov/documents/organization/200368.pdf.
[17] (U) Audit of Department of State Information Security Program (AUD-IT-13-03, November 2012), p. 6-7, available at http://oig.state.gov/documents/organization/202261.pdf.
[18] (U) United States Department of State, Fiscal Year 2012 Agency Financial Report: Delivering Results to the American People, Management's Discussion and Analysis, Internal Controls, Financial Management Systems, p. 57.
[19] (U) OIG has completed the fieldwork for the FY 2013 FISMA audit and issued in July 2013 an inspection report, *Inspection of the Bureau of Information Resource Management, Office of Information Assurance* (ISP-I-13-38, July 2013).
[20] (U) *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, Nov. 2011).
[21] (U) National Institute of Standards and Technology IR7298, Revision 1, *Glossary of Key Information Security Terms*, Feb. 2011.

(SBU) In addition, [Redacted] (b)(5) [redacted]

(SBU) In its FY 2012 FISMA report, OIG again noted that the ATO for OpenNet had not been renewed. [Redacted] (b)(5) [redacted]

(SBU) In its FY 2013 FISMA report, [Redacted] (b)(5) [redacted]

(SBU) When systems are allowed to operate without a [redacted] [Redacted] (b)(5) [redacted]

(U) Absence of Baseline Controls

(SBU) In its FY 2011 FISMA report,[22] [Redacted] (b)(5) [redacted] Such controls are the starting point for the security control selection process, which are chosen based on the severity of the security category and associated risk.[23] [Redacted] (b)(5) [redacted]

(SBU) In its FY 2012[24] FISMA reports, [Redacted] (b)(5) [redacted]

[22] **(U)** *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, Nov. 2011).
[23] **(U)** Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, Feb. 2004; FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* Mar. 2006; National Institute of Standards and Technology Special Publication 800-53, rev. 3, *Recommended Security Controls for Information Systems*, Aug. 2009.
[24] **(U)** *Audit of Department of State Information Security Program* (AUD-IT-13-03, Nov. 2012).

(U) Ineffective Security Scanning and Configuration Management Controls

(SBU) In its FY 2011 FISMA report, [Redacted] (b) (5) [redacted] Finally, the Bureau of Diplomatic Security did not have the administrative credentials needed for Demilitarized Zone servers[26] to perform periodic scanning.

(SBU) In its FY 2012 FISMA report,[27] [Redacted] (b) (5) [redacted]

(SBU) [Redacted] (b) (5) [redacted] GAO made related findings in its July 2011 report on information security.[29] It noted that the Department faced marked challenges in the implementation of iPost because iPost "does not provide a complete view of the information security risk to the [D]epartment" and that the Department "may not have reasonable assurance that data within iPost are accurate and complete [enough] to make risk management decisions." GAO recommended that the Department take action to improve the iPost database. [Redacted] (b) (5) [redacted]

(SBU) In its FY 2013 FISMA report, [Redacted] (b) (5) [redacted]

---

[25] **(U)** Discovery scans are used to identify accessible hosts on a computer network.

[26] **(U)** NISTIR 7298, rev.2, *Glossary of Key Information Security Terms*, May 2013, defines Demilitarized Zone (DMZ) as a perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

[27] **(U)** *Audit of Department of State Information Security Program* (AUD-IT-13-03, Nov. 2012).

[28] **(U)** iPost is a system intended to provide the capability to monitor outputs of the various network monitoring applications. It allows key personnel to monitor network, computer, and application resources; check for potential problems; initiate corrective actions; and gather performance, compliance, and security data for near real-time and historical reporting.

[29] **(U)** *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain* (GAO-11-149, July 2011).

[Redacted] (b) (5)

(U) Inadequate Access Controls

(SBU) Access controls are the risk management mechanisms and policies that restrict access to computer resources. In FY 2012, [Redacted] (b) (5) [30] Access controls are intended to provide reasonable assurance that system resources such as hardware, data files, and underlying operating systems are protected against unauthorized access, modification, or impairment from both internal and external threats.

(SBU) As of April 3, 2013, the Department's Information Technology Asset Baseline (ITAB) database identified 362 computer systems subject to FISMA reporting requirements.[31] In its FY 2012 audit fieldwork, [Redacted] (b) (5) The 2010 Wikileaks incident, in which a trusted insider illegally facilitated the release of classified Department documents without authorization, is a prime example of a trusted insider[33] who took advantage of access control weaknesses to collect and expose sensitive and classified Department information.

(SBU) In FY 2013, OIG found another instance of access control weakness. Specifically, OIG reported that 36 employees assigned to the [Redacted] (b) (5)

[30] **(U)** *Audit of Department of State Access Controls for Major Applications* (AUD/IT-12-44, Sept. 2012), available at http://oig.state.gov/documents/organization/200368.pdf.

[31] **(U)** Data obtained from Bureau of Information Resource Management/Business, Management, and Planning/Strategic Planning Office/Portfolio Management, as of April 3, 2013. The ITAB database has 3,105 entries that include systems, applications, and databases, but only 362 of those entries are identified as FISMA reportable.

[32] **(U)** A host is a computer that is connected to a Transmission Control Protocol/Internet Protocol network, including the Internet, and each host has a unique Internet Protocol address.

[33] **(U)** Julie Tate, "Judge sentences Bradley Manning to 35 years," *Washington Post*, published on Aug. 21, 2013, and accessed on Sept. 13, 2013, http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement. In August 2013, U.S. Army PFC Bradley Manning was convicted of leaking the "largest cache of classified documents in U.S. history" and was sentenced to 35 years in prison. "Bradley Manning case signals US vulnerability to 'insider' cyberattack," published on Dec. 22, 2011, and accessed on Sept. 23, 2013, http://www.csmonitor.com/USA/2011/1222/Bradley-Manning-case-signals-US-vulnerability-to-insider-cyberattack.

[Redacted] (b)(5) [34] Pursuant to 12 FAM 232, those systems can only be accessed by individuals possessing appropriate clearances. The 36 employees did not possess such clearances.

(U) Additional vulnerabilities involving access controls potentially exist throughout the Department. On August 20, 2013, the Bureau of Information Resource Management (IRM) reported that the Department had a total of 6,369[35] system administrators. According to IRM officials, system administrators are given network-wide permissions to allow them to collaboratively manage and troubleshoot issues.[36] However, such broad access by large numbers of system administrators also subjects the system to risk. The recent, highly-publicized breach of information pertaining to national security matters by Edward Snowden, a contract systems administrator, starkly illustrates the issue.[37]

(U) Cyber Security Management Weaknesses

In July 2013, OIG reported on an inspection[38] of IRM's Office of Information Assurance, which is responsible for the Department's cyber security program and collaborates with the Bureau of Diplomatic Security on information security responsibilities. OIG identified a number of conditions that required management's attention, including weaknesses ranging from organizational structure to the mishandling of certification and accreditation to absence of a strategic plan and mission statement.

(U) Risk Management and Continuous Monitoring Strategies

(U) In its FY 2013 FISMA report, OIG found deficiencies consistent with those identified in FY 2011 and FY 2012. For instance, the Department had failed to complete risk management and continuous monitoring strategies and to implement an enterprise-wide continuity of operations plan. In addition to these uncorrected deficiencies, OIG also identified new deficiencies in active directory and role-based security training.

(SBU) Although the Chief Information Officer (CIO) has verbally articulated his ideas for risk management and continuous monitoring, no documented strategy for either exists. The absence of such formal documentation, and its concomitant acceptance by Department management, can heighten the Department's vulnerability to internal and external information security threats.

---

[34] **(U)** *Audit of Department of State Information Security Program* (AUD-IT-14-03, October 2013).
[35] **(U)** According to an IRM August 2013 Excel spreadsheet, additional employees who have been granted network-wide access were not included in the total number of system administrators reported. For example, database administrators were not identified as system administrators but are also granted elevated privileges.
[36] **(U)** *Audit of Department of State Access Controls for Major Applications* (AUD/IT-12-44, Sept. 2012), available at http://oig.state.gov/documents/organization/200368.pdf.
[37] **(U)** Edward Snowden, a contracted employee working with the National Security Agency, allegedly leaked sensitive information to the media in May 2013.
[38] **(U)** *Inspection of the Bureau of Information Resource Management, Office of Information Assurance* (ISP-I-13-38, July 2013).

(SBU) In addition, [Redacted] (b)(5)

(U) Recommendations

(U) Because of the continued existence of a FISMA significant deficiency that the Department has not resolved for three fiscal years, OIG makes the following recommendations.

(U) Recommendation 1. OIG recommends that Department management, through the Management Control Steering Committee, accept OIG's findings and elevate the existing Federal Information Security Management Act significant deficiency designation of the Information System Security Program to a Federal Managers Financial Integrity Act (FMFIA) material weakness. As a material weakness, the Department must report it externally in its FY 2013 FMFIA annual statement of assurance.

(U) Recommendation 2. OIG recommends that Department management, through the Management Control Steering Committee, direct the Bureau of Information Resource Management to develop, on a timely basis, a comprehensive corrective action plan to address the existing Federal Information Security Management Act significant deficiency designation of the Information System Security Program.

(U) Recommendation 3. OIG recommends that Department management, through the Management Control Steering Committee, direct the Office of the Chief Information Officer to employ the services of the National Security Agency to conduct independent penetration testing to further evaluate the Information System Security Program and outline a range of technical and procedural countermeasures to reduce risks.

United States Department of State
Comptroller
P.O. Box 150008
Charleston, SC 29415-5008

DEC 13 2013

UNCLASSIFIED

MEMORANDUM

TO: OIG – Steve A. Linick

FROM: CGFS – James L. Millette, Chairmen of the Management Control Steering Committee

SUBJECT: Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program (AUD-IT-14-04)

The Management Control Steering Committee (MCSC) would like to thank the OIG for providing us the Management Alert on Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program dated November 12, 2013. The MCSC takes its review of internal controls seriously and values the cooperative input from the OIG. Before the final MCSC meeting on December 5, all members were provided your alert as well as IRM's response of November 25. The information provided was considered in our discussion of the level of weaknesses in this area. This memo responds to your request for a written response from the MCSC and information on actions taken or planned for your memo's three recommendations.

First, on your request for a corrective action plan, the MCSC agrees. The MCSC has had to deal with the issue of the FISMA review and the disagreement over the level of weakness in the control environment for the past few years, and we wanted to ensure that the MCSC had a better process in place to address and assess this issue in FY 2014. Specifically, the MCSC has required IRM to prepare and present a corrective action plan to the MCSC. Further, the MCSC has requested that the plan be agreed to by its members and reviewed by the OIG, that it prioritize those areas that IRM, DS and OIG agree should receive the highest attention, and that it be established by no later than the end of January 2014. IRM issued a draft of the plan to committee members to begin discussions on December 6. I believe these actions, once completed, will address your second

recommendation. Similar to other corrective action plans, IRM will be required to report on the status of the plan at each MCSC meeting which will serve to monitor progress.

Your memo recommended that the MCSC direct IRM to employ the services of the National Security Agency (NSA) to conduct independent penetration testing. The Committee believes that DS, like the OIG, has direct lines to the Secretary and has the capability to be independent in these matters. In addition, DS assured the Committee that they have the capability and work with and have the confidence of NSA in these matters. We believe OIG would not disagree that DS has the capability to adequately perform the testing. However, we fully understand the issue of perception of independence. Therefore the MCSC is supportive of DS and IRM having further discussions with the OIG on this matter to determine the best plan of action to perform penetration testing that meets the needs of the OIG and Department management. In addition, at the meeting, we suggested that there may be other alternatives to NSA, such as using a 3rd party to review the methodology used by DS. Ms. Disalto indicated that the OIG would welcome additional discussions including the potential of an alternative 3rd party.

As noted at the MSCS meeting, IRM and DS are committed to protecting the Department's systems and agree with the recommendations the OIG published in the 2013 FISMA report. However, they respectfully disagree on the level of severity these weaknesses collectively represent. As a result of careful consideration of the information presented by the OIG, IRM, and DS at the MCSC meeting, and in the respective memorandums, the Committee decided to report the weaknesses in the Department's ISS Program as a significant deficiency under FMFIA for FY 2013.

As Chair of the MCSC, I would like to extend my appreciation for the information provided in your memo. Let me assure you that the Committee takes the reported weaknesses very seriously. I hope you find the actions of the MCSC and the information contained herein responsive to your request. The Committee believes that our efforts over the coming year will advance the Department's information security posture and address OIG concerns identified in your memo. Again, we extend our appreciation for your staff's efforts, and the OIG's participation in the MCSC and Senior Assessment Team. MCSC welcomes and looks forward to future FISMA evaluation results and information from the OIG.

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

JAN 13 2014

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from Attachment)

TO: Management Control Steering Committee

FROM: OIG - Steve A. Linick

SUBJECT: OIG's response to MCSC regarding *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (AUD-IT-14-04)

(U) Thank you for your December 13, 2013, response to the Office of Inspector General (OIG) Management Alert regarding significant and recurring weaknesses in the Information System Security Program of the Department of State (Department).

(U) As mentioned previously, OIG identified, in its FY 2013 Federal Information Security Management Act (FISMA) report, multiple control weaknesses that exist throughout the Department's Information System Security Program. These control weaknesses constitute a significant deficiency under FISMA and a material weakness under the Federal Managers Financial Integrity Act (FMFIA). OIG identified similar significant deficiencies in its annual FISMA reports for both FY 2011 and FY 2012. Several authorities, including FISMA,[1] Office of Management and Budget (OMB) guidance, and the *Foreign Affairs Manual,* require immediate corrective action of any significant deficiency, as well as external reporting as a material weakness under FMFIA.

(U) OIG made three recommendations to Department management through the Management Control Steering Committee (MCSC). OIG considers Recommendation 1, pertaining to reporting the FISMA significant deficiency designation as a FMFIA material weakness, unresolved. In its response, the MCSC acknowledges that OIG's findings rise to the level of a "significant deficiency under FMFIA for FY 2013," but the MCSC does not agree that the significant deficiency needs to be externally reported as a FMFIA "material weakness." However, OMB guidance states that "FISMA requires agencies to report a significant deficiency as…a material weakness under [FMFIA]."[2]

---

[1] 44 U.S.C § 3544(c)(3).

[2] **(U)** OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" (Sept. 27, 2012), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf.

(U) OIG considers Recommendation 2, pertaining to the development of a comprehensive corrective action plan to address the existing FISMA significant deficiency, resolved because of actions taken to implement the recommendation. However, the recommendation will remain open until OIG reviews and accepts documentation showing that the Bureau of Information Resource Management (IRM) has developed a comprehensive corrective action plan to address the existing FISMA significant deficiency designation.

(U) OIG considers Recommendation 3, pertaining to independent penetration testing, unresolved. The MCSC indicated that it is supportive of the Bureau of Diplomatic Security (DS) and IRM having further discussions with OIG on this matter, but it further stated that "OIG would not disagree that DS has the capability to adequately perform the testing." The issue, however, is not about DS's "capability" but its independence and perceived independence. According to the National Institute of Standards and Technology (NIST):

> An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that the assessor is free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness.[3]

Because DS is actively involved in the Department's Information System Security Program, it cannot be considered an independent, impartial assessor. The recommendation will remain open until OIG reviews and accepts documentation showing that independent penetration testing has been implemented. The penetration testing must be performed by the National Security Agency or an equally qualified organization independent of the Department and approved by OIG.

(U) If you have any questions, please contact Norman P. Brown, Acting Assistant Inspector General for Audits, at brownnp2@state.gov or Jerry Rainwaters, Information Technology Division Director, at rainwatersj@state.gov.

Attachment: As stated.

cc: D(B) – William J. Burns
D(H) – Heather A. Higginbottom
S – David E. Wade
M – Patrick F. Kennedy

[3] **(U)** NIST SP 800-37, rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Feb. 2010.

A – Joyce A. Barr
BP – Barbara Retzlaff
CA – Janice Jacobs
CGFS – James Millette
CGFS/DCFO – Chris Flaggs
CGFS/DCFO/MC – Carole Clay
CGFS/DCFO/MC – Michelle Carter
DGHR – Hans Klemm, Acting
DS – Gregory B. Starr
EAP – Daniel Russel
ECA – Lee Satterfield, Acting
INL – William R. Brownfield
IRM – Steven C. Taylor
L – Richard Visek
OBO – Lydia Muniz
PM – Thomas Kelly, Acting
PRM – Anne Richard