



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

JUL - 5 2011

MEMORANDUM

TO: CIO – Susan Swart

FROM: OIG – Harold W. Geisel

SUBJECT: *Management Letter Related to Review of Department of State Information Security Program for FY 2010 (AUD/IT-11-26)*

Attached for your review and action is a copy of the subject report. Williams, Adley & Company, an independent external auditor, at the direction of the Office of Inspector General, prepared this management letter. Based on your response, OIG considers Recommendation 1 closed. However, please provide your response to the report and information on actions taken or planned for Recommendation 2 within 30 days of the date of this memorandum. Actions taken or planned are subject to followup and reporting in accordance with the attached compliance response information.

OIG incorporated your comments as appropriate within the body of the report and included them in their entirety as Appendix A.

OIG appreciates the cooperation and assistance provided by your staff during this audit. If you have any questions, please contact Evelyn R. Klemstine, Assistant Inspector General for Audits, at (202) 663-0372 or Jerry Rainwaters, Director, Information Technology Division, at (703) 284-1841 or by email at rainwatersJ@state.gov.

Attachments: As stated.

cc: DS – (b) (6)

UNCLASSIFIED

**Management Letter Related to
Review of Department of State
Information Security Program for FY 2010**

**AUD/IT-11-26
July 2011**

Williams, Adley & Company, LLP
1250 H Street, NW
Suite 1150
Washington, DC 20005

UNCLASSIFIED

UNCLASSIFIED



June 14, 2011

Office of Inspector General
U.S. Department of State
Washington, D.C.

Williams, Adley & Company, LLP (referred to as "we" in this letter), is pleased to provide the Office of Inspector General (OIG) the management letter pertaining to information security control issues that were not reported during our FY 2010 review of the Department of State's (Department) Information Security Program. We reviewed the Department's Information Security Program as required by the Federal Information Security Management Act and in accordance with Office of Management and Budget and National Institute of Standards and Technology regulations and standards.

This review of the additional information security control issues was performed under Contract No. SAQMMA10F2159. We communicated the results of our review and the related findings and recommendations to the Department's Office of Inspector General.

We appreciate the cooperation provided by Department personnel during the review. If you have any questions, please contact Ben Nakhavanit, Senior IT Audit Manager, or Bob Fulkerson, IT Audit Director, at (202) 371-1397.


Kola Isiaq, CPA
Managing Partner

WILLIAMS, ADLEY & COMPANY-DC, LLP
Management Consultants/Certified Public Accountants
1250 H Street, NW, Suite 1150 • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161

UNCLASSIFIED

Management Letter

Information Security Control Issues

Williams, Adley and Company, LLP (referred to as “we” in this management letter), conducted, on behalf of the Office of Inspector General (OIG), an independent evaluation of the Department of State’s (Department) Information Security Program as required by the Federal Information Security Management Act (FISMA) and in accordance with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) regulations and standards.

In addition to the findings identified in the FY 2010 report *Review of Department of State Information Security Program* (AUD/IT-11-07, November 2010), we identified two additional information security weaknesses that require your attention and that are discussed individually within this report:

- Security Training – Lack of maintenance of classified information nondisclosure agreements.
- Contingency Planning – Lack of evidence for enterprise-wide Business Impact Analysis (BIA) for Primary Mission Essential Functions (PMEF).

Although the recommendations to the draft management letter were addressed to the Bureau of Diplomatic Security (DS), the Bureau of Information Resource Management (IRM) presented its “coordinated” response with DS and the Bureau of Administration and provided a “consolidated reply” to the recommendations, which is in Appendix A.

Background

The FY 2010 report measured the Department’s security program against the standards contained in NIST Federal Information Processing System (FIPS) Publication (Pub) 200, *Minimum Security Requirements for Federal Information and Information Systems*. This publication is applicable to all information within the Federal Government and all Federal information systems and is the basis for the application of the security controls defined in NIST Special Publication (SP) 800-53, revision 3, *Recommended Security Controls for Federal Information Systems*. The requirements in FIPS Pub 200 are consistent with those contained in section 8b(3) of Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, as analyzed in appendix IV, “Analysis of Key Sections,” of the circular. Supplemental information on OMB Circular A-130 is provided in appendix III of the circular.

Security control weaknesses directly related to FISMA were provided to the Department in OIG’s November 2010 report (AUD/IT-11-07).

UNCLASSIFIED

Scope and Methodology

We conducted the review from June through September 2010 and in accordance with FISMA, OMB, and NIST guidance. We and OIG believe that the evidence obtained provides a reasonable basis for the findings and conclusions represented in this letter.

We used the following laws, regulations, and policies to evaluate the adequacy of the controls in place at the Department:

- OMB Memorandums M-02-01, M-04-04, M-06-19, and M-10-15.¹
- Department policies and procedures.
- Federal laws, regulations, and standards (such as the Computer Security Act of 1987; FISMA; and OMB Circular A-130, appendix III).
- NIST SPs, FIPS Pubs, other applicable NIST publications, and industry best practices.

The weaknesses we identified and the related recommended corrective actions are as described.

Lack of Maintenance of Classified Information Nondisclosure Agreements

The Department did not obtain signed copies of Standard Forms (SF) 312, Classified Information Nondisclosure Agreement, for four of 25 new employees included in our sample for testing. The Foreign Affairs Manual (FAM)² requires the bureau, post, or unit security officer to ensure that each new employee signs an SF 312 acknowledging that he or she has read, understands, and agrees to abide by the Department's rules for accessing classified information at the beginning of employment and before accessing classified information. In addition, NIST SP 800-53³ requires Federal agencies to obtain from employees "signed acknowledgement . . . indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system."

DS determined that SFs 312 were missing for two of the four employees because the security officer (from post) had not submitted the forms. For another employee, the position was designated nonsensitive, which did not require access to classified information. Therefore, no briefing was authorized, and the SF 312 was not signed. DS could not determine why the SF 312 was missing for the fourth employee.

We noted that DS does not have procedures in place to routinely, on a quarterly, semiannual, or annual basis, reconcile the number of new employees hired by the Department with the number of SFs 312 received from all of the bureaus and posts. Additionally, DS does

¹ OMB Memorandums M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*; M-04-04, *E-Authentication Guidance for Federal Agencies*; M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; and M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

² 12 FAM 563.2, "Responsibilities of Post Security and Unit Officers," and 12 FAM 564.1, "Briefings - Initial."

³ NIST SP 800-53, rev. 3, PL-4, "Rules of Behavior."

UNCLASSIFIED

not have procedures to identify specific employees who have not completed and signed the SFs 312. (The current process involves manually signing the SFs 312.)

Without a signed SF 312, the Department has no record that an employee understands and has acknowledged the rules of behavior for Federal information and information systems and may not be able to hold an employee accountable for actions that may be contrary to FAM and NIST requirements.

Recommendation 1: We recommend that the Bureau of Diplomatic Security (DS) develop and implement new internal controls to compare and reconcile, on a quarterly, semiannual, or annual basis, the number of signed Standard Forms (SF) 312, Classified Information Nondisclosure, for new employees with the actual number of new employees hired by the Department of State. The new controls should be designed to identify, by bureau or office, personnel who have not completed and submitted a signed SF 312. Because of the number of SFs 312 and the manual intensive process in place to compare and reconcile SFs 312, DS should consider implementing an automated process.

Management Response. In the consolidated reply, DS stated that it “respectfully disagree[d] with the recommendation based upon the relevant authorities governing the use of non disclosure agreements for the use of classified information.” Instead, DS stated that the signed acknowledgement (for the rules of behavior) is addressed by the Department’s initial and annual cyber security awareness training. DS requested that the recommendation “be removed” from the management letter.

OIG Analysis. Based on management’s statement and the documentation it cited describing the internal controls in place to ensure that only authorized individuals are granted access to classified systems, OIG considers this recommendation closed. During the FY 2011 OIG FISMA evaluation, the initial security awareness training program and its supporting documentation will be reviewed.

Lack of Evidence for Enterprise-Wide Business Impact Analysis for Primary Mission Essential Functions

The Bureau of Administration, Office of Emergency Management, did not provide evidence that an enterprise-wide BIA had been conducted. In February 2008, OMB, through the Department of Homeland Security (DHS), established Federal Continuity Directive 2 (FCD2), *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, which requires all Federal agencies to conduct an enterprise-wide BIA to consolidate the agency’s Primary Mission Essential Functions (PMEF) under a single recovery document by prioritizing the functions. The PMEF is essential to identifying critical and essential Department functions that must be performed to support the performance of National Essential Functions before, during, and after an emergency situation occurs. Each agency’s PMEF needs to identify critical and primary functions that need to be performed on either a continuous basis or that need to be resumed within 12 hours after a disaster or significant event occurs and that must be maintained for up to 30 days or until normal operations can be resumed.

UNCLASSIFIED

The Office of Emergency Management provided copies of the PMEFs but not of the supporting BIAs. Also, although IRM has performed specific BIAs at the application and system level, IRM did not provide a copy of the enterprise-wide BIA that prioritizes the recovery processes based on the Department's assessment of critical communications support needs for each of the Department's mission-essential functions. Therefore, we concluded that the Department does not have an enterprise-wide BIA.

Without performing a BIA at the enterprise level in conjunction with the PMEF, the Department will not meet the requirements set forth in FCD2, which may impact DHS's efforts to develop and implement a recovery program to address the National Essential Functions.⁴

Additionally, IRM-documented recovery strategies may not be appropriate and relevant to the Department's missions to ensure that critical and primary functions are recovered within the required timeframes and continued at a temporary recovery backup facility for 30 days, as required by FCD2.

Recommendation 2: We recommend that the Bureau of Information Resource Management, in conjunction with the Bureau of Administration, Office of Emergency Management, develop and document a comprehensive enterprise-wide Business Impact Analysis in conformance with Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*.

Management Response: In the consolidated response, IRM, "in conjunction with" the Bureau of Administration, "respectfully disagree[d]" with "the placement" of the recommendation in the "instant Management Letter based upon the lack of relevance to the controlling authority." IRM stated that while the requirements specified in FCD2 are "critical and essential, any Department weaknesses associated with implementing those requirements are not directly relevant to implementation of FISMA and its associated authorities."

OIG Analysis: OIG considers this recommendation applicable to FISMA, as resiliency and contingency planning is directly related to information security and OMB specifically asks about the status of BIAs in its annual OIG FISMA metrics. Therefore, OIG considers this recommendation unresolved. This recommendation can be closed pending OIG's review and acceptance of Office of Emergency Management and IRM documentation for the enterprise-wide BIA for the PMEFs identified, as required by OMB.

⁴ These functions are defined as the eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency.



United States Department of State

Washington, D.C. 20520

April 21, 2011

MEMORANDUM

TO: OIG/AUD – Mr. Jerry Rainwaters

FROM: IRM/BMP/SPO/SPD – Robert Glunt RG

SUBJECT: Response to Draft *Management Letter Related to Review of Department of State Information Security Program for FY 2010*

IRM would like to extend its appreciation for the opportunity to review and provide comment to the draft Management Letter related to the OIG's review of the Department of State Information Security Program for FY 2010.

While it is not our intention to provide detailed explanations of implementation efforts, IRM and the other Bureaus involved preparing the responses, wish to articulate rationale for their position on the two recommendations provided.

Responses were coordinated with the Bureau of Diplomatic Security and the Bureau of Administration. Please consider this a consolidated reply to your request.

Lack of Maintenance of Classified Information Nondisclosure Agreements

Recommendation 1: We recommend that the Bureau of Diplomatic Security (DS) develop and implement new internal controls to compare and reconcile, on a quarterly, semiannual, or annual basis, the number of signed Standard Forms (SF) 312, Classified Information Nondisclosure, for new employees with the actual number of new employees hired by the Department of State. The new controls should be designed to identify, by bureau or office, personnel who have not completed and submitted a signed SF312. Because of number of SFs 312 and the manual intensive process in place to compare and reconcile SFs 312, DS should consider implementing an automated process.

UNCLASSIFIED

UNCLASSIFIED

Response: The Bureau of Diplomatic Security respectfully disagrees with the recommendation based upon the relevant authorities governing the use of non disclosure agreements for the use of classified information.

Executive Order 12968, *Access to Classified Information*, states in Section 3.1 that “no employee shall be deemed eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.” Executive Order 12968 goes on to say only those employees granted access to classified information must “have signed an approved non disclosure agreement.”

Executive Order 13526, *Classified National Security Information*, states in Section 4.1 that only those “who have met the standards for access to classified information shall receive contemporaneous training on the proper safeguarding of classified information”. The Executive Order defines contemporaneous as a time period when all three conditions are satisfied:

- a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;
- the person has signed an approved nondisclosure agreement; and
- the person has a need-to-know the information.

The Foreign Affairs Manual section cited by the OIG’s Management Letter (e.g., 12 FAM 564.1) is consistent with the aforementioned Executive Orders where it states “each new employee is required to read and sign Form SF-312, Nondisclosure Agreement at the time of entrance on duty and prior to being afforded access to national security (classified) information.”

As such, the applicable Executive Orders and the Department’s implementing policy both stand for the proposition that only those individuals granted access to classified information are required to execute a non-disclosure agreement.

The NIST Special Publication 800-53 cited by the OIG’s Management Letter is misplaced in that the publication does not apply to national security systems and the cited requirement (e.g., “signed acknowledgement... indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and information systems”) is addressed by the Department’s initial and annual cyber security awareness training.

The Department maintains an up-to-date database of every new cleared employee that has signed an SF-312. Executed SF-312s are entered into a DS database and

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

the original form is forwarded to HR for inclusion in the individual's official personnel file (OPF), in accordance with National Archives Office of Information Security Oversight guidance.

Accordingly, the Bureau of Diplomatic Security respectfully requests Recommendation 1 be removed from the Management Letter.

Lack of Evidence for Enterprise-Wide Business Impact Analysis for Primary Mission Essential Functions

Recommendation 2: We recommend that the Bureau of Information Resource Management, in conjunction with the Bureau of Administration, Office of Emergency Management, develop and document a comprehensive enterprise-wide Business Impact Analysis (BIA) in conformance with Federal Continuity Directive 2, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process.

Response: The Bureau of Information Resource Management, in conjunction with the Bureau of Administration respectfully disagree with the placement of Recommendation 2 in the instant Management Letter based upon the lack of relevance to the controlling authority.

The purpose of the Federal Information Security Management Act of 2002 (FISMA) is to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."

Federal Continuity Directive 2 (FCD2), *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, was established to help agencies identify their Mission Essential Functions (MEF) and potential Primary Mission Essential Functions (PMEF). The Bureau of Administration has completed identifying Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) as required by the Inter Agency Board (IAB). Business Impact Analyses (BIAs) have been completed for the identified Primary Mission Essential Functions (PMEFs). All processes have been performed in accordance with Federal Continuity Directive 2 (FCD2).

While the requirements specified in the Federal Continuity Directive 2 (FCD2), are critical and essential, any Department weaknesses associated with implementing those requirements are not directly relevant to implementation of FISMA and its associated authorities.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

Accordingly, the Bureau of Information Resource Management, in conjunction with the Bureau of Administration, respectfully request Recommendation 2 be removed from the instant Management Letter and be included in an OIG report that is relevant to the subject matter in question.

UNCLASSIFIED

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
<http://oig.state.gov>

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.