



Office of Inspector General

~~SENSITIVE BUT UNCLASSIFIED~~

**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Office of Audits

**Audit of Department of State Access Controls
for Major Applications**

Report Number AUD-IT-12-44, September 2012

~~Important Notice~~

~~This report is intended solely for the official use of the Department of State of the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. § 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~SENSITIVE BUT UNCLASSIFIED~~



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel", written in a cursive style.

Harold W. Geisel
Deputy Inspector General

Acronyms

AIS	automated information system
CA	Bureau of Consular Affairs
DS	Bureau of Diplomatic Security
FAM	<i>Foreign Affairs Manual</i>
IRM	Bureau of Information Resource Management
ISSO	Information Systems Security Officer
IT	information technology
ITAB	Information Technology Asset Baseline
NCD	Net-Centric Diplomacy
OIG	Office of Inspector General
SMART-C	Classified State Messaging and Archive Retrieval Toolset

(U) Table of Contents

<u>(U) Section</u>	<u>(U) Page</u>
(U) Executive Summary	1
(U) Background.....	3
(U) Objective.....	5
(U) Audit Results	5
(SBU) Finding A. Protection of Sensitive Cables Remains a Challenge	6
(b) (5)	10
(SBU) Finding C. Account Management Procedures Need Strengthening.....	11
(SBU) Finding D. System Administrator Activities Are Not Monitored Effectively	15
(SBU) Finding E. Patch Management Program for Databases Is Not Effective	16
(U) List of Recommendations.....	20
(U) Appendices	
A. (U) Scope and Methodology.....	22
B. (U) Office of Inspector General Reports Related to Audit	31
C. (SBU) Proposed Net-Centric Diplomacy Security Enhancements	33
D. (SBU) Bureau of Information Resource Management Response	34
E. (SBU) Bureau of Diplomatic Security Response	40
F. (SBU) Bureau of Consular Affairs Response.....	43
G. (U) Bureau of Human Resource Response	44
(U) Major Contributors to This Report.....	46

(U) Executive Summary

(U) Access controls consist of physical and logical controls that are intended to provide reasonable assurance that system resources such as hardware, data files, application programs, and underlying operating systems are protected against unauthorized access, operation, modification, disclosure, loss, or impairment. Physical access controls ensure that system assets are physically protected from unauthorized access, and logical access controls provide assurance that only authorized users may access system data and programs. Access controls on the major applications and databases that store sensitive information within the Department of State (Department) must be suitably robust to prevent unauthorized access.

(U) The objective of this audit was to determine the effectiveness of logical access controls pertaining to selected major applications used by the Department. Specifically, the audit was to determine whether logical access controls were in place and were operating effectively.

~~(SBU)~~ The Office of Inspector General (OIG) found that the Department had made overall progress toward implementing effective logical access controls for major applications. However, during the audit, OIG found five weaknesses pertaining to logical access controls in the applications and related databases reviewed both domestically and at the three embassies visited: Embassy Buenos Aires, Argentina; Embassy Madrid, Spain; and Embassy Accra, Ghana. These five weaknesses are described as follows:

- ~~(SBU)~~ Protection of Sensitive Department Cables

~~(SBU)~~ Two years after the unauthorized release of sensitive cables to the public through the Wikileaks organization, ~~(b) (5)~~ cable-related applications such as Net-Centric Diplomacy (NCD) and Classified State Messaging and Archive Retrieval Toolset (SMART-C). Progress in addressing the NCD weaknesses that made the Wikileaks incident possible has been very slow.

- (U) Vulnerability Scanning

~~(SBU)~~ No formal vulnerability scanning process existed for databases as part of the risk management strategy, even though important operations such as consular affairs and financial management routinely rely on databases to support operations. Further, the Bureau of Diplomatic Security (DS) had not procured database scanning software necessary to accomplish this task. Lack of a database vulnerability scanning process weakens the Department's ability to proactively identify and remediate database security configuration weaknesses before they are exploited.

¹ (U) The alleged copying and release of thousands of Department cables to the public was accomplished by the Wikileaks organization.

- (U) Account Management

(SBU) OIG identified account management deficiencies. Specifically, requirements in the *Foreign Affairs Manual* (FAM) (b) (5) were not always being followed. Moreover, system administrators did not perform periodic account revalidation, which was contrary to FAM requirements as well as deleterious to system security.

- (U) Oversight of System Administrator Activities

(SBU) OIG found that audit logs for all of the applications audited were not reviewed periodically. OIG learned that because of limited staff, there was an operational need to provide all system administrators with the same permissions to enable other system administrators to perform the tasks necessary to continue operations when other system administrators are not available. (b) (5)

- (U) Patch Management

(SBU) OIG found that database administrators were not following the Department's patch management policies for its databases. (b) (5)

Patch management is an important factor in mitigating database vulnerability risks, and up-to-date patch installation can help allay these risks.

(SBU) Weaknesses in logical access controls render sensitive information in Department applications and databases vulnerable to compromise, jeopardizing the confidentiality, integrity, and availability of the stored and processed information.

(U) OIG made 10 recommendations associated with the five finding areas to enhance the security posture of the Department's major applications. The most significant of these recommendations are as follows:

- (SBU) Identify and obtain personnel who have the expertise to develop the needed security enhancements to the NCD application.
- (SBU) Develop a comprehensive strategy for periodic database vulnerability scanning to ensure that database vulnerabilities are identified and remediated.
- (SBU) Develop a patch management strategy to ensure that database security patches are applied in a timely manner.
- (SBU) Identify and provide appropriate training for post SMART-C administrators to ensure clarity of the SMART-C access controls features.

- (SBU) Periodically review and remove [REDACTED] (b) (5) to prevent potential malicious use [REDACTED] (b) (5)
- (SBU) Perform periodic reviews of audit logs to proactively detect and investigate potential security incidents.

(U) In August 2012, OIG provided a draft of this report to the Bureaus of Information Resource Management (IRM), Diplomatic Security (DS), Consular Affairs (CA), and Human Resources (HR). OIG made 10 recommendations.

- (U) Recommendations 1, 2, 3, 4, 7, 9, and 10 were addressed to IRM. IRM concurred with Recommendations 1, 2, 4, 7, 9, and 10 but did not concur with Recommendation 3. (IRM's response is in Appendix D.)
- (U) Recommendation 5 was addressed to DS, which concurred with the recommendation. (DS's response is in Appendix E.)
- (U) Recommendation 8 was addressed to CA, which concurred with the recommendation. (CA's response is in Appendix F.)
- (U) Recommendation 6 was addressed to HR. HR did not state concurrence or nonconcurrence with the recommendation but indicated that a process was in place to address the recommendation and requested that the recommendation "be removed or closed." However, OIG determined through its fieldwork, that the process described in the response was not working as intended. (HR's response is in Appendix G.)

(U) Based on the responses to the 10 recommendations, OIG considers eight recommendations (Nos. 1, 2, 4, 5, 7, 8, 9, and 10) resolved, pending further action, and two recommendations (Nos. 3 and 6) unresolved. IRM and HR, respectively, need to implement control procedures to address the weaknesses identified in Recommendations 3 and 6.

(U) For Recommendation 3, IRM did not present sufficient justification to address the necessary oversight of the system administrators to protect sensitive Department information. OIG believes that the seriousness of this weakness requires management to oversee the system administrators and hold them accountable for their actions.

(U) Actions stated in HR's response to Recommendation 6 were not supported by what OIG found in its recent fieldwork. That is, the system administrators have not been receiving the monthly Separation Reports. However, based on the January 2012 changes stated in HR's response, this situation may be improving.

(U) The bureaus' responses to each recommendation and OIG's replies to these responses are presented after each recommendation.

(U) Background

(U) Effective logical access controls are critical for any organization that depends on information technology (IT) and even more important for Federal Government agencies, such as the Department, where maintaining the public's confidence both locally and internationally is

essential. The widespread use of the Internet has changed how agencies conduct business. Although use of the Internet has brought about many benefits for agencies to help them meet their mission objectives, it also exposes Federal networks and applications to potentials threats.

(U) Without effective logical access controls, information systems are vulnerable to attack by individuals and groups who may have malicious intent to intrude and use their unauthorized access to compromise the confidentiality, integrity, and availability of these systems. Over the past several years, Federal agencies have reported an increasing number of security incidents, including the Wikileaks incident that resulted in the unauthorized release of sensitive cables to the public.

(U) OMB Circular A-130, Appendix III,² further establishes a minimum set of controls to be included in Federal automated information security programs. These controls include logical access controls such as separation of duties enforced by limitations on the processing privileges of individuals. IRM manages the Department's computer networks.³ The Department's bureaus provide mission-oriented systems and applications to Department users in support of their respective functions. User access controls to these systems and applications, both physical and logical controls, are administered by the respective bureaus and are required to meet the minimum control standards set forth in the Department's policies. The Chief Information Officer (CIO) is responsible for directing and administering the Department's information security program and for serving as the principal adviser to the Secretary of State on the development, implementation, and, as necessary, the revision of policies, plans, and programs for information resources management.

(U) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3,⁴ provides the recommended controls needed to enforce access to Federal information and information systems. For example, least privilege controls require "only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

(U) The Department's FAM sets forth policies and procedures that require all personnel accessing the Department's automated information system (AIS) to be given access levels based on a need-to-know⁵ basis, appropriate supervision, and knowledge of their AIS security responsibilities.

³ (U) Computer networks are information systems implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

⁴ (U) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, rev. 3, Aug. 2009.

⁵ (U) "Need to know" is a method of isolating information resources based on users' needs to have access to that resource in order to perform their jobs but no more. The terms "need to know" and "least privilege" express the same idea. "Need to know" is generally applied to people, while "least privilege" is generally applied to processes.

(U) OMB Circular A-130, Appendix III, defines a “major application” as “an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.” Effective logical access controls are therefore paramount in preserving the confidentiality, integrity, and availability of these applications. As of April 2011, the Department’s Information Technology Asset Baseline⁶ (ITAB) contained 197 active major applications. To attain its audit objective, OIG planned to review logical access controls for a sample of major applications from ITAB. (Sampling details are in Appendix A.)

(U) Objective

(U) The objective of this audit was to determine the effectiveness of logical access controls pertaining to selected major applications used by the Department. Specifically, the audit was to determine whether logical access controls were in place and were operating effectively.

(U) Audit Results

~~(SBU)~~ OIG reviewed logical access processes and procedures around major applications pertaining to account authorization, periodic account revalidation, concept of least privilege,⁷ separation of duties, audit log monitoring, and database vulnerability assessments. OIG’s final sample comprised 19 major applications. OIG found weaknesses pertaining to logical access controls in the applications and related databases reviewed both domestically and at the three embassies visited during the audit: Embassy Buenos Aires, Embassy Madrid, and Embassy Accra. Of the 19 applications sampled, OIG performed a manual review of access controls processes and procedures for 16⁸ applications and determined the following:

- ~~(SBU)~~ Of 16 applications, 11 had procedures in place for account authorization and 14 had access controls features that enforced the concept of least privilege.
- ~~(SBU)~~ Systems administrators for 13 of 16 applications did not have ~~(b) (5)~~
- ~~(SBU)~~ Systems administrators and personnel officers for 14 of 16 applications did not have formal processes for obtaining formal notifications of ~~(b) (5)~~
- ~~(SBU)~~ For all 16 applications reviewed, there were no formal processes in place for ~~(b) (5)~~
- ~~(b) (5)~~

⁶(U) ITAB is the Department’s official inventory of applications.

⁷ (U) The concept of least privilege is the security objective of granting users only those accesses they need to perform their official duties.

⁸ (U) Of the remaining three applications from OIG’s sample of 19, two applications, the Consular Lookout and Support System (CLASS) and the Automated Biometric Identification System (ABIS) were back-end processing applications and were not manually reviewed by OIG. The Travel Document Issuance System (TDIS) was not manually reviewed because of the geographical distribution of its user base and OIG’s resource limitations. Related databases for all three applications were subjected to automated scanning. Further, OIG reviewed the Consular Electronic Application Center (CEAC) and found that it is a public facing application, to which OIG’s audit procedures generally do not apply.

- (b) (5) [REDACTED] (Database vulnerability scans could not be conducted for six of 19 major applications in OIG’s final sample because of the scope limitations detailed in Appendix A, “Scope and Methodology.”)

(SBU) Based on the information cited, OIG found that overall progress has been made toward the implementation of effective logical access controls for major applications but noted that challenges remained. The Department needs to address several control weaknesses, as described in Findings A–E, that were found both domestically and at the three overseas embassies OIG visited.

~~(SBU)~~ Finding A. Protection of Sensitive Cables Remains a Challenge

(SBU) Two years after the Wikileaks incident, logical access controls for key cable-related applications continued to have weaknesses (b) (5) [REDACTED]. Within OIG’s sample of 19 major applications, two applications, NCD and SMART-C, (b) (5) [REDACTED]. NCD was the application involved in the Wikileaks cables incident. (b) (5) [REDACTED]

(b) (5) [REDACTED]

(U) The FAM¹¹ requires the Department to establish “personnel security procedures which require that all employees accessing any of the Department’s classified automated information system (AIS) processing resources . . . to have the appropriate access levels and need to know in connection with the performance of official duties.”

(U) Further, the FAM¹² states, “The data center manager and the system manager enable the audit trail feature on the operating system and install any required security software to record security incidents listed in 12 FAM 637.1-9.”

⁹ (U) Telegrams, also called “cables,” are the official record of Department of State policies, program activities, post operations, and personnel management. Official communications are to be preserved as a cable or a record e-mail. These messages are available through several internal resources.

(b) (5) [REDACTED]

(5)¹¹ (U) 12 FAM 631.1, “Personnel Security.”

¹² (U) 12 FAM 637.3-3, “Establishing Audit Trails and Logs.”

(U) Net-Centric Diplomacy Application

~~(SBU)~~ NCD was developed for the purpose of sharing diplomatic reporting information, including cables, with the Department and other Government agencies. This sharing of information is accomplished through the Secret Internet Protocol Router Network¹³ (SIPRNet). The shared diplomatic cables consist of SIPDIS¹⁴ captioned cables. These are cables deemed appropriate for interagency sharing. In the Wikileaks incident, the alleged perpetrator downloaded several thousand cables and is alleged to have provided this information to an unauthorized source.

~~(SBU)~~ IRM officials stated that access to NCD via SIPRNet was discontinued after the Wikileaks incident. However, as of March 12, 2012, when OIG met with IRM officials, OIG found the following logical access controls weaknesses for NCD:

(b) (5)



~~(SBU)~~ IRM officials stated that a project had been initiated to redesign NCD to address the access control weakness after the Wikileaks incident. Per a plan of action provided to OIG by the NCD team (NCD.09.00.00 Plan of Action, dated February 12, 2012), the purpose of the redesign effort was to make software modifications to enhance the security posture of NCD. The

¹³ (U) SIPRNet is the Department of Defense-funded, Defense Information Systems Agency-managed, secret-level classified Intranet. SIPRNet provides Internet-like connectivity to a host of agencies throughout the Federal Government.

¹⁴ (U) SIPDIS is the Department's distribution caption that facilitates inter-agency information sharing of classified and unclassified cables via the U.S. Government's SIPRNet.

¹⁵ (U) *Evaluation of Department of State Information Security Program* (AUD/IT-12-14, Nov. 2011).

¹⁶ Authentication means verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

¹⁷ (U) "Hard coded" means that data value or behavior is written directly into a program.

¹⁸ (U) The source code is the form in which a computer program is written by the programmer.

¹⁹ (U) The NCD redesign effort comprised four subprojects, known collectively as "Eclipse."

software security requirements addressed in the redesign included the addition of user authentication, implementation of code changes to reduce data vulnerabilities, configuration of the non-SIPDIS caption exclusion capability, audit trail capability, user-based download threshold alerts, ability to turn off certain NCD features, and the capability to remove comments to preserve integrity cables. (Details of these security enhancements are in Appendix C.) However, IRM officials stated that the enhancements had not been completed for three primary reasons: (1) a lack of technical expertise on the part of the contractor supporting the application; (2) difficulty finding contractor personnel with top secret/sensitive compartmented information clearances; and (3) difficulty in understanding the NCD application because the Bureau of Resource Management did not provide the full source code for NCD, as well as sufficient documentation for the application, during the transition to IRM.

(U) SMART-C Application

~~(SBU)~~ SMART-C provides users with the ability to send e-mails and cables and can be accessed by users with ClassNet access. Regarding SMART-C, OIG determined the following:

- ~~(SBU)~~ All six post administrators at the embassies visited had unrestricted access to the content of all captioned cables at their respective embassies. In addition, all four SMART administrators at the Main State Messaging Center have unrestricted access to the content of all cables. IRM officials stated that all the system administrators require full access to cables so that they can collaboratively manage and troubleshoot issues such as those related to the delivery of the cables. ~~(b) (5)~~

- ~~(SBU)~~ SMART-C audit logs did not provide the information needed for post administrators to detect abnormal end user or administrator activity. IRM Messaging Office personnel stated that the current audit log capabilities of SMART-C were not developed for post administrator use but for SMART-C developers to facilitate the detection of application issues. Thus the audit log was useful to the development team but was not useful for detecting unusual activity by users or administrators.
- ~~(SBU)~~ There was a lack of clarity regarding the use of Role Based Access Controls²⁰ (RBAC) features, such as the use of Traffic Analysis by Geography and Subject²¹ (TAGS) captions, and dissemination rules among post administrators. Post administrators stated that the lack of clarity regarding the RBAC features was due to insufficient SMART training. When post administrators responsible for administering and securing SMART-C are unclear about the application's security features, confidentiality of the contents of captioned cables could be at risk.

²⁰ (U) RBAC is a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

²¹ (U) TAGS are labels to help ensure that the right telegrams are seen by the right readers.

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~(SBU)~~ Some of the Federal Government's most sensitive information exists in cables stored in applications such as NCD and SMART-C. Without resolving the logical access controls issues inherent in these applications, an incident similar to Wikileaks could occur. Additionally, if SMART-C administrators do not receive the appropriate training to enable them to fully understand and implement the RBAC features of the application, there is the risk that sensitive cables could be exposed to unintended audiences. Also, without a useful audit trail of user activity in both NCD and SMART-C, administrators are less likely to detect and investigate suspicious activity relating to cable access.

~~(SBU)~~ **Recommendation 1.** OIG recommends that the Chief Information Officer acquire the technical resources and implement the enhancements identified by the Net-Centric Diplomacy (NCD) team in NCD.09.00.00 Plan of Action, dated February 12, 2012, to ensure that users do not have broader access to cables than what is required to perform their duties.

~~(SBU)~~ **Management Response.** IRM concurred with the recommendation, stating that actions will be taken "to acquire the necessary technical resources to implement" the Plan of Action. IRM further stated, "As of June 11, 2012, these resources have been acquired and a full team of developers is in place and actively working on the NCD.09.00.00 software release."

~~(SBU)~~ **OIG Reply.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing actions IRM has taken to enhance the security posture of NCD as detailed in the NCD.09.00.00 Plan of Action.

~~(SBU)~~ **Recommendation 2.** OIG recommends that the Chief Information Officer establish standard training requirements for post Classified State Messaging and Archive Retrieval Toolset (SMART-C) and ensure that system administrators receive required training before they are assigned and annually thereafter.

~~(SBU)~~ **Management Response.** IRM concurred with the recommendation, stating that the Foreign Service Institute had "established week-long classroom and long distance system administrator training based on training requirements from IRM."

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing actions taken by IRM to improve the training of system administrators.

~~(SBU)~~ **Recommendation 3.** OIG recommends that the Chief Information Officer implement logical access controls to ensure that system administrators do not have the ability to read information within sensitive cables that they do not need to perform their administrative duties.

~~(SBU)~~ **Management Response.** IRM did not concur with the recommendation, stating that because of "critical mission functions of Embassies abroad, and the impact upon

safety issues, Foreign Service Information Technology personnel are required to have full administrative access to all systems.”

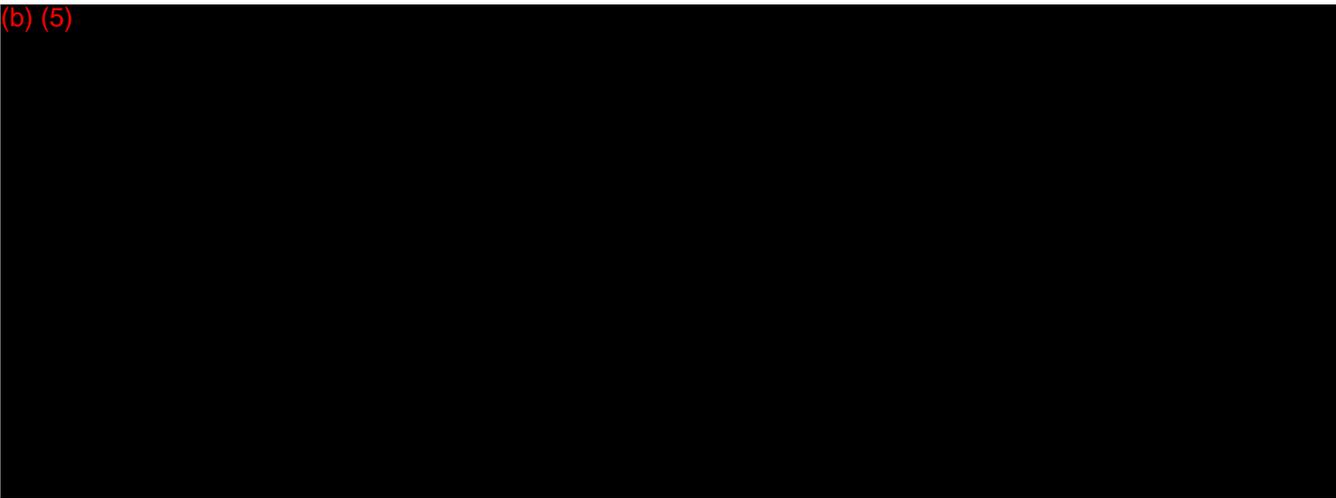
~~(SBU)~~ **OIG Reply.** While OIG recognizes the critical nature of embassies’ operations and the important role of Foreign Service Information Technology personnel, accountable and controlled access to sensitive information such as captioned cables must be maintained. A remedy to promote accountability and control, while granting access to legitimate information when needed, would be to assign system administrators unique accounts with permissions that logs access to information. This action, along with effective oversight, would help protect access to sensitive Department information and fix accountability. OIG considers this recommendation unresolved and will continue discussions with IRM during the audit compliance process to pursue implementation of the recommendation.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the Chief Information Officer equip the Net-Centric Diplomacy (NCD) and Classified State Messaging and Archive Retrieval Toolset (SMART-C) applications with audit trail capabilities to log user and administrator activity.

~~(SBU)~~ **Management Response.** IRM concurred with the recommendation, stating that as of May 31, “The audit trail capability had been implemented in NCD.” IRM further stated, “The audit log contains ALL administrative changes to SMART.” IRM also stated that it, “in consultation with DS, will continue to seek [a] commercial or custom solution” that detects anomalies in major applications but that it “has been unable to find a COTS product that will validly detect anomalies.”

~~(SBU)~~ **OIG Reply.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation supporting audit trail capabilities and showing that the Department has implemented a solution that detects anomalies in major applications.

(b) (5)



²² (U) 12 FAM 615.1, “Assistant Secretary, Bureau of Diplomatic Security (DS).”

(b) (5)

(U) The FAM²³ states, “DS/SI/CS [DS’s Security Infrastructure Directorate, Computer Security], the Evaluation and Verification Program personnel, must scan for vulnerabilities in the information system²⁴ periodically, as well as when significant new vulnerabilities affecting the system are identified and reported.”

(b) (5)

~~(SBU)~~ **Finding C. Account Management Procedures Need Strengthening**

~~(SBU)~~ OIG identified one or more account management deficiencies for the 16 applications reviewed. Specifically, system administrators and personnel officers generally did not have formal processes for removing user and administrator access from applications when an employee changed jobs within the Department, retired, or resigned. In addition, system administrators did not perform either periodic account revalidation, which was contrary to requirements in the FAM as well as being deleterious to system security. The deficiencies occurred because system administrators were not adhering to the existing procedures for performing these activities as prescribed in the FAM. Without ensuring that system owners

²³ (U) 5 FAM 1065.5, “Vulnerability Scanning.”

²⁴ (U) The NIST glossary of key Information Security terms defines an “information system” as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.” Per this definition, the major applications in the scope of this audit and their related databases are examples of the “information system” referenced in 5 FAM 1065.5.

comply with the FAM regarding the removal of unneeded accounts in a timely manner, there is the risk of unauthorized access to information.

~~(SBU)~~ **Removing User and Administrator Access**

~~(SBU)~~ OIG determined that for 14 of 16 major applications reviewed, standardized processes had not been implemented to ensure that system administrators were notified in a timely manner ~~(b) (5)~~

The FAM requires that personnel officers notify the data center manager, the system manager, and the Information Systems Security Officer (ISSO) immediately of any employee or contractor who has access to the system whose employment has been terminated for any reason so that access privileges can be revoked. ~~(b) (5)~~

~~(SBU)~~ Only one of the system administrators for the 16 major applications OIG reviewed was able to provide evidence of consistent notification from personnel officers to facilitate the removal of accounts of departing employees. ~~(b) (5)~~

~~(b) (5)~~ The system administrators stated that they received notification of employee departures sometimes through the employee's supervisor and other times from the employee as part of checkout procedures when an employee departed. One system administrator stated that he found out that an employee was leaving the Department only after he received a group e-mail from the departing employee to the entire staff.

(U) Account Revalidation

~~(SBU)~~ OIG determined that for 13 of 16 applications reviewed, there were no standardized processes for performing periodic account revalidation to identify accounts no longer required. OIG found that the process was haphazard. For instance, one application's administrator stated that revalidation was performed as part of his occasional troubleshooting of account management issues. In another instance, a system administrator stated that e-mails were sent on a monthly basis to system owners requiring them to confirm accounts but that no responses from system owners were received and no followup e-mails were sent. In other cases, no periodic account revalidation was performed. According to the FAM,²⁶ "The ISSO reviews the list of AIS users on a periodic basis to determine whether all users are authorized access to the AIS." ~~(b) (5)~~

²⁵ (U) 12 FAM 621.3-3, "System Access."

²⁶ (U) 12 FAM 622.1-8, "Monitoring System Users."

~~(SBU)~~ Account Management Issues With Bureau of Consular Affairs Applications

~~(SBU)~~ OIG found account management weaknesses specific to Bureau of Consular Affairs (CA) Consular Shared Tables application used in creating, synchronizing, and managing users for consular applications including, but not limited to, the Passport Information Electronic Records System (PIERS) and the Consular Consolidated Database (CCD) at the three embassies visited (Buenos Aires, Madrid, and Accra). The following weaknesses were identified:

- ~~(SBU)~~ OIG determined that no formal processes existed at the three embassies to facilitate the assignment of roles to new or transferring users. The consular managers stated that they relied on experience in determining what roles should be assigned to users. According to the FAM,²⁷ the ISSO and system administrators must control and limit access to the level necessary for users to perform their official duties. Without implementing formal processes, there is the risk of users being given broader access than required to perform their duties.
- ~~(SBU)~~ OIG determined that multiple active accounts existed for three users in Embassy Buenos Aires and four users in Embassy Madrid. (b) (5)

[REDACTED]

The consular managers also stated that they did not disable the previous accounts because of an oversight on their part. According to the FAM,²⁸ an authorized user must initially be assigned a unique ID and password and may be assigned more than one user ID and password only if it is required for the performance of the user's duties. Without controlling the ability to create multiple user accounts, accountability may be compromised, since transactions cannot be accurately traced to the actual user.

- ~~(SBU)~~ OIG determined that accounts were not disabled for six users in Embassy Buenos Aires and one user in Embassy Madrid who no longer worked at those embassies. The consular managers stated that these accounts remained active because of an oversight on their part. The FAM²⁹ requires that the system manager, in conjunction with the ISSO, revoke user access privileges for personnel who are transferred or terminated. (b) (5)

[REDACTED]

- ~~(SBU)~~ OIG determined that all three embassies had not implemented a formal process for provisioning users to the applications. Consular managers did not provide any

²⁷ (U) 12 FAM 622.1-2, "System Access Control."

²⁸ (U) 12 FAM 622.1-3, "Password Controls."

²⁹ (U) 12 FAM 621.3-3, "System Access."

reason as to why they did not have a formal process. According to the FAM,³⁰ supervisors must complete a system access request form for each staff member who requires access to the application. The FAM also requires that the ISSO and the system manager control and limit access to the level necessary for users to perform their official duties. Without following a formal and consistent process, there is a risk of unauthorized users being granted access to the applications.

(U) Recommendation 6. OIG recommends that the Bureau of Human Resources institute a formal process to notify system owners on a monthly basis of employee departures to ensure the timely removal of accounts of departing or transferring employees.

(U) Management Response. HR did not state concurrence or nonconcurrence with the recommendation. However, HR stated, “Since 2012, HR/EX, through coordination with the office of the Managing Director of CGFS/DCFO (at that time RM/DCFO), has been submitting a monthly Separation Report to all system owners for appropriate action. DCFO regularly provides HR/EX with updates to the system owner distribution list. This list includes designated points of contact as determined by System and Business Managers throughout the Department.”

(U) The response further stated, “At the time of origin, the Report was based upon the *effective* Date of Separation as recorded in the Global Employment Management System, GEMS. Due to the appearance of a gap in the data when individual actions were not processed in a timely manner by bureaus, HR/EX revised the report logic so that, since January 2012, it has been based upon the *processed* date. The report, of course, continues to show the effective date so that system owners can take proper action. Due to the fact [that] the requested HR report is in place and is distributed to system owners on a monthly basis, DGHR respectfully requests that this recommendation be removed or closed.”

~~(SBU)~~ **OIG Reply.** The process HR explained indicates that HR is taking action to address the issue of a process for notifying system owners of departing employees, but there is a breakdown in the process. OIG determined that although monthly Separation Reports are being submitted, system administrators were not receiving the results. IRM, in coordination with HR, should determine why the monthly reports are not being received.

~~(SBU)~~ This recommendation is unresolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IRM, in coordination with HR, has implemented actions to notify system owners of the personnel changes.

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Chief Information Officer (CIO) require system owners to annually revalidate user and administrator accounts, remove

³⁰ (U) Ibid.

those accounts that no longer require access, and certify to the CIO that revalidation has been completed.

~~(SBU)~~ **Management Response.** IRM “substantively agree[d]” with the recommendation, stating that “[s]ystem owners will receive clear guidance to annually revalidate user and administrator accounts and remove those accounts that no longer require access.”

~~(SBU)~~ **OIG Rely.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts the guidance issued to system owners pertaining to annual revalidation requirements.

~~(SBU)~~ **Recommendation 8.** OIG recommends that the Bureau of Consular Affairs (CA), Office of Consular Systems and Technology, provide additional guidance to key users of CA’s applications at post to ensure that consular managers and other key users of those applications understand administrative features related to creating and managing user accounts for consular applications.

~~(SBU)~~ **Management Response.** CA agreed with the recommendation, stating that it and its Office of Consular Systems and Technology and Office of the Executive Director are “working to develop standard guidance for consular managers and key application users to safeguard the integrity and accountability of consular processes.” CA further stated that it “will establish consistent procedures for regularly reviewing, validating, and decommissioning user accounts, as well as adding, deleting, and modifying user roles to ensure all users have appropriate access based on clearance level, citizenship status, organization, and need to know.”

~~(SBU)~~ **OIG Reply.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts guidance issued to consular managers and key application users to safeguard the integrity and accountability of consular process.

~~(SBU)~~ **Finding D. System Administrator Activities Are Not Monitored Effectively**

~~(SBU)~~ OIG determined, for all 16 major applications it reviewed, that audit logs pertaining to system administrator activities were not being reviewed monthly by ISSOs, as required by the FAM.³¹ System administrators stated that because of limited staff, there was an operational need to provide all system administrators with the same permissions to enable other system administrators to perform the necessary tasks to continue operations when other administrators were not available. However, when systems administrators all have the same level of privileged access to system resources and there is no effective oversight over their activities, ~~(b) (5)~~

~~(b) (5)~~ Without periodic reviews of audit logs of administrator activity, potential security incidents may not be detected and resolved in a timely manner.

³¹ (U) 12 FAM 629.2-7, “Establishing and Review of Audit Trails/Logs.”

~~(SBU)~~ **Recommendation 9.** OIG recommends that the Chief Information Officer institute a formal process to require system owners to certify that the Information Systems Security Officer has reviewed audit logs monthly in order to detect and resolve potential security incidents in a timely manner.

~~(SBU)~~ **Management Response.** IRM agreed with the recommendation, stating, “The ISSO and key system administrators of owning sites will be required to review audit logs monthly in order to detect and resolve potential security incidents in a timely manner.”

~~(SBU)~~ **OIG Reply.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that ISSOs and key system administrators are reviewing audit logs monthly.

~~(SBU)~~ **Finding E. Patch Management Program for Databases Is Not Effective**

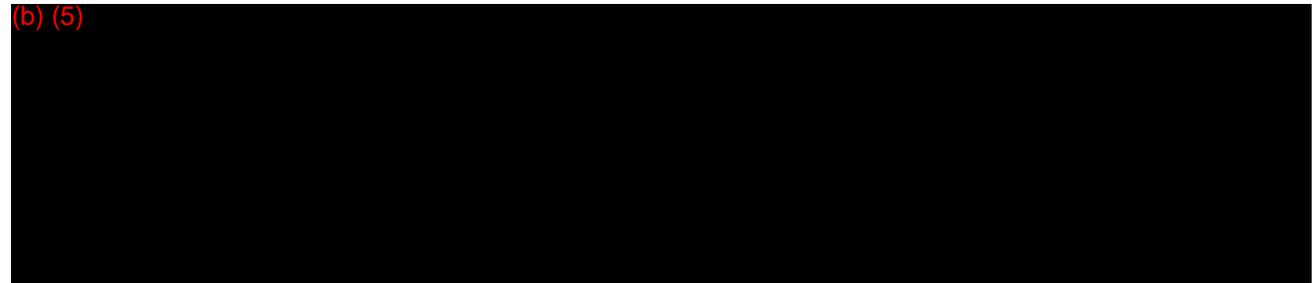
~~(SBU)~~ From a sample of 19 applications, OIG performed an automated vulnerability assessment of databases related to 13 applications: seven applications from CA, four applications from DS, and two applications from the Office of the Executive Secretary (ES). Based on its review, OIG determined that the Department did not have an effective patch management program for databases relating to six CA applications, four DS applications, and one ES application. (b) (5)



(U) The FAM³³ requires that system administrators follow guidelines and procedures established by the Department’s Enterprise Patch Management Program (EPM) and apply patches in an expeditious manner.

~~(SBU)~~ Specifically, OIG found 11 patching issues from its assessment of the databases related to the following 13 applications reviewed:

(b) (5)



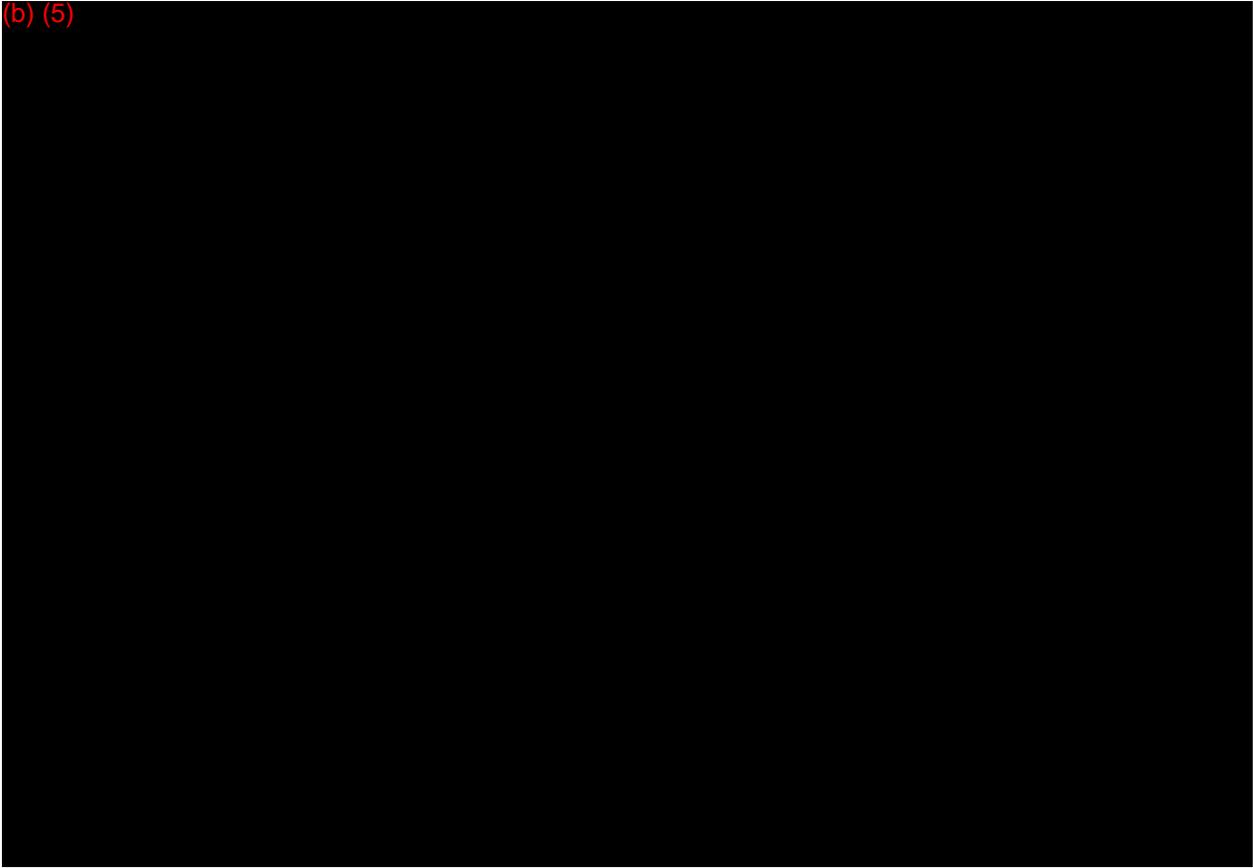
(b) (5)



³³ (U) 5 FAM 866, “Patch Management.”

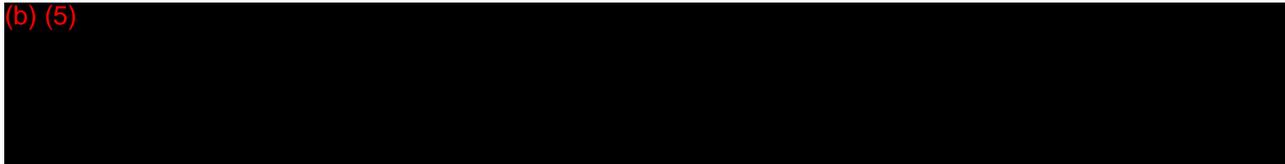
³⁴ (U) The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions are known as “patches,” “hot fixes,” and “service packs.”

(b) (5)



- (U) Secretariat Telegram Processing System (STEPS II) – No patching issues were found with this database.

(b) (5)

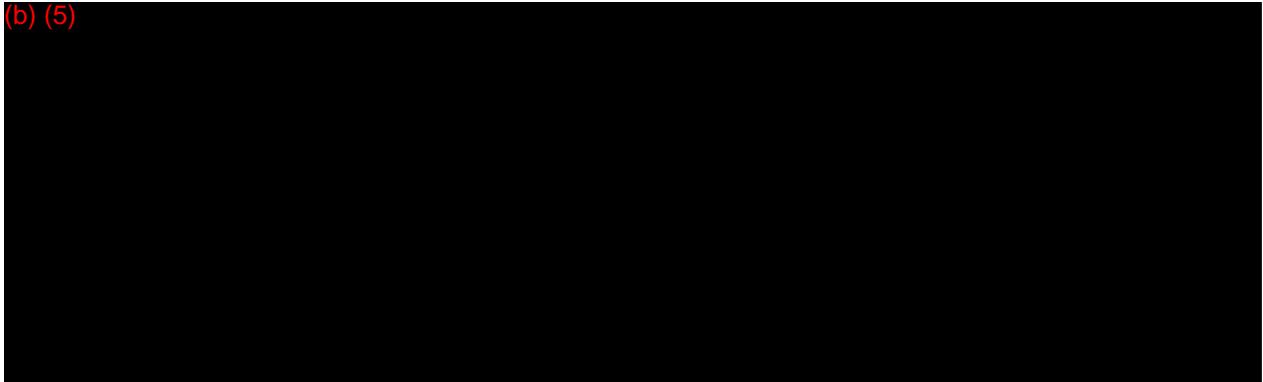


(U) The Department is a key steward of sensitive information such as passport records. Up-to-date database patch installation can help mitigate vulnerabilities associated with flaws in software code that may lead to unauthorized access to sensitive data.

(b) (5)



(b) (5)



(U) The 19 major applications reviewed and their related finding areas are shown in Figure 1.

~~(SBU)~~ **Figure 1. List of Major Applications and Related Finding Areas**

Applications	Findings						
	A	B ^a	C			D	E
			i ^b	ii ^c	iii ^d		
Automated Biometric Identification System (ABIS) ^e							
Consular Consolidated Database (CCD)			√	√	√	√	√
Consular Electronic Application Center (CEAC) ^f						√	√
Consular Lookout and Support System (CLASS)							√
Crisis Emergency Planning Application Classified (CEPA-C)			√	√		√	√
Electronic State Configuration Resource-ClassNet (e-SCORE)			√	√		√	
Investigative Management System (IMS-C)			√	√		√	√
Net-Centric Diplomacy (NCD)	√		√	√		√	
Passport Information Electronic Records System (PIERS)			√	√	√	√	√
Secretariat Telegram Processing System (STEPS II)			√			√	
Secretariat Tracking and Retrieval System (STARS)			√			√	√
Secure Integrated Logistics Management System (S-ILMS)				√		√	
Security Incidents (SECINTS)			√	√		√	√
SMART Core Messaging-Classified (SMART-C)	√		√	√		√	
State Archiving System 2 (SAS 2)			√	√		√	
SY Namecheck (SYNCH)			√	√		√	√
The Office of Foreign Missions information			√	√		√	
Travel Document Issuance System (TDIS)							√
Visa Opinion Information Service (VOIS)			√	√		√	√

^(U) ^a Finding B is not specific to any application.

~~(SBU)~~ ^b Removing user and administrator access.

~~(SBU)~~ ^c Account revalidation.

^(U) ^d See section “Account Management Issues With Bureau of Consular Affairs Applications” in report.

^(U) ^e OIG understood that CLASS and ABIS are back-end processing applications, so these applications were not manually reviewed by OIG. TDIS was not reviewed because of the geographical distribution of its user base and OIG resource limitations. However, OIG performed a vulnerability scan on these applications’ databases.

^(U) ^f CEAC is a public facing Web site. OIG’s limited manual review areas applied to this application. However, OIG performed a vulnerability scan on its database.

^(U) Source: OIG analysis.

(U) List of Recommendations

~~(SBU)~~ **Recommendation 1.** OIG recommends that the Chief Information Officer acquire the technical resources and implement the enhancements identified by the Net-Centric Diplomacy (NCD) team in NCD.09.00.00 Plan of Action, dated February 12, 2012, to ensure that users do not have broader access to cables than what is required to perform their duties.

~~(SBU)~~ **Recommendation 2.** OIG recommends that the Chief Information Officer establish standard training requirements for post Classified State Messaging and Archive Retrieval Toolset (SMART-C) and ensure that system administrators receive required training before they are assigned and annually thereafter.

~~(SBU)~~ **Recommendation 3.** OIG recommends that the Chief Information Officer implement logical access controls to ensure that system administrators do not have the ability to read information within sensitive cables that they do not need to perform their administrative duties.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the Chief Information Officer equip the Net-Centric Diplomacy (NCD) and Classified State Messaging and Archive Retrieval Toolset (SMART-C) applications with audit trail capabilities to log user and administrator activity.

~~(SBU)~~ **Recommendation 5.** (b) (5)



(U) Recommendation 6. OIG recommends that the Bureau of Human Resources institute a formal process to notify system owners on a monthly basis of employee departures to ensure the timely removal of accounts of departing or transferring employees.

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Chief Information Officer (CIO) require system owners to annually revalidate user and administrator accounts, remove those accounts that no longer require access, and certify to the CIO that revalidation has been completed.

~~(SBU)~~ **Recommendation 8.** OIG recommends that the Bureau of Consular Affairs (CA), Office of Consular Systems and Technology, provide additional guidance to key users of CA's applications at post to ensure that consular managers and other key users of those applications understand administrative features related to creating and managing user accounts for consular applications.

~~(SBU)~~ **Recommendation 9.** OIG recommends that the Chief Information Officer institute a formal process to require system owners to certify that the Information Systems Security Officer has reviewed audit logs monthly in order to detect and resolve potential security incidents in a timely manner.

~~(SBU)~~ **Recommendation 10.** (b) (5)



(b) (5)



(U) Scope and Methodology

(U) The focus of this audit was to determine whether the Department had developed effective logical access controls around its major applications and related databases and provided management with timely results regarding the effectiveness of these controls.

(U) OIG interviewed application and systems administrators and obtained the necessary evidence and documentation to gain an understanding of logical access controls around the applications in the scope of the audit.

(U) In addition, OIG used commercial-off-the-shelf (COTS) database scanning software to perform database vulnerability assessments. OIG selected DbProtect, a product created by Application Security, Inc., and configured the software to utilize the built-in Defense Information Systems Agency Security Technical Implementation Guide for databases, which meets the requirements of the Department's database configuration policies. DbProtect was used to perform a vulnerability and configuration scan against a sample of the Department's databases and highlighted areas of risk and where database security process improvements were needed. Based on this analysis, the software provided detailed remediation instructions to eliminate database vulnerabilities and misconfigurations. OIG met with Database Administrators to validate the results to ensure that false positives were eliminated.

(U) To evaluate the adequacy of the logical access controls for the selected applications and related databases, OIG used the following criteria:

- (U) Department policies and procedures in the *Foreign Affairs Manual* (FAM).
- (U) Office of Management and Budget (OMB) Circular No. A-130, Appendix III.¹
- (U) National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Publications Standards (FIPS).
- (U) Memorandum M-11-06, Memorandum for the Heads of Executive Departments and Agencies, "WikiLeaks—Mishandling of Classified Information," November 28, 2010.

(U) The Office of Inspector General (OIG) performed this audit from December 2011–May 2012 in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

(U) OIG discussed its findings and proposed recommendations with officials from the Department of State's (Department) Bureau of Administration, the Bureau of Diplomatic Security (DS), the Bureau of Human Resources (HR), the Bureau of Information Resource Management (IRM), the Bureau of Intelligence and Research (INR), the Bureau of Overseas

¹ (U) OMB Circular A-130, *Management of Federal Information Resources*, app. III, "Security of Federal Automated Information Resources."

Buildings Operations (OBO), and the Executive Office of the Secretary on June 27, 2012. Additionally, management staffs at Embassy Buenos Aires (Argentina), Embassy Madrid (Spain), and Embassy Accra (Ghana) were briefed on preliminary findings on January 27, February 3, and February 10, 2012, respectively.

(U) Scope Limitation

(U) According to the FAM,² DS is responsible for conducting vulnerability assessments related to the Department's network systems. Since DS was already positioned to perform the network assessments, OIG made an effort to conduct database vulnerability scans as part of the access controls audit using DS infrastructure.

(U) To conduct database scans outside the DS domain, OIG requested and then created a new service account for its scanning tool DbProtect. However, this new service account lacked the necessary permissions on the DbProtect console to enable the tool to work properly. OIG requested that the newly created service account be added to the local administrative group on the console to give the tool the same rights that enabled it to scan databases within the DS domain. OIG determined that the new service account was never added to the local administrator group as requested. On the appointed scan date, DS officials told OIG that the newly created account had expired. DS officials attempted to recreate the account but were unable to do so within the timeframe required to meet the scanning schedule.

(U) Work Related to Internal Controls

(U) OIG performed steps to assess the adequacy of internal controls by performing manual and automated assessments of logical access controls around major applications and related databases. For example, OIG conducted manual assessments at three embassies, including determining whether accounts were properly authorized, periodic account revalidation was performed, concept of least privilege was implemented, adequate oversight existed over system administrators, and the Department's patch management program for database management systems was effective. Furthermore, OIG used an industry-recognized vulnerability assessment tool to test logical access control weaknesses in the databases related to the major applications in the scope of this report. The assessment tool was configured to utilize the Department's standard database security configuration settings as a basis for identifying any logical access control weaknesses. OIG validated the results of the assessment with database administrators to ensure that certain application-dependent settings identified by the tool as a finding were ruled out.

(U) The internal control deficiencies identified during this audit are detailed in the "Audit Results" section of this report.

² (U) 12 FAM 615.1, "Assistant Secretary, Bureau of Diplomatic Security (DS)."

(U) Use of Computer-Processed Data and Data Reliability

(U) To assess the reliability of computer-processed data, OIG reviewed electronic documentation related to the data sources and performed tracing of data to source documentation. More specifically, OIG obtained, from IRM, a listing of major applications and then verified the accuracy of this list by confirming the existence of each application on the list in Information Technology Asset Baseline (ITAB), the Department's official inventory of major applications. From these efforts, OIG determined that the data were sufficiently reliable to support the conclusions and recommendations in this report.

(U) Detailed Sampling Methodology

(U) OIG's sampling objective was to assess the effectiveness of logical access controls around the Department's major applications. Specifically, the testing of a sample of major applications will assist in determining whether logical access controls are in place and operating effectively.

(U) This work was conducted at the domestic bureaus and the three embassies listed. The applications selected for review were obtained using a nonstatistical sampling method known as judgmental sampling. Because this method uses discretionary criteria to effect sample selection, the audit team was able to use information garnered during its preliminary work to aid in making informed selections.

(U) Prime considerations in selecting the three overseas sites included the geographical distribution of the posts, the recency of OIG site visits, and the nature of the controls to be evaluated. The major applications under review and their related application controls have been generally implemented uniformly at all overseas posts; consequently, OIG was able to gain a perspective of overseas conditions pertaining to the design and operating effectiveness of these controls in general from visiting these three locations.

(U) Identification of Population and Selection of Samples

(U) After identifying ITAB as the Department's official inventory of major applications, OIG requested and received from IRM a listing of all active major applications as of April 5, 2011. The sum of the inventory, or population, was 197 applications.

(U) In ITAB, the major applications are generally assigned to one of three categories—High, Moderate, and Low—based on their potential impact level.³ However, OIG noted that some applications in the population did not have an assigned category; consequently, a fourth category was added.

(U) To attain the maximum audit coverage given the available resources, OIG grouped the entire population of 197 applications into the four categories and then judgmentally

³ (U) FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," Feb. 2004.

determined the number of applications to sample and review from each category based on various factors. For instance, OIG opted to review all of the applications in the High category because of the relatively small number of applications in that group and their potential impact. For all the other categories, however, a sample of the applications was selected for review, and this was generally accomplished randomly, although this was not always the case. For the Moderate category, four applications were selected for the original sample. Two of these applications were selected randomly, and the other two applications, Passport Information Electronic Records System (PIERS) and the Travel Document Issuance System (TDIS), were selected purposely since they had been selected for audit in an audit plan for a prior year but had to be deferred because of resource constraints. All 35 of the original samples were selected in this manner, and OIG ultimately sampled and reviewed only 19 of the original samples shown in Table 1.

(U) Table 1. Population and Samples for the Department’s Major Applications

Category	Population Total	Original Sample Size	Exclusions From Original Sample	Final Sample Size
High	28	27*	10	17
Moderate	125	4	2	2
Low	17	2	2	0
Uncategorized	27	2	2	0
Total	197	35	16	19

*Although DS Source was in ITAB, the official inventory of the Department’s major applications, it was excluded from the original sample because it resides on the U.S. Government’s SIPRNet and not on the Department’s Network. This effectively reduced the population of “High” applications from 28 to 27.

(U) Descriptive information on the original sample of 35 major applications, which subsumes the final sample actually reviewed by OIG of 19 applications, as well as explanations for the exclusion of 16 applications from the final sample, are provided in Table 2.

~~(SBU)~~ **Table 2. Original and Final Samples of the Department’s Major Applications**

System	ITAB Description	Excluded From or Included in the Final Sample
Secure Integrated Logistics Management System (S-ILMS)	Secure ILMS is a secure version of ILMS. S-ILMS is a Web-based system that will enhance the Department's ability to manage its requisitioning, procurement, receiving, and distribution on the classified network (ClassNet).	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see “Scope Limitation” in this appendix).
State Archiving System 2 (SAS 2)	SAS2 provides access to the Department’s automated Central Foreign Policy File. SAS2 captures all significant substantive reporting between the Department and its overseas posts.	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see “Scope Limitation” in this appendix).
Automated Biometric Identification System (ABIS)	ABIS is a Commercial Off-the-Shelf (COTS) product developed by Identix Incorporated. The ABIS system is an enterprise-level facial-recognition matching program.	Included in final sample.

~~**SENSITIVE BUT UNCLASSIFIED**~~

System	ITAB Description	Excluded From or Included in the Final Sample
Consular Affairs Classified Intranet (CACLI)	The CACLI Web site was the direct result of a congressional mandate requiring a consolidated repository of information pertaining to terrorist trends and activities to be utilized by consular personnel.	Excluded because application was retired during audit.
Consular Consolidated Database (CCD)	The Consular Consolidated Database is a set of databases located in Washington, DC, that hold all current data and all archived data from all CA post databases around the world.	Included in final sample.
Consular Electronic Application Center (CEAC)	The Consular Electronic Application Center is an Internet-based full service application service center whereby applicants for visa services can complete and submit an application.	Included in final sample.
Consular Lookout and Support System (CLASS)	The Consular Lookout and Support System (CLASS) is used by passport agencies, consulates, and border inspection agencies to perform name checks on visa and passport applicants in support of the issuance process.	Included in final sample.
Visa Opinion Information Service (VOIS)	VOIS is a .NET Web application with single sign-on authentication provided by the Consular Consolidated Database (CCD) DataMart.	Included in final sample.
AlarmNet	AlarmNet provides the connectivity for the Department of State Domestic Access Control and Intrusion Detection system. It is the backbone of the system that lets you into the building.	Excluded because of resource constraints.
Crisis Emergency Planning Application Classified (CEPA-C)	CEPA-C assists posts in the development of their emergency action plans according to the new Emergency Planning Handbook.	Included in final sample.
Freedom of Information System (FOIA)	The Freedom of Information Act (FOIA) Case Tracking System is a fully automated system designed to easily track and maintain all case information and activities resulting from requests for information.	Excluded because application was retired during audit.
Investigative Management System (IMS-C)	IMS-C captures all classified case-related information; automates, integrates, and improves DS's investigative business processes; establishes a central index encompassing all DS classified investigations; and provides investigative and/or intelligence analysis and analytical processing while creating internal and external electronic data sharing.	Included in final sample.

~~SENSITIVE BUT UNCLASSIFIED~~

System	ITAB Description	Excluded From or Included in the Final Sample
Post Security Profile Application (PSPA)	The Post Security Profile Application (PSPA) will support the DS's mission. PSPA stores crisis plans for posts worldwide.	Excluded because application was retired during audit.
Security Incidents (SECINTS)	Provides a method of tracking violations reported on the handling, storage, and reproduction of information as well as the protection of automated information systems.	Included in final sample.
SY Namecheck (SYNCH)	SYNCH, which is owned and maintained by DS, automates the tasks associated with tracking personnel clearance status and clearance folder locations.	Included in final sample.
The Office of Foreign Missions Information System (TOMIS)	The Office of Foreign Missions Information System (TOMIS) is an integrated, custom application system designed to support Office of Foreign Missions (OFM) and Chief of Protocol (S/CPR) activities.	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see "Scope Limitation" in this appendix).
COMSEC Accounting Reporting and Distribution System (CARDS)	CARDS is required to support the Department's electronic Black Key Distribution System (BKDS) and Communications Security (COMSEC) accounting and inventory functions worldwide via ClassNet.	Excluded because of resource constraints.
Electronic State Configuration Resource – ClassNet (ClassNet e-SCORE)	This is a Web-based configuration management system for Department information technology (IT) hardware and software domestically and overseas. ClassNet e-SCORE contains classified post information, and component-level IT hardware and software information.	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see "Scope Limitation" in this appendix).
Machine Readable Travel Document Public Key Infrastructure and Signature Delivery Service (MRTD PKI and SDS)	The Machine Readable Travel Document (MRTD) Public Key Infrastructure (PKI) is a system of hardware, software, and policies that enables digital signing of data embedded on electronic passports.	Excluded because of resource constraints.
Net-Centric Diplomacy (NCD) ^a	The NCD system is designed expressly to share diplomatic reporting information with the Department and the interagency community on the U.S. Government's SECRET network, accessible to all Department employees through the Department's ClassNet network.	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see "Scope Limitation" in this appendix).
Public Key Infrastructure and BLADE (PKI/BLADE)	The Department's Public Key Infrastructure is a system of hardware, software, and policies that provide an infrastructure enabling both digital signature and strong	Excluded because of resource constraints.

~~**SENSITIVE BUT UNCLASSIFIED**~~

System	ITAB Description	Excluded From or Included in the Final Sample
	cryptography across the enterprise.	
SMART Core Messaging-Classified (SMART-C)	SMART is a software integration and development project to reengineer and modernize the formal and working messaging processes and systems in the Department. SMART Core Messaging provides direct, secure, and controlled communication to employees worldwide and to other Government agencies.	Included in final sample, but OIG was not able to perform all the work originally planned because of a scope limitation (see “Scope Limitation” in this appendix).
ProjNet-C	ProjNet-C is the classified version of ProjNet. ProjNet facilitates construction project design reviews. Design documents for specific construction project are made available on a need-to-know basis through a secure extranet allowing on-line collaboration between architecture firms and OBO staff.	Excluded because of resource constraints.
Chief of Mission and Special Embassy Programs Database (CSEP)	This automated application supports the information requirements of the Chiefs of Mission Authority, National Security Decision Directive-38, and the Office of Rightsizing (M/MR). The database maintained by this application contains detailed data on full-time permanent American Department of State positions.	Excluded because of resource constraints.
Secretariat Tracking and Retrieval System (STARS)	STARS is a critical application that tracks approximately 70,000 foreign policy memoranda (action, briefing, and information) and correspondence for the Secretary and six Principal Officers of the Department. STARS provides a store of document images.	Included in final sample.
Secretariat Telegram Processing System (Second Edition) – (STEPS II)	STEPS stores, handles, and routes telegrams. Designed to help deliver telegrams to the Principals and other appropriate offices as quickly as possible. Receives telegrams from the State communications center and disseminates them to POEMS users.	Included in final sample.
WREN	The Secretary's Worldwide Remote Email Network (WREN) provides the Secretary with a mobile communications package in support of a fully transportable computer network.	Excluded because of resource constraints.
Electronic Visa Application Form (EVAF)	EVAF is an on-line version of form DS-156 for the Internet. Applicants are able to enter data directly into the on-line data entry forms and then generate and print the completed	Excluded because of resource constraints.

~~**SENSITIVE BUT UNCLASSIFIED**~~

System	ITAB Description	Excluded From or Included in the Final Sample
	application forms for presentation to post.	
Remote Data Entry System (RDS)	RDS is used overseas to assist in the collection on nonimmigrant visa applicant data. There are two application components: RDS Client Software and RDS Server Software. The RDS Client software is distributed to remote sites outside the Consulates. The server software is used to connect to the Non-Immigrant Visa (NIV) database over the network and upload data collected by the client software.	Excluded because application was retired during audit.
Passport Information Electronic Records System (PIERS) ^b	The PIERS system, PIERS Query, replaces Passport Files miniaturization Web (PFM Web) and Passport Files Miniaturization (PFM). PIERS Query is the single Web portal for all passport data.	Included in final sample.
Travel Document Issuance System (TDIS) ^c	TDIS is the Parent for the automated passport system that issues electronic machine-readable passports domestically in conformance with worldwide standards established by the International Civil Aviation Organization (ICAO).	Included in final sample.
Budget Allocation Tracking System (BATS)	The Budget Allocation Tracking System (BATS) is an HROnline component application used for tracking and controlling HR budgets, commitments, obligations, and expenditures against the various HR appropriations, allotments, organizations, functions, and object codes.	Excluded because of resource constraints.
F-77	The F-77, "Report of Potential Evacuees," is submitted by all Foreign Service posts. The reports provide detailed data on the number and location of American citizens and other potential evacuees abroad.	Excluded because of resource constraints.
Consular Visa Systems (CVS) ^d	The visa consolidation program is a strategic effort that will transform and modernize the systems supporting visa operations domestically at Department headquarters, the Kentucky Consular Center (KCC), the National Visa Center (NVC), and overseas at all visa processing posts.	Excluded because of resource constraints.
Executive Agency Personnel Support (EAPS)	The Executive Agency Personnel Support (EAPS) system is a Web-based application used to review, validate, audit, and continuously manage individual agencies'	Excluded because of resource constraints.

~~**SENSITIVE BUT UNCLASSIFIED**~~

System	ITAB Description	Excluded From or Included in the Final Sample
	overseas personnel, assignment, and position data.	

^a ~~(SBU)~~ This application was the source of the Wikileaks Department of State documents.

^b (U) This system had previously been selected for audit as a followup to report *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) and therefore was not part of the random sample.

^c (U) Ibid.

^c (U) This application has since been withdrawn.

(U) Source: OIG analysis.

(U) Office of Inspector General Reports Related to Audit

(U) Reports issued by the Office of Inspector General (OIG), Office of Audits, identified areas of weaknesses in access controls.

- (U) *Review of Department of State Information Security Program* (AUD/IT-11-07, November 2010)

(U) In this review, OIG found that the application software that controls access to OpenNet Everywhere (ONE) software, which is the Department of State's (Department) remote access tool, was configured to allow the use of a non-NIST compliant encryption algorithm.¹ Additionally, OIG found that ONE was not configured to terminate a user's online session after 20 minutes of inactivity. The *Foreign Affairs Manual*² (FAM) requires remote access program managers to configure the remote session to terminate "after 20 minutes of inactivity." OIG is awaiting confirmation on the status of the related recommendations from the Department.

(U) Further, OIG found issues with the Department's continuous monitoring program, including access controls around applications. Specifically, OIG found that scanning tools used by the Department do not assess Oracle configurations for control weaknesses, which could adversely impact application access controls. Scanning results for routers, firewalls, and Demilitarized Zone servers are therefore not captured in iPost, the Department's main continuous monitoring tool.

- (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)

(U) In this review, OIG found that the Department had not implemented adequate controls to prevent or detect unauthorized access, similar to those controls in place at the Internal Revenue Service and the Social Security Administration. At those two agencies, large amounts of electronic Personally Identifiable Information (PII) are protected by access controls, such as having tiered user access permissions for granting access at level needed (for example, limited to full), blocking user access from certain records, and conducting audits of access activity logs. The related recommendation has not been closed as of June 2012.

(U) OIG's Office of Inspections issued one report related to the current audit that identified access weaknesses.

¹ (U) *Information Security Program at the Department of State* (AUD/IT-11-07, Nov. 2010).

² (U) 12 FAM 682.2-3, "Configuring Remote Access Accounts."

- (U) *Inspection of the Bureau of Consular Affairs, Office of Consular Systems and Technology* (ISP/I-11-51, May 2011)

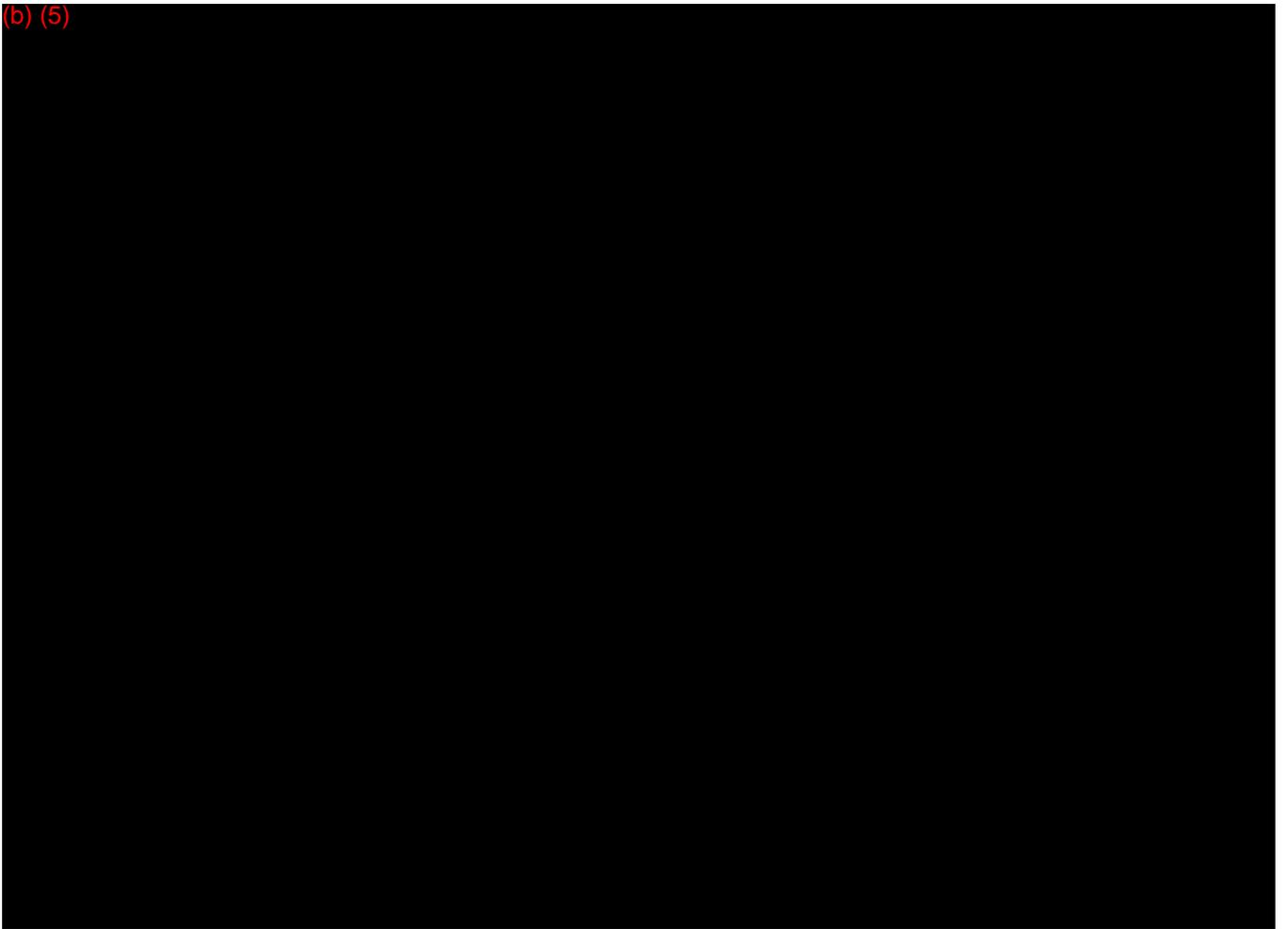
(U) Access control weaknesses were noted in this report. One key judgment noted was the following: “Access controls for assigning and tracking user accounts in various critical systems in the Office of Consular Systems and Technology (CST) need to be strengthened.” Specifically, the report noted, among other weaknesses, that Government supervisors were not able to verify that contractor Database Administrator (DBA) roles and responsibilities accurately reflected their assigned duties. Therefore, the potential existed for a developer or DBA to perform other activities such as testing and/or migrating changes to production without anyone being aware of these actions, which leads to inadequate separation of duties issues. Also, the contractor DBA’s user accounts are created and monitored by contractors themselves. Although CST government management approval is required at the initial user access request, there is no regular Government staff review to ensure that continued access is necessary for contract staff. The report identified two recommendations related to access controls that were unresolved as of June 2012.

~~(SBU)~~ **Proposed Net-Centric Diplomacy Security Enhancements**

~~(SBU)~~ The Net-Centric Diplomacy (NCD) team has initiated an application redesign project aimed at enhancing the security posture of NCD. Per a plan of action provided to the Office of Inspector General (OIG) by the NCD team (NCD.09.00.00 Plan of Action dated February 12, 2012), the purpose of the redesign effort was to make software modifications to enhance the security posture of NCD.

~~(SBU)~~ The key software security requirements identified and to be addressed in the redesign effort included the following:

(b) (5)





United States Department of State

Washington, D.C. 20520

August 22, 2012

MEMORANDUM

TO: OIG – Ms. Evelyn Klemstine
 OIG – Mr. Jerry Rainwaters

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

SUBJECT: OIG Audit of Department of State Access Controls for Major
 Applications, AUD/IT-12-44, August 2012

The purpose of this memorandum is to provide a response to the subject audit. IRM comments on recommendations 1, 2, 3, 4, 7, 9 and 10 are attached.

IRM concurs with most, but not all, OIG recommendations associated with the subject audit. Recommendation 4 references both NCD and SMART-C, so IRM's response has been split to address NCD and SMART-C, separately.

Audit of the Department of State Access Controls for Major Applications
AUD/IT-12/44
August 2012

Recommendation 1: OIG recommends that the Chief Information Officer acquire the technical resources and implement the enhancements identified by the Net-Centric Diplomacy (NCD) team in NCD.09.00.00 Plan of Action, dated February 12, 2012, to ensure that users do not have broader access to cables than what is required to perform their duties.

IRM Response: IRM concurs with the recommendation to acquire the necessary technical resources to implement the NCD.09.00.00 Plan of Action. As of June 11, 2012, these resources have been acquired and a full team of developers is in place and actively working on the NCD.09.00.00 software release.

Certain security enhancements identified in the NCD.09.00.00 Plan of Action – such as those to ensure users do not have broader access to cables than required to perform their duties – were implemented in an incremental release to NCD (version 8.5.2). This release mitigates the major risks identified in the NCD Certification and Authorization (C&A) process and allows IRM the authority to continue operating NCD while moving forward with NCD.09.00.00 development to address the remaining security enhancements and open defects. The scheduled release date of this new NCD version is January, 2013. The original scheduled release date of NCD .09.00.00 for October 2012 was postponed to address the major risks identified during the C&A.

Recommendation 2: OIG recommends that the Chief Information Officer establish standard training requirements for post Classified State Messaging and Archive Retrieval Toolset (SMART-C) and ensure that system administrators receive required training before they are assigned and annually thereafter.

IRM Response: IRM concurs with Recommendation 2. FSI established week-long classroom and long distance system administrator training based on training requirements from IRM. As well, IRM has developed the draft SMART Messaging Guidebook, currently under review by IRM/BMP/GRP/GP for publication, which provides specific guidance on the proper handling of sensitive

captions and cables for translation into RBAC provisioning for each user. There is also an extensive online catalog of documentation and videos for training.

Additionally IRM will restate its expectation that all system administrators take FSI's system administrator training and annually re-familiarize themselves with the material.

Recommendation 3: OIG recommends that the Chief Information Officer implement logical access controls to ensure that system administrators do not have the ability to read information within sensitive cables that they do not need to perform their administrative duties.

IRM Response: IRM does not concur with Recommendation 3. System administrators have access to all incoming and outgoing messages, the former to redirect dissemination if required, the latter to ensure compliance with State Department standards for formatting and application of metadata (e.g., captions). Because SMART standardizes formatting and metadata, there are fewer messages that require administrator access. Nonetheless, to ensure the timely delivery of traffic in the case of user or system error, there is no class of message to which an administrator can be logically denied access. SMART logs provide a record of message access through dissemination and search by all employees, including system administrators. Additionally, administrators at a post can only view and access incoming and outgoing traffic at assigned posts, they do not have access outside their post unless specifically granted. A post user can see another post's cables only if the SMART administrator at the original post grants them access.

Due to the critical mission functions of Embassies abroad, and the impact upon safety issues, Foreign Service Information Technology personnel are required to have full administrative access to all systems. In the event of local crisis such as civil disorder, each Foreign Service IT officer must be able to perform each other's technical duties.

The same principle applies domestically with respect to core functions of IRM, such as SMART. Unrestricted administrative access to the SMART database ensures each administrator can respond in an immediate manner to troubleshoot issues related to this core function upon which key Department decision makers are dependent to perform the Department's mission critical functions as identified by the Office of Emergency Management.

Recommendation 4: OIG recommends that the Chief Information Officer equip the Net-Centric Diplomacy (NCD) and Classified State Messaging and Archive Retrieval Toolset (SMART-C) applications with audit trail capabilities to log user and administrator activity.

IRM Response: IRM concurs with recommendation 4 in reference to Net Centric Diplomacy (NCD). As of May 31, an audit trail capability has been implemented in NCD. With this capability, NCD administrators are now auditing the following user activities: Login, Logout, File Opened, Read Cable, Print Cable, Search Query, File Modified, File Deleted, and File Download. NCD system administrators receive an Email alert whenever any of these auditable events exceed a pre-defined limit. If, after analyzing the alerts, any suspicious activity is identified, users are prohibited from performing these operations for an administrator-determined period of time. This allows time to investigate the activity.

As part of the daily administration of NCD, two system administrators review the audit logs for each NCD server. They are monitoring the above activities along with indications of unauthorized changes to the configuration settings and attempts to execute unauthorized software within the NCD system. The audit logs are backed up daily and retained for 6 months in accordance with NIST requirements and State Department IT security policy.

IRM concurs with Recommendation 4 in reference to Classified State Messaging and Archive Retrieval Toolset (SMART-C). The audit log contains ALL administrative changes to SMART. Both MSMC and post administrators have access to the audit log from the main SMART page. The SMART audit log provides a record of actions performed on the SMART database and allows administrators (both MSMC and Post) to find actions based on when they occurred, who performed them, the users affected by them, text within the actions, and other criteria.

IRM, in consultation with DS, will continue to seek commercial or custom solution, but to date has been unable to find a COTS product that will validly detect anomalies. Commercial systems look for departures from routine practices, e.g., a credit card user begins charging high-value items in a different country. However patterns of standard usage among State Department SMART users are so different that we do not have a norm from which variance might trigger an alert.

Recommendation 7: OIG recommends that the Chief Information Officer (CIO) require system owners to annually revalidate user and administrator accounts, remove those accounts that no longer require access, and certify to the CIO that revalidation has been completed.

IRM Response: IRM substantively agrees with the recommendation. System owners will receive clear guidance to annually revalidate user and administrator accounts and remove those accounts that no longer require access. Additionally, this guidance will be incorporated into role-based training for personnel with elevated privileges. IRM will continuously monitor stale user accounts to ensure that stale user account scoring in iPost occurs at each site level. This will allow site level owners to address stale accounts in their organizational units (OU). This change in iPost will occur in October of this calendar year.

Recommendation 9: OIG recommends that the Chief Information Officer institute a formal process to require system owners to certify that the Information Systems Security Officer has reviewed audit logs monthly in order to detect and resolve potential security incidents in a timely manner.

IRM Response: IRM agrees with the recommendation. The ISSO and key system administrators of owning sites will be required to review audit logs monthly in order to detect and resolve potential security incidents in a timely manner. Additionally, this guidance will be incorporated into role-based training for personnel with elevated privileges.

(b) (5)



~~SENSITIVE BUT UNCLASSIFIED~~

September 10, 2012

TO: OIG – Ms. Evelyn Klemstine
 OIG – Mr. Jerry Rainwaters

FROM: IRM/BMP/SO/SPD – Robert Glunt *RG*

SUBJECT: OIG Audit of Department of State Access Controls for Major
 Applications, AUD/IT-12-44, August 2012

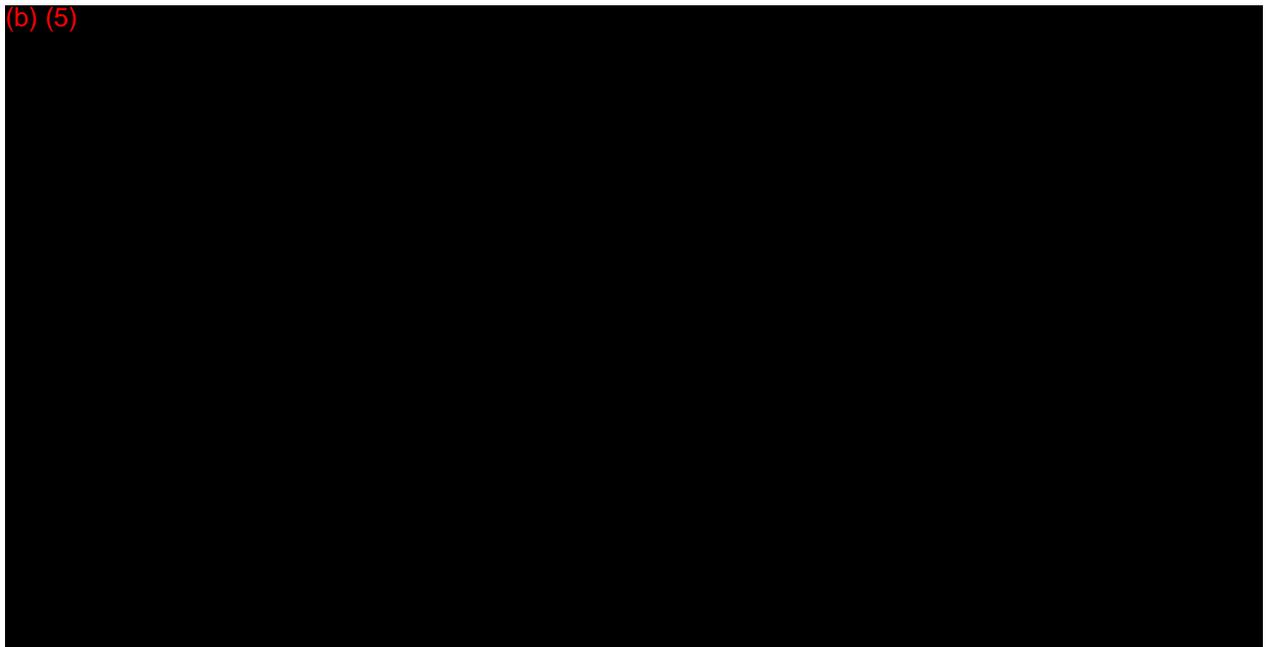
Attached please find IRM's updated response to OIG Recommendation 10, cleared by the Bureaus of Diplomatic Security and Consular Affairs.

IRM's response to recommendation 3, sent to the OIG on 8/22/12, was cleared by the Bureau of Diplomatic Security, without change.

SENSITIVE BUT UNCLASSIFIED

Audit of Department of State Access Controls for
Major Applications, Report # AUD/IT-12-44, August 2012

(b) (5)



~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

(SBU) Appendix E



United States Department of State

Washington, D.C. 20520

www.state.gov

SEP 07 2012

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from attachment)

**INFORMATION MEMO TO OIG – DEPUTY INSPECTOR GENERAL
HAROLD W. GEISEL**

FROM: DS – Eric J. Boswell 

SUBJECT: Compliance Response and DS Comments – Audit of Department of
State Access Controls for Major Applications, Report AUD/IT-12-44,
August 2012

(U) Attached is the Bureau of Diplomatic Security's comments and follow-up response to Recommendation 5 of the subject report.

Attachment:
As stated.

SENSITIVE BUT UNCLASSIFIED
(UNCLASSIFIED when separated from attachment)

~~SENSITIVE BUT UNCLASSIFIED~~

SENSITIVE BUT UNCLASSIFIED

**DS Comments to U.S. Department of State and the
Broadcasting Board of Governors Office
Inspector General Office of Audits
Audit of Department of State Access Controls for Major Applications
Report # AUD/IT-12-44, August 2012**

Comments & Corrections

1. **(SBU) OIG Report:** Table 2, center column, titled “Original and Final Samples of the Department’s Major Applications,” the entry for Investigative Management System (IMS-C) reads: (Page 22)

“IMS-C captures all classified case-related information; automates, integrates, and improves OIG’s investigative business processes; establishes a central index encompassing all DS classified investigations; and provides investigative and/or intelligence analysis and analytical”

DS Comment (09/06/2012): Please revise the entry to read:

“IMS-C captures all classified case-related information; automates, integrates, and improves DS’s investigative business processes; establishes a central index encompassing all DS classified investigations; and provides investigative and/or intelligence analysis and analytical”

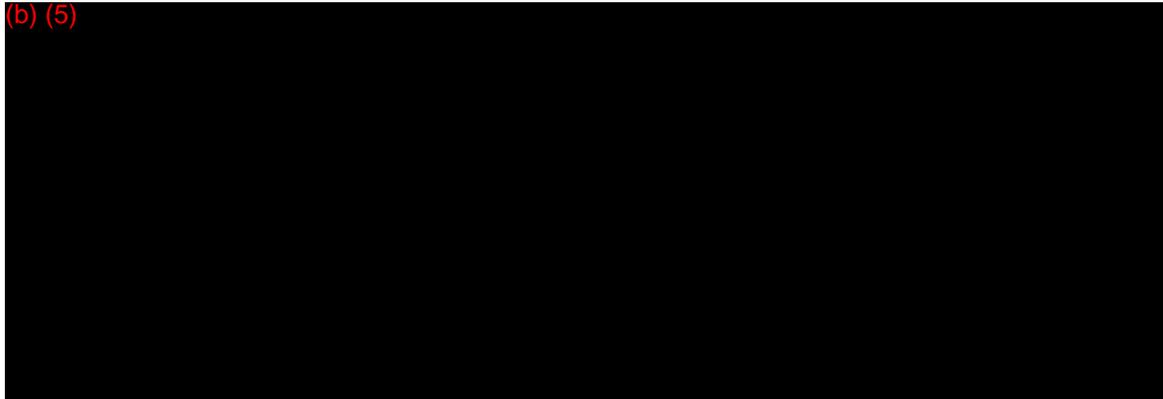
SENSITIVE BUT UNCLASSIFIED

~~SENSITIVE BUT UNCLASSIFIED~~

SENSITIVE BUT UNCLASSIFIED

Audit of Department of State Access Controls for
Major Applications
Report # AUD/IT-12-44, August 2012

(b) (5)



SENSITIVE BUT UNCLASSIFIED

~~SENSITIVE BUT UNCLASSIFIED~~



United States Department of State

Assistant Secretary of State
for Consular Affairs

Washington, D.C. 20520

UNCLASSIFIED

August 16, 2012

MEMORANDUM

TO: OIG – Harold W. Geisel, Acting

FROM: CA – James D. Pettit, Acting *JDP*

SUBJECT: Compliance Response to OIG Inspection on *Audit of Department of State Access Controls for Major Applications AUD/IT-12-44*

Thank you for the opportunity to submit a compliance response for Audit of Department of State Access Controls for Major Applications. CA is an action/coordinating entity on Recommendation 8. We have reviewed the recommendation in the report and have the following update:

Recommendation 8: The OIG recommends that the Bureau of Consular Affairs (CA), Office of Consular Systems and Technology, provide additional guidance to key users of CA's applications at post to ensure that consular managers and other key users of those applications understand administrative features related to creating and managing user accounts for consular applications. (Action: CA)

CA Response August 16, 2012: CA agrees with the recommendation. CA's Office of Consular Systems and Technology and Office of the Executive Director are working to develop standard guidance for consular managers and key application users to safeguard the integrity and accountability of consular processes. CA has looked in to consolidating existing user roles, and is developing guidance that will outline clear and consistent instructions for each role.

CA will establish consistent procedures for regularly reviewing, validating, and decommissioning user accounts, as well as adding, deleting, and modifying user roles to ensure all users have appropriate access based on clearance level, citizenship status, organization, and need to know.

UNCLASSIFIED



United States Department of State

Washington, D.C. 20520

MEMORANDUM

TO: IG – Mr. Harold W. Geisel, Acting

FROM: DGHR – Linda Thomas-Greenfield *LTG*

SUBJECT: Draft Report - Audit of Department of State Access Controls for Major Applications

Thank you for the opportunity to provide comment regarding the above-named OIG audit report draft. We would like to take this opportunity to respond to Recommendation 6.

Recommendation 6: OIG recommends that the Bureau of Human Resources institute a formal process to notify system owners on a monthly basis of employee departures to ensure the timely removal of accounts of departing or transferring employees.

DGHR Response:

Since 2010, HR/EX, through coordination with the office of the Managing Director of CGFS/DCFO (at that time RM/DCFO), has been submitting a monthly Separations Report to all system owners for appropriate action. DCFO regularly provides HR/EX with updates to the system owner distribution list. This list includes designated points of contact as determined by System and Business Managers throughout the Department.

At the time of origin, the Report was based upon the *effective* Date of Separation as recorded in the Global Employment Management System, GEMS. Due to the appearance of a gap in the data when individual actions were not processed in a timely manner by bureaus, HR/EX revised the report logic so that, since January 2012, it has been based upon the *processed* date. The report, of course, continues to show the effective date so that system owners can take proper action.

Due to the fact that the requested HR report is in place and is distributed to system owners on a monthly basis, DGHR respectfully requests that this recommendation be removed or closed.

(U) Major Contributors to This Report

(U) Jerry Rainwaters, Director
Division of Information Technology
Office of Audits

(U) Isaac Apea, Audit Manager
Division of Information Technology
Office of Audits

(U) Steve Matthews, Technical Lead/Audit Manager
Division of Information Technology
Office of Audits

(U) Oludayo Onafowokan, Senior IT Auditor
Division of Information Technology
Office of Audits

(U) Jamie Horvath, Senior IT Auditor
Division of Information Technology
Office of Audits

(U) Ernie Arciello, Statistician
Division of Audit Operations
Office of Audits

(U) Audrey Urbanczyk, Writer-Editor
Division of Audit Operations
Office of Audits

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

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 oig.state.gov

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

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~