~~SENSITIVE BUT UNCLASSIFIED~~

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

Memorandum
Report of Inspection

Summary of FY 2004 Information Systems Security Issues

Report Number IT-I-05-01, March 2005

~~IMPORTANT NOTICE~~

~~This report is intended solely for the official use of the Department of State or 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 or 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~~

TABLE OF CONTENTS

SUMMARY

The end of another year presents an opportunity for the Office of Inspector General (OIG) to report the most important information systems security concerns identified during the FY 2004 inspections. OIG inspected more than 40 posts and bureaus, gaining valuable insight into the Department of State's ongoing information systems security effort. Modernizing the global information technology (IT) systems, a move championed by Secretary Colin L. Powell and executed by the Chief Information Officer (CIO), is proving successful. Installing advanced information systems, however, must be met with an equivalent advancement in systems security. It is here where the Department can improve its performance.

The inspections of FY 2004 uncovered systems security issues that cross regional and bureau boundaries, allowing OIG to suggest several areas for improvement Department-wide. The Information Systems Security Officer (ISSO) program is struggling at several posts. Patch management procedures and other essential emergency planning and recovery documentation are missing or inadequate. Several change control boards (CCB) at posts are noncompliant with Department guidelines.[1] At the root of these and other problems, management's guidance and oversight of IT security practices needs improvement. OIG discusses these issues below and also provides an overview of the issues specific to the bureaus inspected in FY 2004.

[1] CCBs are local forums of IT staff and usually regional security officers (RSOs) who discuss software and hardware issues at posts and approve use of nonstandard software to support post operations, when fully justified.

GLOBAL SYSTEMS SECURITY ISSUES

INFORMATION SYSTEMS SECURITY OFFICER PROGRAM

The ISSO program is struggling to take hold in many locations. Roughly a third of the inspections reported shortcomings in the ISSO program, with many posts having severe infractions.[2] Common findings include the following:

- failure to perform and document random checks of user libraries and mailboxes for classified material stored on unclassified systems, to include checks for unapproved material (11 inspections);
- essential systems security documentation is missing or inadequate (15 inspections);
- users observed not locking workstations while away from their desk (five inspections);
- inadequate communication among management, U.S. and foreign service national IT personnel, and RSOs (five inspections);
- inadequate separation of duties among system managers, information management officers (IMOs), and ISSOs, leading to weak internal control of IT resources (11 inspections);
- incomplete coordination between IT and human resource (HR) staff to deactivate or delete user accounts of departing employees, especially for users with multiple accounts and administrative rights;
- a lack of proper enforcement not only of the policies in place, but also of management's responsibility to ensure that ISSO functions are properly carried out; and
- configuration settings that deviate from Department standards.

[2] A single inspection may include several geographic locations and include embassies and consulates general, or offices in the Washington bureaus.

In accordance with Department requirements (12 FAM 600), the ISSO is responsible for implementing the Department's information systems security program on all classified and unclassified automated information systems. He or she should advise the security officer on automated information systems security issues and work closely with the systems manager, other ISSOs, and the information programs officer. Throughout this process, the ISSO should ensure risk is mitigated to an acceptable level.

Most posts understood the importance of improving their ISSO practices. However, frequently posts were aware of inadequacies but did not have the staff to fully support the ISSO program. Deficiencies in the ISSO program were generally in two areas: (1) a lack of trained information systems security personnel, and (2) insufficient prioritization, guidance, oversight, and accountability from senior and middle management. It is the CIO's responsibility to provide the ISSOs with proper guidance to carry out their work requirements. The Enterprise Network Management Office (ENM) is developing a toolset to automate many of the ISSO's tasks. This is a welcome step to improve the program, but more must be done to fulfill the mandate issued more than four years ago to implement successful ISSO programs at every post (12 FAM 600).

Recommendation 1: The Chief Information Officer must ensure that the information systems security officer's duties and responsibilities are prioritized such that not fulfilling them translates into unacceptable performance for the information management officer and the information systems security officer.

Information Management and ISSO Oversight

IMOs at several posts appear unaware of all their security responsibilities. These managers are tasked with creating successful ISSO programs through proper training, guidance, and accountability. Their position descriptions often lack specific details regarding required IT security responsibilities. A successful information management and systems security program at post translates into a successful embassy evaluation.

Six inspections showed fragmentary or nonexistent work requirements for ISSOs. Eleven inspections revealed incomplete, nonexistent, or undocumented random checks of user libraries, documents, and mailboxes for unapproved material or classified material on unclassified machines. In four instances, inappropriate sexual material was found. Another site had more than 50 gigabytes of unapproved material on its servers, dramatically affecting backup times and wasting valuable resources.

Two sites had no ISSO program, in practice or in writing. Many other locations were not training their security staff to perform the most basic ISSO duties. Nearly every infraction was the result of inadequate training in or oversight of information systems security practices. Successful security programs require fully trained management and staff capable of the critical task of securing the Department's systems.

Communication among IT personnel at posts could also improve. Inspections showed numerous instances where problems could be avoided if IT staff had more open lines of communication.

The Department could benefit by drawing on the resources and success of the embassies to pull up the constituent posts within their domain. Improved regional support would also provide help to remote posts that need it but cannot justify additional full-time personnel. This is especially true of posts in Africa, which are not only short-handed, but whose less experienced specialists are required to accomplish more work. If the Department cannot staff the numerous hard-to-fill positions in a region, then it must increase the regional support to fill the gaps. OIG expects to release a report in 2005 regarding the support provided by Regional Information Management Centers (RIMC).

Overall, the quality of information management and ISSO oversight at posts is poor. The ISSO program at posts is lacking the adequate training and oversight of information systems security practices needed to be effective.

Recommendation 2: The Chief Information Officer should coordinate with the Director General to ensure that position descriptions for the information management officers include specific details regarding required information technology security responsibilities.

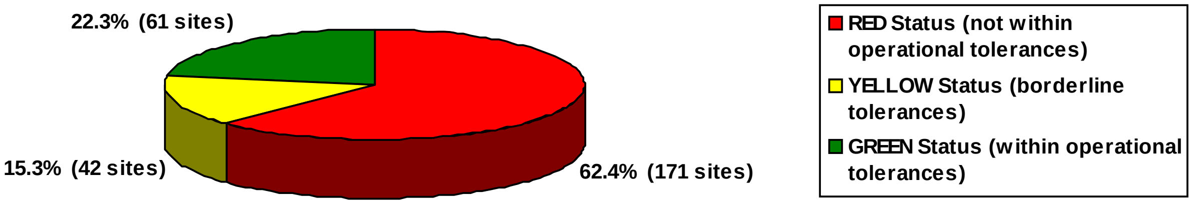
Patch Management Procedures

Over time, most software is discovered to have flaws that, if not fixed, can leave a computer open to disruption or attack. Patches are released to fix these flaws, and they are a vital part in any effective information systems security effort.

Six inspections revealed patch management procedures that do not comply with 5 FAM 866. Patch management objectives must include: applying patches in a timely manner; proper documentation of patch status; coordination among IT staff, management, and users; and notices sent to the Department indicating compliance with these objectives.

The Department is addressing patch management issues with mixed results. It has successfully deployed a tool that automates much of the patch application process. Posts, however, are not accessing the full potential of this tool. Some posts do not patch their systems regularly. Many posts still apply patches individually and do not know how to automate this process, even though the training is available online. Recent statistics from ENM's patch bulletin web site indicate a majority of posts are not installing patches, as shown in figure 1.

Figure 1: Patch Management at 274 Department Sites



Source: http://enm.irm.state.gov (as of December 17, 2004).

Some IT personnel abroad dispute these numbers and say that the reporting tool is flawed. Nevertheless, the numbers are consistent with OIG findings that patch management at posts needs marked improvement.

Many reasons are given as to why patch management is unsuccessful thus far. Many posts want the freedom to administer their systems as they see fit, rather than having them remotely administered from Washington. Other posts cite a shortage of staff, uninformed staff, and the continuous release of patches as contributing factors. Regardless of the reason, the patch management status quo is not tenable. A CIO initiative to enforce appropriate patch management procedures abroad would substantially lessen vulnerabilities to the Department's information systems.

Recommendation 3: The Chief Information Officer should establish written guidance and procedures on what actions will be taken if overseas posts do not install the patches the Department releases.

PLANNING DOCUMENTATION

Documenting procedures is a vital step in proper information systems management. Often, having a recovery plan in place can reduce downtime from days to hours or less in the event of a system failure. Documentation is also necessary for budgeting and staffing reasons. Often, specialists are rotated into areas needing immediate assistance, such as Embassy Baghdad and its supporting posts. They are typically the Department's most knowledgeable IT personnel, and their rotation places acute shortages at home posts. Having written documentation noticeably improves the learning curve for replacement specialists at post, saving valuable time and money and ultimately providing better service. Moreover, not having this basic paperwork shows that a post does not understand or is not following Department procedures.

During its inspections, OIG found many of the required post-specific documents either incomplete or nonexistent. Key documents include, but are not limited, to the following:

- Contingency Plans, which are designed to ensure continuity of operations under adverse conditions and should operate in conjunction with the Emergency Action Plan and with other posts, providing automated information systems backup processing capabilities. (13 inspections)
- Information Systems Security Plans provide an overview of automated information systems security and the means for improving the protection of IT resources. They also delineate the responsibilities and expected behaviors of all individuals accessing the systems. (11 inspections)

- IT Budget Plans must include the planned life cycle of all Information Program Center assets and current and future IT projects and services. They should look to future IT needs and plan accordingly. (4 inspections)
- Other such documents as topology maps, wiring diagrams, and patch management procedures must be current and tested frequently. (multiple inspections)

Overall, nearly half of the inspections uncovered problems within documentation.

Recommendation 4: The Chief Information Officer should inform the posts and bureaus of the requirements for information systems documentation and develop and implement procedures for verifying and validating that all requirements are met.

Local Change Control Board

The local CCB provides a forum for IT staff and RSOs to discuss whether or not to allow new software or hardware onto the post's IT systems. Though most posts have a local CCB, OIG found many were not fully cognizant of their role. OIG reminds bureaus that:

1. posts are required to inform the Department regularly of their CCB decisions;

2. posts should inform users of CCB decisions, including any penalties for noncompliance; and

3. as stated in 12 FAM 425 (a), RSOs play an integral part in systems security and must regularly work with ISSOs to form a cohesive security team at post.

An additional concern is the growing use of Universal Serial Bus (USB) drives, also known as "pen" or "thumb" drives. A single USB drive may have a gigabyte or more of storage space, which is ample room to store unapproved software, inappropriate material, classified material, or even an entire operating system undetectable by IT personnel. The Department currently defers to posts the choice to approve or disapprove the use of USB drives. This leads to different, even contradictory, policies at posts or even no policy at all.

The Department should determine the appropriate use of USB drives, and OIG advises the development of a Department-wide policy regarding their use.

Recommendation 5: The Chief Information Officer should develop policy and implementing guidance on the use of Universal Serial Bus storage drives on all Department systems.

In the interim, OIG urges local CCBs that currently use USB drives to establish and enforce a USB drive policy, with input from the RSO.

REGIONAL BUREAU-SPECIFIC OBSERVATIONS

This section highlights areas of concern within the bureaus OIG inspected during FY 2004. Although each bureau had its own specific issues, such as power outages, lack of training, unapproved Internet connections, and missing documentation, OIG found that issues such as the deficiencies in the ISSO program as well as shortages in personnel span across several bureaus.

Bureau of African Affairs

Posts in Africa operate with a high number of first-tour officers and specialists, including IMOs. Most posts are understaffed and lack sufficient IT training, funding, and infrastructure. Positions are frequently difficult to fill and often staffed, if at all, by inexperienced managers and specialists. For example, the IMO position was vacant for nearly a year in Embassy Addis Ababa, and Embassy Lesotho had no IMO. Temporary duty employees were often used to fill management positions, but churning through managers often has negative results. Embassy Asmara had six management officers in eight months, and Embassy Djibouti had seven in three years. OIG addressed these concerns in May 2004.[3]

Power outages are a regular event in Africa and have caused significant damage to IT equipment at Embassies Addis Ababa and Mbabane. Although outages are to be expected in underdeveloped areas, the Department should encourage all posts in Africa to test and reevaluate the adequacy of uninterruptible power supplies, surge suppression devices, and generators to avoid further damage to equipment. More regional support would help. Additionally, replacement parts and technicians should be available to repair dilapidated equipment in a timely manner.

[3] See *Strengthening Leadership and Staffing at African Hardship Posts* (ISP-I-04-54).

BUREAU OF EUROPEAN AND EURASIAN AFFAIRS

European posts are among the best funded and well equipped in the Department. Despite this, many are not meeting their IT security and systems management responsibilities. Half of the European inspections in 2004 revealed notable deficiencies in their ISSO programs. A basic ISSO duty is to check and document the search for unapproved or inappropriate material. Embassies Athens, The Hague, Prague, Ankara, and Consulate General Istanbul did not perform this basic task. Management control of the ISSO program and site security needs improvement to ensure the proper oversight of IT practices.

Department policy requires separation of duties in information systems management. European posts, though largely cognizant of their ISSO duties, often claim that they are short-handed and cannot properly staff IT and ISSO positions. Thus, IT specialists perform both system management and systems security duties. This arrangement, though tolerable in small posts with a limited user base, is not acceptable in large posts critical to U.S.-European relations. Separating management and security provides vital checks and balances.

As mentioned previously, posts must apply the Department's approved patch across all Department software. (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) .

BUREAU OF NEAR EASTERN AFFAIRS

The Bureau of Near Eastern Affairs (NEA) is struggling to realize the full potential of the ISSO program. The bureau's ISSO, for example, claimed to work on ISSO-related duties for only 15 minutes a day. As a result, the inspection team found many problems with basic systems security, including:

- users not given the required security briefing before account access, nor a yearly security refresher;
- external Internet connections that were unapproved;
- an acute lack of documentation of all kinds;
- and configuration settings that differ from Department standards.

IT personnel in NEA thought that they were in general compliance with Department security guidelines. This indicates a lack of training for IT and other NEA staff. NEA told OIG that it is addressing the issues that OIG's inspections found.

NEA posts abroad have many of the same problems facing the Department as a whole. Posts are hampered by personnel shortages as staff are rotated to support Embassy Baghdad. Four of the five inspections of NEA posts contain classified IT findings. For more information, see the classified security reports for Embassies Abu Dhabi, Doha, Kuwait, and Muscat.

Bureau of East Asian and Pacific Affairs

The Bureau of East Asian and Pacific Affairs (EAP) is, like NEA, struggling to meet the requirements of the ISSO program. EAP had two IT specialist vacancies during the inspections, a common explanation for gaps in information systems security. Essential planning and emergency recovery documentation was also missing, as was the assignment of a qualified alternate ISSO. Patch management procedures were also inadequate. Additional staffing and increased awareness of the Department's requirements should help alleviate these problems.

EAP posts abroad experienced the same problems found throughout the Department, including notable deficiencies in ISSO programs. One inspection revealed a consulate general with no ISSO program, and another so weak that it was de facto nonexistent.

Many posts in this region are similar to those in Africa, where OIG said that increased regional support could offset a lack of permanent IT specialists. This is especially true in China.

For more information systems security issues at EAP posts, please see the classified security reports for RIMC Bangkok and Embassies Bangkok, Beijing, Seoul, and Ulaanbataar.

CONCLUSION

The continuing effort to modernize the Department's information systems is proving successful. An equal challenge, however, continues to be the proper management and security of these advanced systems. OIG recognizes this challenge and commends the Department's efforts thus far. Improvements in the ISSO program, patch management and emergency documentation, local CCB operations, and management and oversight of these areas will help provide the Department with the means necessary to meet its information systems security challenges.

RECOMMENDATIONS

Recommendation 1: The Chief Information Officer must ensure that the information systems security officer's duties and responsibilities are prioritized such that not fulfilling them translates into unacceptable performance for the information management officer and the information systems security officer.

Recommendation 2: The Chief Information Officer should coordinate with the Director General to ensure that position descriptions for the information management officers include specific details regarding required information technology security responsibilities.

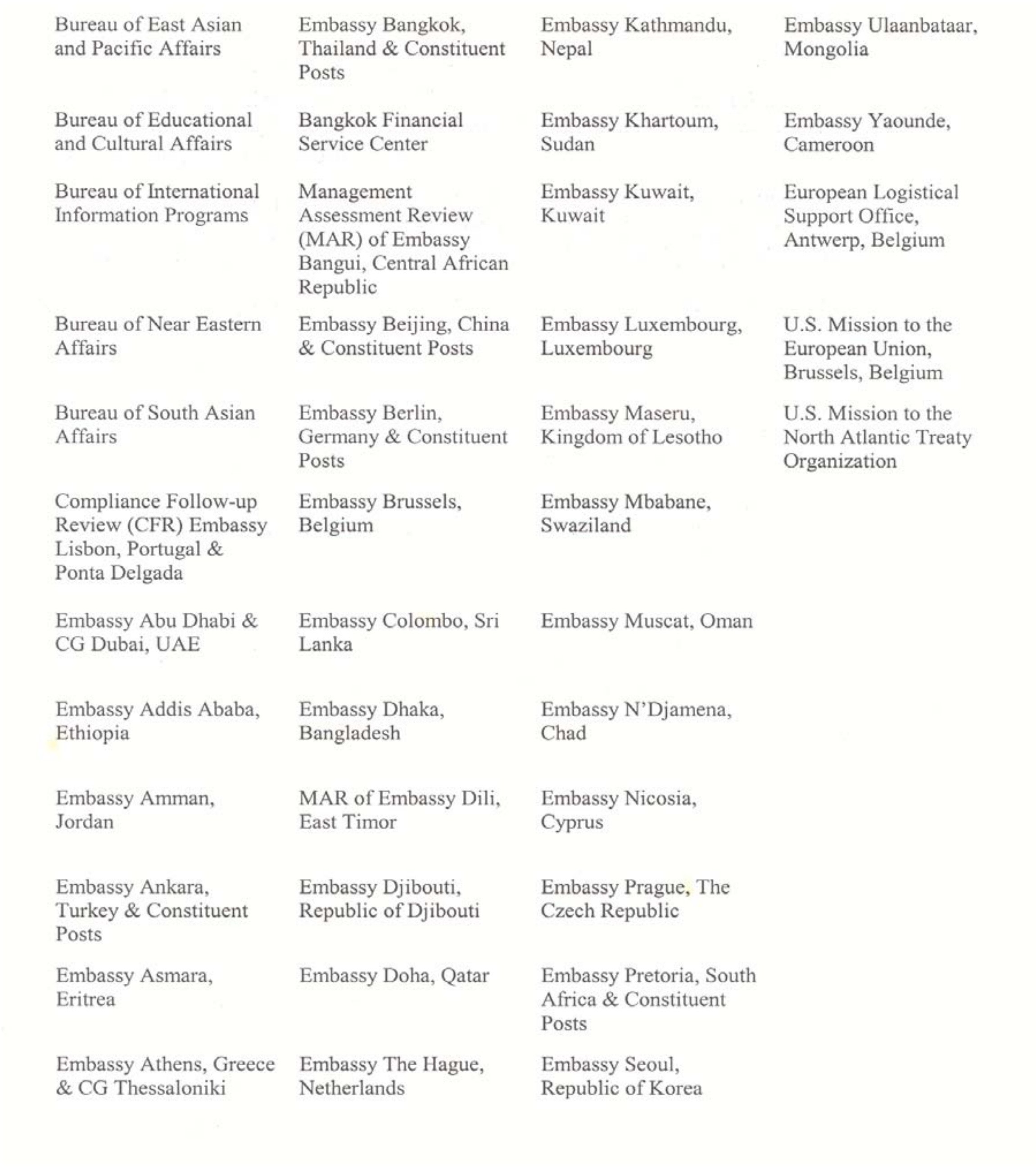
Recommendation 3: The Chief Information Officer should establish written guidance and procedures on what actions will be taken if overseas posts do not install the patches the Department releases.

Recommendation 4: The Chief Information Officer should inform the posts and bureaus of the requirements for information systems documentation and develop and implement procedures for verifying and validating that all requirements are met.

Recommendation 5: The Chief Information Officer should develop policy and implementing guidance on the use of Universal Serial Bus storage drives on all Department systems.

APPENDIX A

2004 IT Security Inspections



Bureau of East Asian and Pacific Affairs

Bureau of Educational and Cultural Affairs

Bureau of International Information Programs

Bureau of Near Eastern Affairs

Bureau of South Asian Affairs

Compliance Follow-up Review (CFR) Embassy Lisbon, Portugal & Ponta Delgada

Embassy Abu Dhabi & CG Dubai, UAE

Embassy Addis Ababa, Ethiopia

Embassy Amman, Jordan

Embassy Ankara, Turkey & Constituent Posts

Embassy Asmara, Eritrea

Embassy Athens, Greece & CG Thessaloniki

Embassy Bangkok, Thailand & Constituent Posts

Bangkok Financial Service Center

Management Assessment Review (MAR) of Embassy Bangui, Central African Republic

Embassy Beijing, China & Constituent Posts

Embassy Berlin, Germany & Constituent Posts

Embassy Brussels, Belgium

Embassy Colombo, Sri Lanka

Embassy Dhaka, Bangladesh

MAR of Embassy Dili, East Timor

Embassy Djibouti, Republic of Djibouti

Embassy Doha, Qatar

Embassy The Hague, Netherlands

Embassy Kathmandu, Nepal

Embassy Khartoum, Sudan

Embassy Kuwait, Kuwait

Embassy Luxembourg, Luxembourg

Embassy Maseru, Kingdom of Lesotho

Embassy Mbabane, Swaziland

Embassy Muscat, Oman

Embassy N'Djamena, Chad

Embassy Nicosia, Cyprus

Embassy Prague, The Czech Republic

Embassy Pretoria, South Africa & Constituent Posts

Embassy Seoul, Republic of Korea

Embassy Ulaanbataar, Mongolia

Embassy Yaounde, Cameroon

European Logistical Support Office, Antwerp, Belgium

U.S. Mission to the European Union, Brussels, Belgium

U.S. Mission to the North Atlantic Treaty Organization