Office of Inspector General
United States Department of State

AUD-IT-19-36 Office of Audits July 2019

Audit of the Department of State's Local Configuration Control Boards

INFORMATION TECHNOLOGY DIVISION

HIGHLIGHTS
Office of Inspector General
United States Department of State

AUD-IT-19-36

July 2019
OFFICE OF AUDITS
INFORMATION TECHNOLOGY DIVISION

Audit of the Department of State's Local Configuration Control Boards

What OIG Audited

The Department of State (Department) uses a variety of IT systems to execute its global mission. Configuration change control is the process used to ensure that changes to an IT system are formally requested, evaluated, tested, and approved before they are implemented. Changes that affect only local networks can be approved by a post's Local Configuration Control Board (LCCB). Other changes are required to be reviewed and approved by the Department's enterprise-wide Information Technology Configuration Control Board (IT CCB).

OIG conducted this audit to determine whether LCCBs are controlling changes to the Department's IT systems in accordance with Federal requirements and Department policy. The scope of the audit included a review of 236 changes to IT systems approved by LCCBs and detailed testing of 83 changes made to IT systems at 4 posts: Embassy The Hague, The Netherlands; Embassy Branch Office Tel Aviv, Israel; Embassy Seoul, South Korea; and Embassy Dhaka, Bangladesh.

What OIG Recommends

OIG made six recommendations to the Bureau of Information Resource Management (IRM) to improve guidance and oversight of IT configuration change control affecting local networks. On the basis of IRM's response to a draft of this report, OIG considers all six recommendations resolved, pending further action. A synopsis of IRM's response to the recommendations offered and OIG's reply follow each recommendation in the Audit Results section of this report. IRM's response to a draft of this report is reprinted in Appendix B.

What OIG Found

OIG found that LCCBs at selected posts were complying with some but not all Federal requirements and Department policies governing IT configuration change control that affect local networks. Specifically, the change requests reviewed by OIG for this audit generally complied with requirements and policies for approving IT changes at the local level, and the LCCBs informed the IT CCB about changes when required. However, OIG found that the LCCBs did not perform testing or a security impact analysis for any of the 83 change requests selected by OIG for detailed testing. OIG also identified weaknesses in maintaining documentation and found irregularities in some of the change requests.

The weaknesses identified occurred, in part, because of inadequate guidance and oversight of LCCBs by IRM officials at headquarters. Specifically, current guidance to LCCBs does not provide details of what documentation should be maintained to support a change request. Furthermore, the guidance does not provide information on how to perform and document a security impact analysis or on how to establish the manner in which LCCBs should conduct configuration testing before introducing software or hardware to the production environment. OIG also found that the Department had not provided standardized tools that LCCBs could use to efficiently and consistently review and approve local network IT changes.

Addressing these weaknesses is important because, without effective configuration change controls, the risk increases that changes being introduced could compromise the security, efficiency, and effectiveness of a post's systems as well as the data that reside on them. Furthermore, the lack of uniformity and consistency with the current LCCB change request process leads to inefficiencies when LCCB members rotate to a new post assignment.

CONTENTS

OBJECTIVE

The Office of Inspector General (OIG) conducted this audit to determine whether Local Configuration Control Boards (LCCB) were controlling changes to the Department of State's (Department) IT systems in accordance with Federal requirements and Department policy.

BACKGROUND

The Department uses a variety of IT systems to execute its global mission. For example, the Bureau of Consular Affairs uses the Consular Consolidated Database to maintain data, including photographs, from millions of current and archived passport and visa applications. The combination of all the IT systems and the hardware and software that support the systems make up the Department's IT infrastructure. According to Federal Information Processing Standards,[1] information systems used by Federal agencies must meet minimum security requirements. Agencies should develop and implement controls to ensure that these security requirements are met. One requirement is configuration change control or change management.

According to the National Institute of Standards and Technology (NIST), "Configuration change control is the process for ensuring that configuration changes to an information system are formally requested, evaluated for their security impact, tested for effectiveness, and approved before they are implemented."[2] Configuration change control ensures that changes requested for IT systems retain controlled security configuration settings for IT products used in organizational information systems. That is, change control ensures that changes to the system do not introduce a security risk. Changes can be as minor as adding a new type of printer or as significant as deploying an entirely new application. Table 1 describes a standard configuration change control process.

Table 1: Standard Configuration Change Control Process

Configuration Change Step	Description
Request the change	A request for change may originate from any number of sources, including the end user, a help desk, management, vendor-supplied patches, application updates, security alerts, or system scans.
Record the request for the proposed change	A change request is formally entered into the configuration change control process when it is recorded in accordance with organizational procedures. Organizations may use paper-based requests, email, a help desk, or automated tools to track change requests, route them on the basis of workflow processes, and allow for electronic acknowledgements and approvals.

[1] NIST, Federal Information Processing Standards 200, "Minimum Security Requirements for Federal Information and Information Systems," Section 8, "Implementations," March 2006.

[2] NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," § 3.3.2, "Implement the Configuration Change Control Process," 37, August 2011.

Configuration Change Step	Description
Determine whether the proposed change requires configuration control	Some types of changes may be exempt from configuration change control or pre-approved, as defined in the security-focused configuration management* plan and procedures. If the change is exempt or pre-approved, it will be noted on the change request, which allows the change to be made without further analysis or approval; however, system documentation may still need to be updated.
Analyze the proposed change for the change's security impact on the information system	Failing to properly analyze a change for its security impact can undo this effort and expose the organization to attack. The security impact analysis provides the linkage between configuration change control and improved security.
Test the proposed change for security and functional impacts	Testing confirms the impacts identified during analysis and reveals additional impacts.
Approve the change	This step is usually performed by the Change Control Board, which may require the implementation of additional controls if the change is necessary for mission accomplishment but has a negative impact on the security of the system and organization.
Implement the approved change	Once approved, authorized staff members make the change. Depending on the scope of the change, it may be helpful to develop an implementation plan. Implementation includes making changes to configuration parameters as well as updating system documentation. Stakeholders are notified about the change, especially if the change implementation requires a service interruption or alters the functionality of the information system. User and help desk training may be required.
Verify that the change was implemented correctly	Confirm that the change was deployed without issues. Although the initial security impact analysis and testing may have found no impact from the change, an improperly implemented change can cause its own security issues.
Close out the change request	The change request is closed out in accordance with organizational procedures.

* Security-focused configuration management is the management and control of configurations for information systems to enable security and facilitate the management of information security risk.

Source: OIG prepared from information obtained from NIST 800-128, § 3.3.2, "Implement the Configuration Change Control Process," and § 3.3.3, "Conduct Security Impact Analysis," 37–39.

According to the Foreign Affairs Handbook (FAH),[3] the Enterprise Network Management Office, within the Bureau of Information Resource Management's (IRM) Office of Operations, is responsible for the configuration change control process for the Department. The Enterprise Network Management Office has grouped configuration changes into two types: those that affect only local networks and those that could affect the Department's overall IT

[3] 5 FAH-5 H-512, "The Information Technology Change Control Board (IT CCB)."

infrastructure. The changes that affect only local networks can be approved by a post's LCCB.[4] Other changes are required to be reviewed and approved by the Department's enterprise-wide Information Technology Configuration Control Board (IT CCB). This audit was limited to the LCCBs.[5]

According to the Foreign Affairs Manual (FAM),[6] the IT CCB must approve any network capacity changes, including changes to wireless equipment, hardware and software used on a classified system, networked copiers, multi-functional printers, and network scanners or digital scanners. Other changes—specifically locally approved software and hardware functions that are only inside a post's supporting Local Area Network or Virtual Local Area Network segments—can be approved by an LCCB.[7] Even though the LCCBs approve local changes, they are still required to inform IT CCB about the changes.[8] If an LCCB determines that an application would function outside the local network, then the LCCB is required to obtain IT CCB approval to use the application.[9]

AUDIT RESULTS

Finding A: Local Configuration Control Boards Were Complying With Some but Not All Requirements Governing IT Configuration Change Control

OIG found that LCCBs at selected posts were complying with some but not all Federal requirements and Department policies governing IT configuration change control that affect local networks. Specifically, OIG found that all 236 change requests for software and hardware reviewed for this audit functioned only within the local network and were therefore appropriate for approval by the LCCB. In addition, the LCCBs provided information to the IT CCB about each of the approved change requests, as required. However, OIG also found that the LCCBs did not perform testing or a security impact analysis for any of the 83 change requests selected by OIG for detailed testing. OIG likewise identified weaknesses in maintaining documentation and found irregularities in some of the change requests.

The weaknesses identified occurred, in part, because of inadequate guidance and oversight of LCCBs by IRM officials at headquarters. For example, one reason the LCCBs did not comply with all requirements governing IT configuration change control was because the Department had not established guidance to consistently control the LCCB change request process. Specifically, guidance provided to LCCBs at the time of this audit did not detail what documentation should

[4] The Department sometimes uses the name Local Change Control Board rather than Local Configuration Control Board.

[5] OIG issued a separate report on the IT CCB—*Audit of the Department of State's Information Technology Configuration Control Board* (AUD-IT-17-64, September 2017).

[6] 5 FAM 862.3, "Determining What Must Be Sent to the IT CCB."

[7] 5 FAM 862.1(b), "Local IT CCB Responsibilities."

[8] 5 FAM 862.3(k).

[9] 5 FAM 862.3(a).

be maintained to support a change request. Furthermore, the guidance did not provide information on how to perform and document a security impact analysis or establish how LCCBs should conduct configuration testing before introducing software or hardware to the production environment. OIG also found that the Department had not developed standardized tools that LCCBs could use to efficiently and consistently review and approve local network IT changes.

Addressing these weaknesses is important because, without effective configuration change controls, the risk increases that changes being introduced could compromise the security, efficiency, and effectiveness of a post's systems and the data that reside on them. Furthermore, the lack of uniformity and consistency with the current LCCB change request process leads to inefficiencies when LCCB members rotate to a new post assignment.

Local LCCBs Approved and Reported Appropriate Types of Change Requests

According to the FAM, LCCBs may only approve IT change requests for software and hardware that do not function outside the local network.[10] The FAM also provides specific examples of what must be approved by the IT CCB, rather than the LCCBs, including the following:[11]

- All wireless equipment
- All hardware and software used on a classified system
- All networked copiers
- All multi-functional printers

OIG found that all 236 change requests for software and hardware reviewed for this audit function inside the local network and were therefore appropriate for approval by the LCCB. For example, OIG found the LCCBs approved change requests relating to software that enabled staff members to convert files to local language fonts and video editing software that functioned only on the local network. OIG also found the LCCBs approved change requests relating to hardware, such as printers and monitors, that did not include features that would have required IT CCB approval, such as wireless internet, Bluetooth connectivity, or multi-functional printers. OIG also learned through interviews that LCCB members are generally told and generally understand that, if an LCCB member is unsure if the LCCB is allowed to review and approve a request, the member should contact the IT CCB for clarification.

In addition, according to the FAM, "Local CCBs must report local/post activity and approval of IT items to their IT CCB voting representatives and the IT CCB change manager."[12] LCCBs are allowed to review and approve software and hardware changes within the scope of their authority and "all updates to the local IT CCB must be immediately communicated to the IT CCB voting representative."[13] For the 236 change requests that OIG reviewed, LCCBs provided

[10] 5 FAM 862.1(b).

[11] 5 FAM 862.3.

[12] 5 FAM 115.6-2(c), "Local Configuration Control Board (CCB)."

[13] 5 FAM 862.3(k).

information on the approved change requests to the IT CCB, as required. In addition, the LCCB attached copies of change request forms or provided a summary of processed change requests that typically included a unique identifier, a title or description of the change request, the date the request was made, and the LCCB's decision to approve or reject the change.

Testing Configurations and Security Impact Analyses Were Not Performed

NIST states that "organizations [should] fully test secure configurations prior to implementation in the production environment."[14] In addition, the FAM states that LCCBs are responsible for ensuring "that the hardware, software, or network components installed on a [local area network] do not adversely affect the existing local IT infrastructure."[15]

OIG found that the LCCBs did not perform testing on any of the 83 change requests selected by OIG for detailed review. Specifically, the LCCBs did not perform testing before adding software or hardware to the local networks. LCCB officials stated that testing was not done because the officials were not always capable of doing so. The officials stated that they did not necessarily have the expertise or tools to do the testing, so they relied on alternative procedures. For example, the LCCB officials explained that, in some instances, they selected software or hardware only from large, well-known vendors. Post officials said that they believed, under those circumstances, that vulnerabilities were more likely to be publicly known and reported. In other instances, LCCB officials spoke with Information System Security Officers at other posts to see if they were aware of deficiencies with software or hardware or had researched the product online to identify reported vulnerabilities before installing the software or hardware. This practice is inconsistent with both NIST and Department guidance, and the risk in implementing configurations without first testing the hardware, software, or network components installed on a local area network is inherent. In particular, assurance is limited that the newly added configurations will not adversely affect the existing local IT infrastructure and production environment.

In addition, as described previously, a security impact analysis is "conducted by an organizational official to determine the extent to which a change to the information system has or may have affected the security posture of the system."[16] The process for a security impact analysis consists of the following steps:

- Understanding the change
- Identifying vulnerabilities
- Assessing risk
- Assessing impact
- Planning safeguards and countermeasures[17]

[14] NIST 800-128, § 3.2.2, "Implement Secure Configurations," at 34.

[15] 5 FAM 862.1(b).

[16] NIST 800-128, Appendix B, "Glossary," at B-6.

[17] NIST 800-128, § 3.3.3, "Conduct Security Impact Analysis," at 39.

OIG found no evidence that a security impact analysis was conducted for any of the 83 change requests selected for detailed testing. In some instances, IT officials at posts were able to describe their thought process, which included consideration of potential security impacts, that led to the decision to approve a change request, but no documentation existed of any analyses, including potential vulnerabilities, risks, or impacts. Such documentation is necessary to inform designated LCCB members when they rotate to a new post. If change request documentation is not properly maintained, important information on configuration changes to the local network will not be available to new LCCB members when they arrive at post.

Weaknesses in Maintaining Documentation and Irregularities in Some Change Requests

IT system components (hardware, software, and network components) to be added to the local baseline under configuration control must first be processed and approved by the LCCB.[18] The Department provides only general guidance for the LCCB change request authorization process. The text of the guidance acknowledges that this is a "generic" process that "may" be adopted:

1. The originator creates a change request and submits it to the local configuration manager.
2. The local configuration manager assigns a change request number and decides if the change can be approved at the local level by the LCCB or must be sent to the IT CCB.
3. The local change manager creates a change request package for subject matter experts with whatever documents deemed necessary to make an informed decision.
4. Subject matter experts provide input.
5. The LCCB meets to review the IT change request and votes to approve or disapprove.[19]

OIG found that all 236 change control requests reviewed for this audit were processed in electronic or hard-copy format. OIG also noted that the four posts in which audit fieldwork was conducted had a process in place for approving change requests that generally incorporated the Department's guidance. However, OIG identified weaknesses in maintaining documentation and found irregularities in some of the change requests.

Insufficient Documentation To Retain Knowledge of Changes

According to NIST, "Providing an effective method to track changes to systems through configuration management procedures is necessary to achieve transparency and traceability in the security and privacy activities of the organization; to obtain individual accountability for any security or privacy actions; and to understand emerging trends in the security and privacy programs of the organization."[20] As stated by the Government Accountability Office, "Effective

[18] 5 FAM 862.1(b).

[19] Department, Generic Local/Post CCB Change Control Process, March 2003, 1–2.

[20] NIST 800-37, "Risk Management Framework for Information Systems and Organizations," rev. 2, 80 (December 2018).

documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a way to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel; it can also be a method of communicating that knowledge as needed to external parties, such as external auditors."[21]

The Department, however, did not have detailed guidance on what documentation was required to be maintained for each change request approved by an LCCB. The Department's guidance for LCCBs states only that the local change manager should create a change request package for subject matter experts that includes whatever documents the change control manager deems necessary to assist in making a decision.[22] Although NIST emphasizes the importance of documentation,[23] it also does not provide specific guidelines for the documentation that a change request package should include beyond stating that a security impact analysis and testing need to be complete. However, to transfer knowledge of the change request to new officials at the post, the documentation must be sufficient for that official to understand who made the change request, its purpose, when the decision was made, when the change was made, and why the LCCB made the decision to approve or disapprove the request. OIG found that the change request forms at the four posts audited included elements that, if completed, would document most of the information that would be needed (such as the name of the person completing the form, the type of change needed, and the date of the approval). However, OIG found that posts did not have sufficient documentation to explain why the LCCB made specific decisions related to each request. Without sufficient documentation that provides information about previous changes,[24] new IT staff will not have an understanding of what decisions were made and why.

Identified Irregularities in Approving Change Requests

OIG found that 146 of 236 (62 percent) change requests did not include the date the change request was approved. In addition, OIG found that 1 LCCB approved 33 change requests in a single day. Although batch processing of change requests can be done, these 33 change requests represented 77 percent of the post's approvals over a 6-year period. According to post officials, these change requests were formally approved in response to a review conducted by a Regional Cyber Security Officer from the Bureau of Diplomatic Security who identified IT changes at the posts that had not been formally approved by the LCCB. Although IT staff stated that these changes may have been informally approved at an earlier point, this approach was problematic because the LCCB process was not actually followed for those change requests and the changes were formally approved after they had already been made. In addition, OIG found two instances at the same post in which the post's Information Programs Officer, as a member of the LCCB, signed the change request, not only on the basis of his role but also on behalf of

[21] Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014), § 3.10, 29.

[22] Department, Generic Local/Post CCB Change Control Process, at 1.

[23] NIST 800-128, § 3.3.3, "Conduct Security Impact Analysis," at 39.

[24] Ibid.

the individual serving as both the Acting Information Management Officer and the Information Systems Security Officer. Although one other person also signed the change request, this LCCB's charter states that a quorum is required for a vote, and LCCB officials stated that the minimum number of required votes is three. Here, however, only two voters approved these change requests.

Inadequate Framework To Consistently Guide the Change Request Approval Process

The LCCBs did not comply with all requirements governing IT configuration change control in part because the Department had not established a process to consistently guide the change request process. "Having a clearly defined process or framework for the evaluation and approval of change requests, including predefined evaluation criteria, helps to ensure that each proposed and implemented change is evaluated in a consistent and repeatable manner balancing security, business, and technical viewpoints."[25] Although the Department has established standard operating procedures for managing change requests processed by the IT CCB,[26] guidance is limited for LCCBs in processing change requests at the local level. The primary guidance for LCCBs consists of a sample charter included on the IT CCB SharePoint site that states that LCCBs are "requested, but not required [to] include" the following items in change requests:

- Description or proposal of the change or addition
- Name of the network, the system, or both, to which the change relates
- Name of the software or hardware, or a description of the operational process
- Description of how the proposed implementation will address mission goals
- Scope of the change[27]

All the posts at which OIG conducted audit fieldwork used the sample charter as a template to develop their LCCB charter or included language from the sample charter in the LCCB's standard operating procedures. However, because the posts were not required to include all the elements, OIG identified inconsistencies in how posts reviewed and approved change requests. For example, two of the four posts had LCCB members meet to review and approve change requests as a group, although the other two posts forwarded change requests electronically to LCCB members and allowed them to complete their reviews and recommendations independently. In addition, current guidance for LCCBs does not provide details of what documentation should be maintained to support a change request. Furthermore, the guidance does not provide information on how to perform and document a security impact analysis or explain how to establish the manner in which LCCBs should conduct configuration testing before introducing software or hardware to the production environment. As noted previously, officials stated that their posts do not have the technical capability or expertise to perform testing. Some post officials also stated that posts do not have enough staff to perform

[25] NIST SP 800-128, § 3.1.2, "Planning at the System Level," at 30.

[26] In the September 2017 OIG report, *Audit of the Department of State's Information Technology Configuration Control Board* (AUD-IT-17-64), OIG reported deficiencies related to the Enterprise IT CCB processes.

[27] Department, Local Information Technology Change Control Board Charter, § 1.6, "Procedures," 4, 2012.

additional tasks. One post Information System Security Officer stated that if he asks IT CCB for assistance with testing, it may take 6 to 8 months, which is too long for the post's needs. An IRM IT CCB official stated that IRM recognizes that asking posts to perform testing is impractical. The IRM official further stated that IRM is working to develop a methodology to perform testing services for posts, thereby centralizing this activity or, at a minimum, to provide instructions on how to perform testing. Additional guidance providing clear standards and expectations would help alleviate posts' staffing concerns and lack of expertise.

In addition to the lack of standardized LCCB guidance, OIG also found that the Department had not developed and effectively distributed standardized tools that posts could use to efficiently implement the review and approval of IT changes. For example, even though IT CCB had a standardized, electronic change request form for the changes for which it was responsible, the Department had not provided this form to posts for use. As a result, each post had developed its own form.[28] Of the four posts where OIG conducted audit fieldwork, two had developed electronic forms[29] and two used hard-copy forms. An IT CCB official said the IT CCB plans to develop standard operating procedures for LCCBs.

Inadequate Oversight of LCCBs by Headquarters

IRM is responsible for the configuration change control process. According to the FAH,[30] the Enterprise Network Management Office (an IRM office that ultimately reports to the Chief Information Officer) is responsible for the configuration change control process for the Department. Furthermore, according to NIST, the Chief Information Officer is responsible for ensuring that "[a]n organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation."[31] In addition, NIST states that organizations are responsible for "[c]oordinat[ing] and provid[ing] oversight for configuration change control activities."[32] This is consistent with other guidance that explains, "The following attributes contribute to the design, implementation, and operating effectiveness of [oversight]:

- Oversight Structure
- Oversight for the Internal Control System
- Input for Remediation of Deficiencies"[33]

[28] According to NIST 800-128, Appendix E, "Sample Change Request," E-1, a change request form might include the date a request was prepared, who initiated the change request, justification, and urgency, among other information.

[29] Electronic forms are generally preferable to hard-copy forms. For example, electronic forms can contain features, such as automatic time stamps, automatic routing, and digital signatures, that provide better internal controls and data integrity. The electronic form can also require fields to be completed before the form can be submitted, and it can limit who can approve forms.

[30] 5 FAH-5 H-512.

[31] NIST 800-37, Appendix D, "Roles and Responsibilities," at 115–116.

[32] NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Agencies," § CM-3, "Configuration Change Control," F-66, April 2013.

[33] GAO-154-704G, § 2.01, at 24.

In short, to ensure that a program is running effectively, oversight is paramount. OIG determined, however, that the Department's LCCB change control process was not sufficiently designed because it did not include such an oversight function. For example, for the 236 change requests reviewed for this audit, OIG found that IRM did not routinely review change requests to determine whether they were authorized or what their impact could be. Furthermore, although LCCBs were required to submit their approved changes to the IT CCB, no requirement was in place for IRM or the IT CCB to review the configuration changes approved by the LCCBs, nor has IRM formally designated an individual or an office to oversee LCCB actions.

IT Systems Put at Risk and Inefficiencies Created

Without a well-designed and monitored change request process, the Department is at risk of introducing changes that may compromise the security, efficiency, and effectiveness of its systems and the data that reside on them. Because of the insufficient design of the LCCB structure, IRM cannot ensure that each LCCB is performing the process of evaluating changes and considering their risks and impacts to the network before approving the request. Furthermore, IRM cannot ensure that the Department's organization-wide security program is effectively implemented because it may not be aware of configuration changes that could result in security risks. In addition, conducting a security impact analysis "is one of the most critical steps in the configuration change control process with respect to [security-focused configuration management]. Organizations spend significant resources developing and maintaining the secure state of information systems; failing to properly analyze a change for its security impact can undo this effort and expose the organization to attack."[34]

If new software or hardware is added to the network and is not tested, it can cause vulnerabilities that can be exploited by a malicious actor. Implementing changes without sufficient testing could create exploitable vulnerabilities or could interact with other changes or the existing IT infrastructure in unforeseen ways. As a result, data may be lost or stolen, unintentionally or intentionally altered, or be unavailable to support the mission of the Department. In addition, if standard forms, as well as standard operating procedures and requirements, existed for the change request process, Foreign Service Officers moving from post to post would not be required to learn a new process at every post, making their transition more efficient.

> **Recommendation 1:** OIG recommends that the Bureau of Information Resource Management require that all IT configuration changes approved by the Local Configuration Control Boards at overseas posts be tested before implementation, in accordance with Federal requirements and Department of State policies.
>
> **IRM Response:** IRM concurred with the recommendation, stating that it will update the FAM and FAH to require "system owners to test all configuration changes before implementation to network."

[34] NIST 800-128, § 3.3.3, "Conduct Security Impact Analysis," at 39.

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM required that all IT configuration changes approved by the LCCBs at overseas posts be tested before implementation, in accordance with Federal requirements and Department policies.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management require Local Configuration Control Boards to perform and document security impact analyses on all configuration change requests before approval, in accordance with National Institute of Standards and Technology guidance.

IRM Response: IRM concurred with the recommendation, stating that it "will review current policies and FAM/FAH processes and determine if an update is required for [LCCBs] to perform and document security impact analyses on all configuration changes before approval."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM required LCCBs to perform and document security impact analyses on all configuration change requests before approval, in accordance with NIST guidance.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management provide guidance to Local Configuration Control Boards on the documentation regarding IT configuration change requests that must be retained at a post.

IRM Response: IRM concurred with the recommendation, stating that it will update the FAM and FAH to provide "guidance on documentation retention for all configuration changes."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM provided guidance to LCCBs on the documentation regarding IT configuration change requests that must be retained at a post.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and issue standard operating procedures for overseas posts' Local Configuration Control Boards to follow when reviewing, approving, and implementing IT configuration change requests. These standard operating procedures should establish and implement a process that provides for the evaluation, approval, and documentation of IT change requests in accordance with Department of State policies and National Institute of Standards and Technology requirements.

IRM Response: IRM concurred with the recommendation, stating that it "will update FAH policy to provide templates to domestic, post, and missions abroad in support of establishing standard operating procedures when reviewing, approving, and implementing IT configuration change requests."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has issued standard operating procedures for overseas posts' LCCBs to follow when reviewing, approving, and implementing IT configuration change requests.

Recommendation 5: OIG recommends that the Bureau of Information Resource Management develop and implement a methodology to oversee Local Configuration Control Board (LCCB) activities, including LCCB approval of IT configuration change requests at the local level. This methodology should include specific procedures for verification of the LCCB's testing of approved changes, security impact analyses, and retention of required documentation.

IRM Response: IRM concurred with the recommendation, stating that it "will update FAH policy to provide templates to domestic, post, and missions abroad in support of methodology to oversee [LCCB] activities, including LCCB approval of IT configuration change requests."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has implemented a methodology to oversee LCCB activities, including LCCB approval of IT configuration change requests at the local level.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management (IRM) formally designate oversight responsibility for Local Configuration Control Board activities to a specific position or office within IRM and establish a formal mechanism for communicating the oversight roles and responsibilities.

IRM Response: IRM concurred with the recommendation, stating that it "will review current positions within IRM and determine a designated position as the oversight responsibility for [LCCB] activities."

OIG Reply: On the basis of IRM's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has formally designated oversight responsibility for LCCB activities to a specific position or office within IRM and has established a formal mechanism for communicating the oversight roles and responsibilities.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Information Resource Management require that all IT configuration changes approved by the Local Configuration Control Boards at overseas posts be tested before implementation, in accordance with Federal requirements and Department of State policies.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management require Local Configuration Control Boards to perform and document security impact analyses on all configuration change requests before approval, in accordance with National Institute of Standards and Technology guidance.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management provide guidance to Local Configuration Control Boards on the documentation regarding IT configuration change requests that must be retained at a post.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and issue standard operating procedures for overseas posts' Local Configuration Control Boards to follow when reviewing, approving, and implementing IT configuration change requests. These standard operating procedures should establish and implement a process that provides for the evaluation, approval, and documentation of IT change requests in accordance with Department of State policies and National Institute of Standards and Technology requirements.

Recommendation 5: OIG recommends that the Bureau of Information Resource Management develop and implement a methodology to oversee Local Configuration Control Board (LCCB) activities, including LCCB approval of IT configuration change requests at the local level. This methodology should include specific procedures for verification of the LCCB's testing of approved changes, security impact analyses, and retention of required documentation.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management (IRM) formally designate oversight responsibility for Local Configuration Control Board activities to a specific position or office within IRM and establish a formal mechanism for communicating the oversight roles and responsibilities.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Office of Inspector General (OIG) conducted this audit to determine whether Local Configuration Control Boards (LCCB) were controlling changes to the Department of State's (Department) IT systems in accordance with Federal requirements and Department policy.

OIG conducted this audit from October 2018 to March 2019. Audit work was performed in the Washington, DC, metropolitan area; Embassy The Hague, The Netherlands; Embassy Branch Office Tel Aviv, Israel; Embassy Seoul, South Korea; and Embassy Dhaka, Bangladesh. OIG conducted this performance audit in accordance with generally accepted government auditing standards. These 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. Issuance of this report was delayed because of the lapse in OIG's appropriations that occurred from 11:59 p.m. December 21, 2018, through January 25, 2019.

To obtain background information for this audit, OIG researched and reviewed the Department's Foreign Affairs Manual and Foreign Affairs Handbook, National Institute of Standards and Technology requirements, and post policies related to the LCCB process. To better understand the change control process as implemented by posts, OIG performed audit work at four posts. The work consisted of gathering LCCB process documents, reviewing LCCB change requests, and interviewing LCCB board members. OIG also interviewed management of the Department's Information Technology Configuration Control Board (IT CCB) and other personnel from the Bureau of Information and Resource Management (IRM) to gain a better understanding of IRM's role in the LCCB process and in providing oversight of LCCBs.

To determine whether LCCBs have sufficient controls over changes to the Department's IT systems, OIG met with IT CCB management and LCCB board members at selected posts. In addition, OIG conducted walkthroughs at each site visited, assessed a sample of change requests processed at each post, and identified the processes used by each post to approve those change requests. Furthermore, OIG reviewed the documentation associated with each of the selected change requests.

Prior Reports

In September 2017, OIG reported[1] that IT CCB did not authorize or test change requests in compliance with Federal requirements and Department policy. Specifically, OIG found that change requests were not sufficiently authorized at every stage of the review process. This occurred because IRM had not implemented sufficient program management. Furthermore, the IT CCB process was not adequately designed, reviewers and voters were not appointed appropriately, and policies and procedures were inadequate. OIG also found that the

[1] OIG, *Audit of the Department of State's Information Technology Configuration Control Board* (AUD-IT-17-64, September 2017).

Department was unable to meet its internal deadlines for processing more than half the change requests tested. This occurred, in part, because IT CCB had not developed and implemented sufficient monitoring procedures. OIG made 17 recommendations to IRM to improve the Department's review process for change requests submitted to the IT CCB. As of April 2019, all 17 recommendations remained open and implementation was being tracked through the audit compliance process.

Work Related to Internal Controls

To gain an understanding of internal controls, OIG reviewed Department and Federal policies pertaining to configuration management. In addition, OIG interviewed IT CCB management and LCCB members, reviewed a sample of the change requests processed at each post included in the audit, and tested key configuration management controls. Weaknesses related to internal controls are detailed in the Audit Results section of the report.

Use of Computer-Processed Data

OIG used the LCCBs' database to develop a spreadsheet to select samples. This database was obtained from an IRM intranet website that allows LCCBs to upload and store documents such as copies of hard-copy change control requests, copies of handwritten notes, and spreadsheets. Since all change requests were not stored in a centralized location, OIG received change request information from 26 posts. From these 26 posts, 4 were selected for the basis of this audit. To verify the integrity of the data, OIG selected a sample of change requests at each audit site and reviewed the data included in the change requests. In addition, OIG observed the software or hardware that had been modified as a result of the change request to verify that it matched the change request information. Although OIG identified some deficiencies with the data, OIG concluded that the data were sufficient, appropriate, and of adequate quality to select a sample as evidence in support of the findings and conclusions in this report.

Detailed Sampling Methodology

The objective of the sampling process was to select a sample of overseas posts to review LCCB activities and determine whether LCCBs were controlling changes to Department IT systems in accordance with Federal requirements and Department policy.

OIG selected a target universe of four overseas posts as support for the audit objective after considering the resources available to perform the audit. OIG obtained from IRM a list of 251 overseas posts. The data provided by IRM included the number of information system users at each post. OIG selected the posts, using the following criteria:

- Posts that had not been visited as part of an OIG audit or inspection from 2014 through 2018.

- Posts with a higher than average number of system users.[2]
- Posts in different geographic bureaus.

As a result of implementing these criteria, OIG selected Embassy The Hague, Embassy Branch Office Tel Aviv, Embassy Seoul, and Embassy Dhaka for audit work.

OIG obtained a universe of 236 change requests from the selected overseas posts by submitting a data call to each post's Information Management Officer and Information Systems Center staff. OIG's data call was limited to change requests that had been processed at the local level from 2013 to 2018. OIG reviewed the 236 change request forms for certain attributes. Specifically, OIG determined whether the type of change was appropriate to be approved by a post and whether the change request forms included evidence of impact analyses and testing prior to change implementation.

OIG determined that performing detailed testing of 20 change requests for each post would be sufficient for the purposes of the audit. The 20 change requests were chosen using a risk-based selection and a nonstatistical random sampling design. The initial selection was based on the following risk-based factors:

- Missing or incomplete form fields.
- Change requests that indicated the change impacted multiple network types.
- Approved changes for hardware with potentially unauthorized capabilities, such as Wi-Fi connectivity.

After selecting the change requests on the basis of the risk-based factors, OIG then selected additional change requests, using a random number generator. Details of the sample selection at each post are included in Table A.1.

[2] OIG determined that the overseas posts had, on average, 284 IT system users. Therefore, OIG focused on posts that had more than 284 employees. This decision was based on the assumption that larger posts would have processed more change requests. After reviewing additional data, however, OIG determined that no clear correlation existed between the size of the post and the number of change requests. OIG nonetheless concluded that the posts selected using the original criteria were appropriately representative for the purposes of this audit.

Table A.1: Number of Change Requests Selected for Testing at Each Post

Post	Number of Change Requests Selected Using Risk-Based Factors	Number of Change Requests Selected Randomly	Total Number of Change Requests Selected
Embassy The Hague	3	17	20
Embassy Branch Office Tel Aviv	8	15	23*
Embassy Seoul	6	14	20
Embassy Dhaka	5	15	20

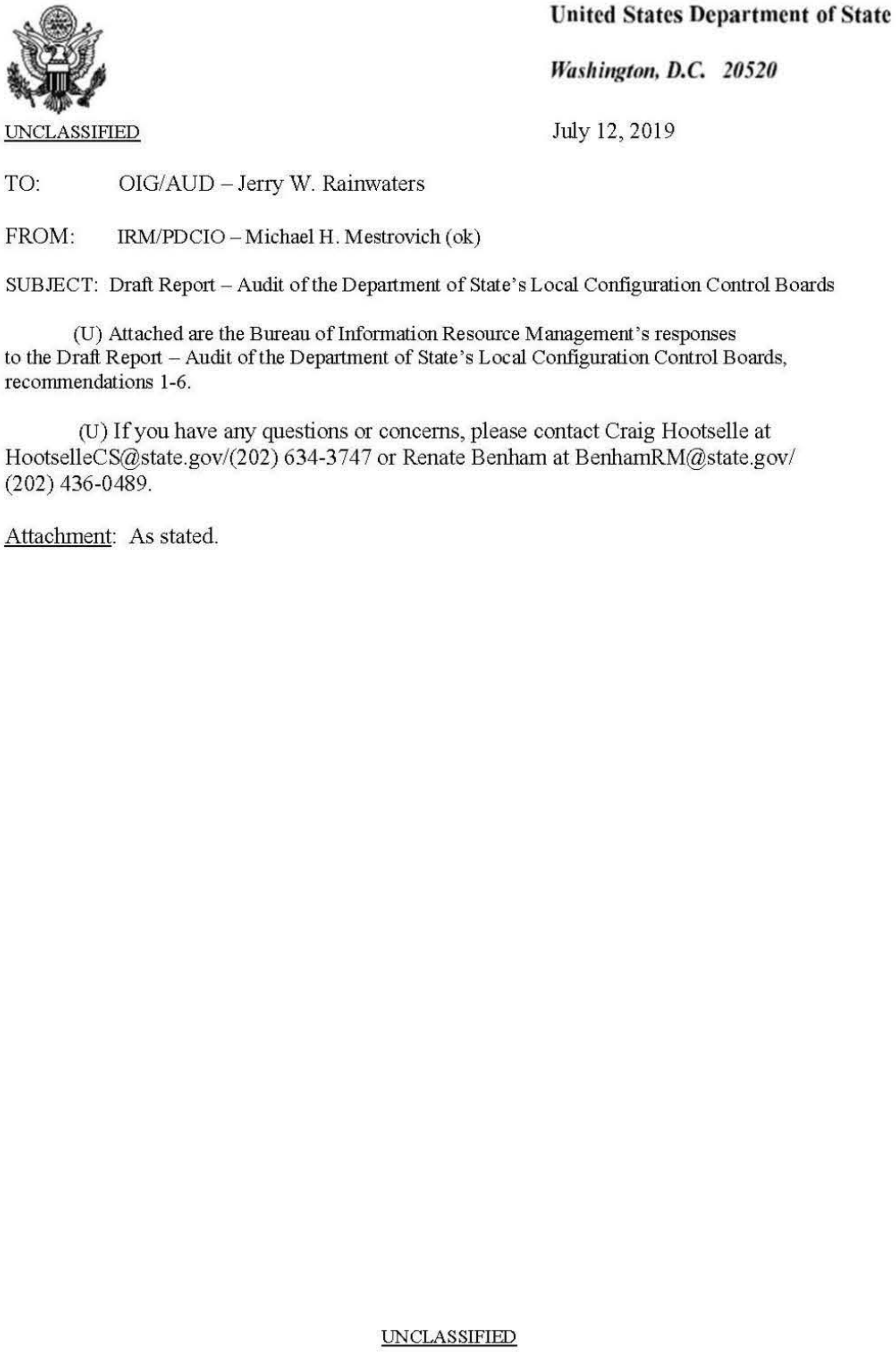
* OIG selected three additional change requests for review at Embassy Branch Office Tel Aviv because some of the change requests had the same unique identifier, despite being for different configuration items.

Source: OIG prepared from sampling plan.

OIG tested these change requests to determine whether:

- Changes were for unauthorized capabilities (for example, multifunction printers) or components (for example, Bluetooth connectivity).
- Changes had additional risks that would only be evident through physical observation.
- Post officials had a reasonable explanation for change request form errors, omissions, or irregularities or for missing data or documentation.

APPENDIX B: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

July 12, 2019

TO: OIG/AUD – Jerry W. Rainwaters

FROM: IRM/PDCIO – Michael H. Mestrovich (ok)

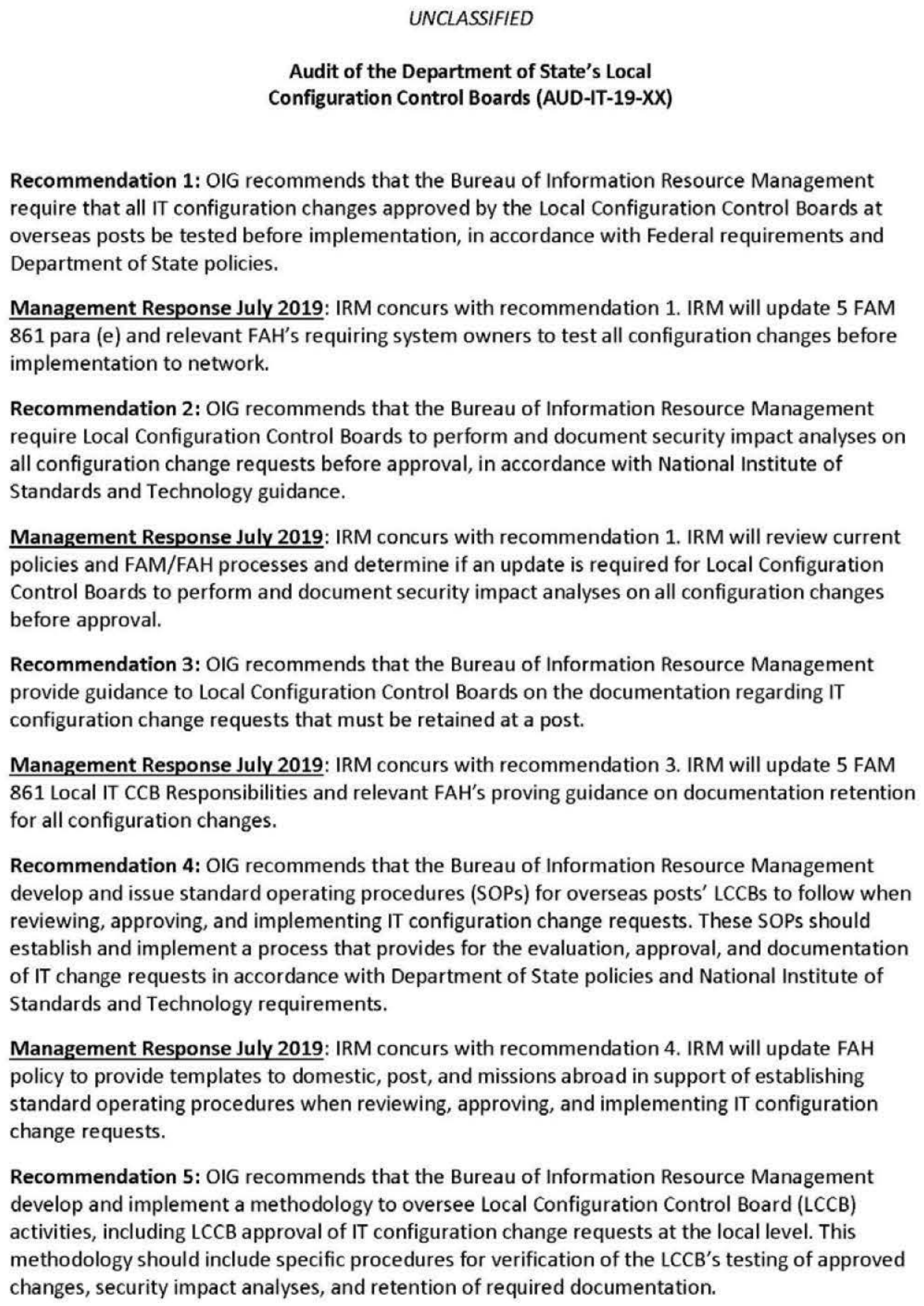
SUBJECT: Draft Report – Audit of the Department of State's Local Configuration Control Boards

(U) Attached are the Bureau of Information Resource Management's responses to the Draft Report – Audit of the Department of State's Local Configuration Control Boards, recommendations 1-6.

(U) If you have any questions or concerns, please contact Craig Hootselle at HootselleCS@state.gov/(202) 634-3747 or Renate Benham at BenhamRM@state.gov/ (202) 436-0489.

Attachment: As stated.

UNCLASSIFIED



UNCLASSIFIED

Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-XX)

Recommendation 1: OIG recommends that the Bureau of Information Resource Management require that all IT configuration changes approved by the Local Configuration Control Boards at overseas posts be tested before implementation, in accordance with Federal requirements and Department of State policies.

Management Response July 2019: IRM concurs with recommendation 1. IRM will update 5 FAM 861 para (e) and relevant FAH's requiring system owners to test all configuration changes before implementation to network.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management require Local Configuration Control Boards to perform and document security impact analyses on all configuration change requests before approval, in accordance with National Institute of Standards and Technology guidance.

Management Response July 2019: IRM concurs with recommendation 1. IRM will review current policies and FAM/FAH processes and determine if an update is required for Local Configuration Control Boards to perform and document security impact analyses on all configuration changes before approval.

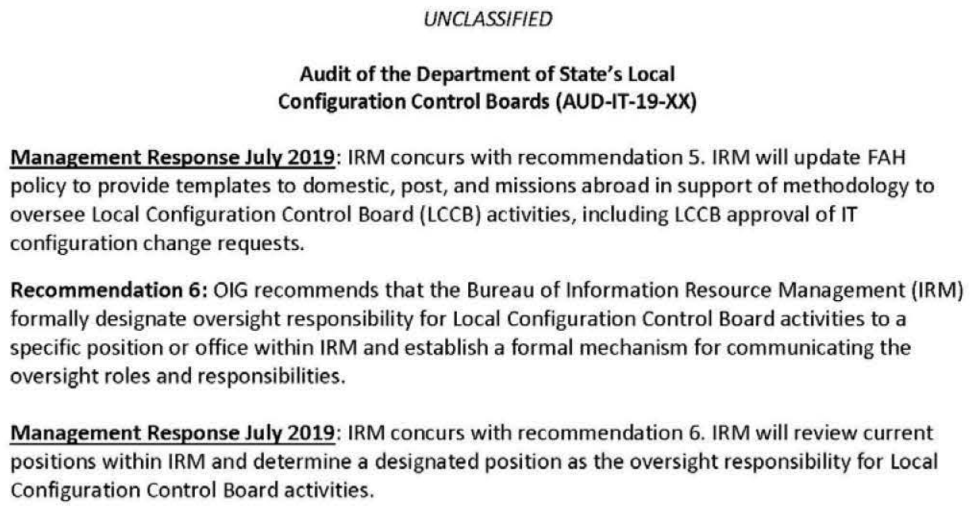
Recommendation 3: OIG recommends that the Bureau of Information Resource Management provide guidance to Local Configuration Control Boards on the documentation regarding IT configuration change requests that must be retained at a post.

Management Response July 2019: IRM concurs with recommendation 3. IRM will update 5 FAM 861 Local IT CCB Responsibilities and relevant FAH's proving guidance on documentation retention for all configuration changes.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and issue standard operating procedures (SOPs) for overseas posts' LCCBs to follow when reviewing, approving, and implementing IT configuration change requests. These SOPs should establish and implement a process that provides for the evaluation, approval, and documentation of IT change requests in accordance with Department of State policies and National Institute of Standards and Technology requirements.

Management Response July 2019: IRM concurs with recommendation 4. IRM will update FAH policy to provide templates to domestic, post, and missions abroad in support of establishing standard operating procedures when reviewing, approving, and implementing IT configuration change requests.

Recommendation 5: OIG recommends that the Bureau of Information Resource Management develop and implement a methodology to oversee Local Configuration Control Board (LCCB) activities, including LCCB approval of IT configuration change requests at the local level. This methodology should include specific procedures for verification of the LCCB's testing of approved changes, security impact analyses, and retention of required documentation.



UNCLASSIFIED

Audit of the Department of State's Local Configuration Control Boards (AUD-IT-19-XX)

Management Response July 2019: IRM concurs with recommendation 5. IRM will update FAH policy to provide templates to domestic, post, and missions abroad in support of methodology to oversee Local Configuration Control Board (LCCB) activities, including LCCB approval of IT configuration change requests.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management (IRM) formally designate oversight responsibility for Local Configuration Control Board activities to a specific position or office within IRM and establish a formal mechanism for communicating the oversight roles and responsibilities.

Management Response July 2019: IRM concurs with recommendation 6. IRM will review current positions within IRM and determine a designated position as the oversight responsibility for Local Configuration Control Board activities.

ABBREVIATIONS

FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
IRM	Bureau of Information Resource Management
IT CCB	Information Technology Configuration Control Board
LCCB	Local Configuration Control Board
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

OIG AUDIT TEAM MEMBERS

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Laura Noordhoek, Audit Manager
Information Technology Division
Office of Audits

Laura Dzuray, Auditor
Information Technology Division
Office of Audits

Reynaldo Gonzales, Auditor
Information Technology Division
Office of Audits

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926
Stateoig.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Coordinator to learn more about your rights.
WPEAOmbuds@stateoig.gov