



# HIGHLIGHTS

Office of Inspector General  
United States Department of State

AUD-IT-19-36

## 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.

July 2019

OFFICE OF AUDITS

INFORMATION TECHNOLOGY DIVISION

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

## 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.