



OIG HIGHLIGHTS

AUD-IT-17-64

UNCLASSIFIED

September 2017

OFFICE OF AUDITS

Information Technology Division

Audit of the Department of State's Information Technology Configuration Control Board

What Was Audited

The Department of State (Department) uses a variety of IT systems to execute its global mission. Configuration change control ensures that unnecessary changes to IT systems, or changes that could introduce security weaknesses, are prevented. A system change could be as minor as adding a new type of printer or as significant as deploying an entirely new application. Enterprise-wide change requests are required to go through a review process led by the Department's Information Technology Configuration Control Board (IT CCB).

Acting on behalf of the Office of Inspector General (OIG), Kearney & Company, P.C. (Kearney), an independent public accounting firm, conducted this audit to determine whether the Department's enterprise-wide IT CCB authorized and tested change requests for the Department's systems in accordance with Federal requirements and Department policies and met its internal deadlines for processing change requests.

What OIG Recommends

OIG made 17 recommendations to IRM to improve the Department's review process for change requests submitted to the IT CCB. On the basis of the Bureau of Information Resource Management's (IRM) response to a draft of this report, OIG considers 15 recommendations resolved, pending further action, and 2 recommendations unresolved. 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 its entirety in Appendix C.

What Was Found

Kearney found the Department's IT CCB did not authorize or test change requests in compliance with Federal requirements and Department policy. Specifically, Kearney found that change requests were not sufficiently authorized at every stage of the review process and change requests were not tested as required. For example, Kearney found that different categories of reviewing officials are not required to approve all change requests and do not always approve them before they move forward in the process. The IT CCB process is deficient in part because IRM has not implemented sufficient program management to execute the IT CCB process. In addition, the IT CCB process is not adequately designed to support the review of change requests. Furthermore, Kearney found deficiencies in the manner in which Technical Reviewers and Voters are appointed, as well as with IT CCB policies and procedures, the database used by the IT CCB to track change requests, and training. As a result of unauthorized and untested change requests, the Department's network, applications, and software are put at risk because of an inconsistently applied and controlled configuration control process.

Kearney found that the Department was unable to meet its internal deadlines for processing more than half the change requests tested that were submitted through the IT CCB process. Untimeliness occurred at every phase of the process. One reason that the IT CCB did not always meet its timeliness metrics was that it has not developed and implemented sufficient monitoring procedures. In addition, Kearney found that, although the IT CCB had established deadlines for the different stages of the change request review process, it did not have a method to track whether these metrics were accomplished. Kearney also found inaccurate data in the database used to track change requests, which makes monitoring more difficult. Also, the IT CCB did not have sufficient policies and procedures in place. As a result of untimely processing of change requests, the Department could be exposed to network vulnerabilities.

_____ Office of Inspector General _____
U.S. Department of State • Broadcasting Board of Governors

UNCLASSIFIED