



Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-17-64

Office of Audits

September 2017

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

INFORMATION TECHNOLOGY DIVISION



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



1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kenarneyco.com

Audit of the Information Technology Configuration Control Board

Office of Inspector General
U.S. Department of State
Washington, D.C.

Kearney & Company, P.C. (Kearney), has performed an audit of the Information Technology Configuration Control Board. This performance audit, performed under Contract No. SAQMMA14A0050, was designed to meet the objective identified in the report section titled "Objectives" and further defined in Appendix A, "Purpose, Scope and Methodology," of the report.

Kearney conducted this performance audit in accordance with *Government Auditing Standards*, 2011 Revision, issued by the Comptroller General of the United States. Those standards require that Kearney plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Kearney believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

Kearney appreciates the cooperation provided by personnel in Department of State offices during the audit.

A handwritten signature in blue ink that reads "Kearney & Company". The signature is stylized and cursive.

Kearney & Company, P.C.
Alexandria, Virginia
August 31st, 2017

CONTENTS

OBJECTIVE.....	1
BACKGROUND	1
AUDIT RESULTS.....	10
Finding A: The Department of State Did Not Authorize or Test Change Requests in Accordance With Federal Requirements and Department Policy.....	10
Finding B: The Information Technology Configuration Control Board Did Not Meet Internal Deadlines for Processing Change Requests.....	34
RECOMMENDATIONS.....	42
APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY	45
Work Related to Internal Controls	46
Use of Computer-Processed Data.....	46
Detailed Sampling Methodology	47
Detailed Survey Methodology.....	51
APPENDIX B: SUMMARY OF RESPONSES TO A CUSTOMER SURVEY.....	52
Survey Questions and Responses	52
APPENDIX C: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE.....	59
ABBREVIATIONS	64

OBJECTIVE

The overall objective of this audit was to determine whether the Department of State's (Department) enterprise-wide Information Technology Configuration Control Board (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.

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 photos, 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 the Federal Information Processing Standards,¹ information systems used by Federal agencies must meet minimum-security requirements. Agencies should develop and implement controls to ensure these security requirements are met. One requirement is configuration change control or change management,² which ensures that changes requested for IT systems retain controlled security configuration settings for IT products employed in organizational information systems. Changes can be as minor as adding a new type of printer or as significant as deploying an entirely new application. The Department has created a change control process to implement this control. Table 1 describes a standard configuration change process.

Table 1: Standard Configuration Change Process

Configuration Change Step	Detailed Description
Prioritize Configurations	In determining the priorities for implementing secure configurations in information systems or IT products, organizations consider system-level impact, risk assessments, vulnerability scanning, and the degree of penetration to the network.
Test Configurations	Organizations fully test secure configurations prior to implementation in the production environment. A number of issues, including software compatibility and hardware device driver issues, may be encountered when implementing configurations.

¹ National Institute of Standards and Technology, Federal Information Processing Standards 200, "Minimum Security Requirements for Federal Information and Information Systems," Section 8, "Implementations," March 2006.

² Federal Information Processing Standards 200 states that this control is required for IT systems that are moderate and high-risk to the enterprise network and infrastructure; however, this control is considered a best practice and is recommended for all systems.

Configuration Change Step	Detailed Description
Resolve Issues and Document Deviations	Testing implementations of secure configurations may introduce functional problems within the system or applications. For example, the new secure configuration may close a port or stop a service that is needed for an operating system or application function. These problems are examined individually and either resolved or documented as a deviation from, or an exception to, the established common secure configuration. When conflicts between applications and secure configurations cannot be resolved, deviations are documented and approved through the configuration change control process, as appropriate.
Record and Approve the Baseline Configuration	The established and tested secure configuration, including any necessary deviations, represents the preliminary baseline configuration and is recorded to support configuration change control/security impact analysis, incident resolution, problem solving, and monitoring activities. Once recorded, the preliminary baseline configuration is approved in accordance with an organization's defined policy. Once approved, the preliminary baseline configuration becomes the initial baseline configuration for the information system and its constituents.
Deploy the Baseline Configuration	Organizations are encouraged to implement baseline configurations in a centralized and automated manner using automated configuration management tools, automated scripts, and vendor-provided mechanisms.

Source: Prepared by Kearney & Company, P.C., from information obtained from the National Institute of Standards and Technology, Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," Section 3.2.2, "Implement Secure Configurations," August 2011.

According to the Foreign Affairs Handbook (FAH),³ the Enterprise Network Management Office (ENM) within the Bureau of Information Resource Management's (IRM) Office of Operations is responsible for the configuration change control process for the Department. ENM has grouped configuration changes into two types: those that only affect local networks and those that could affect the Department's overall IT infrastructure. The changes that only affect local networks can be approved by a post's Local Configuration Control Board.⁴ Other changes are required to be reviewed and approved by the Department's enterprise-wide IT CCB.⁵ This audit was limited to the enterprise-wide Configuration Control Board.

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

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

⁵ In its policies and on its website, the Department defines the IT CCB as both the Information Technology Configuration Control Board and the Information Technology Change Control Board. Although the names appear to be treated interchangeably, this report uses the name included on the IT CCB website (that is, Configuration Control Board).

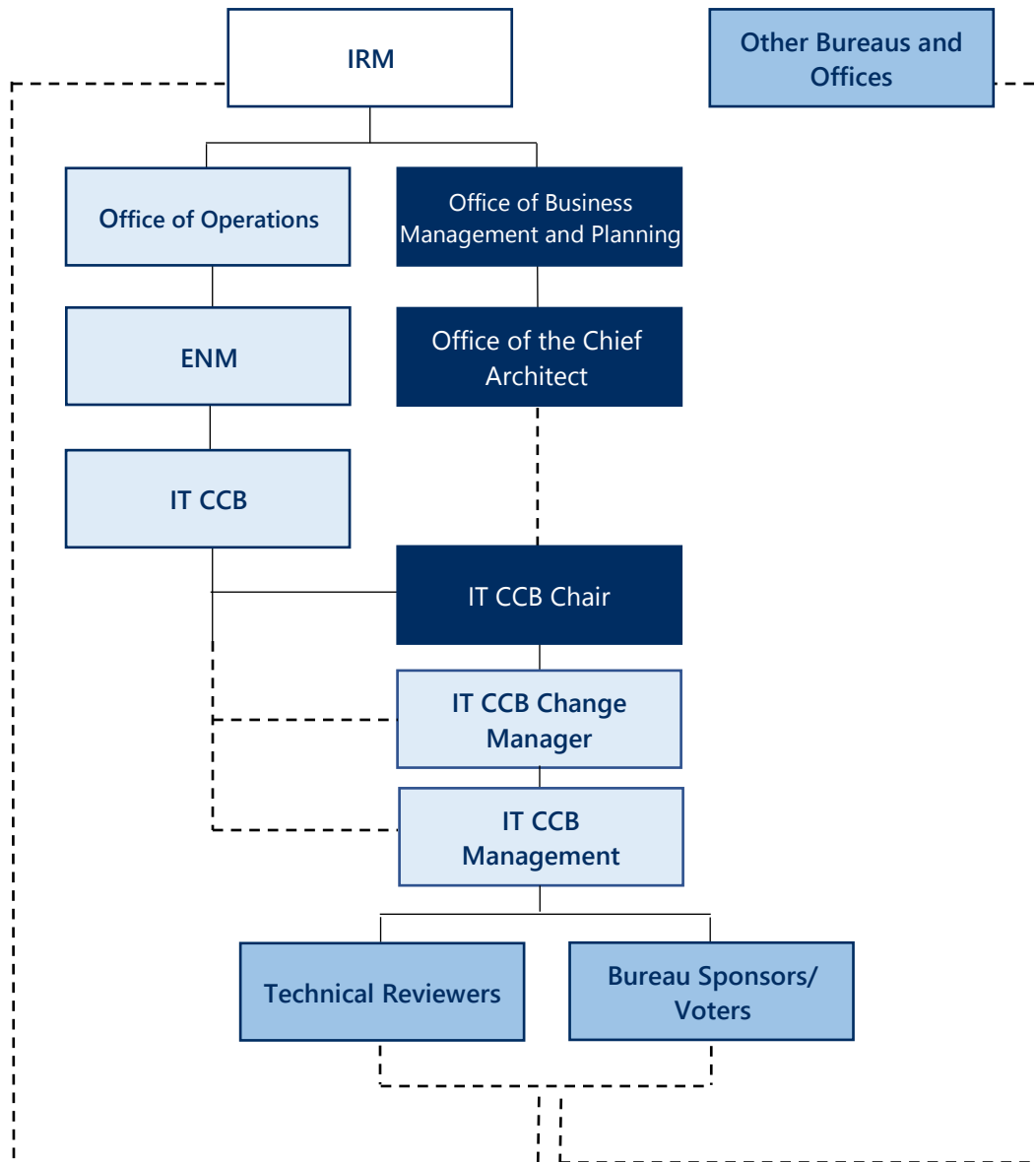
The enterprise-wide IT CCB charter requires the IT CCB to ensure the availability, reliability, integrity, security, interoperability, and performance of the enterprise infrastructure, as well as ensuring that changes do not degrade any infrastructure performance. Further, the IT CCB is required to approve changes to both classified and unclassified networks. According to the Foreign Affairs Manual (FAM), the enterprise-wide IT CCB must approve any network capacity changes, including changes to all wireless equipment, hardware and software used on a classified system, networked copiers, multi-functional printers, and network scanners or digital scanners.⁶ In addition, the IT CCB must ensure that all changes are seamless and do not cause unplanned disruptions to the services provided by the Department's IT networks and systems. Because IT devices and services interact in complex and sometimes unforeseeable ways, the IT CCB must consider the impact of a change on all Department stakeholders, rather than solely on the individual making the request.

IT CCB Organization

Although the responsibility for the IT CCB resides within ENM, as shown in Exhibit 1, officials from many bureaus and offices participate in the IT CCB process.

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

Exhibit 1: IT CCB Organization*



* Solid lines depict organizational placement. Dashed lines depict the bureaus or offices in which the employees that fill those roles work.

Source: Prepared by Kearney & Company, P.C., from information obtained on the IRM website.

IRM ensures the secure flow of vital knowledge and communication throughout the Department.⁷ The Office of Operations provides day-to-day operations for the Department's enterprise networks,⁸ including managing networks, developing applications, integrating software, and safeguarding the Department's IT systems. ENM is responsible for modernizing

⁷ IRM Homepage, <https://www.state.gov/m/irm/>, accessed in May 2017.

⁸ 1 FAM 275, "Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS)."

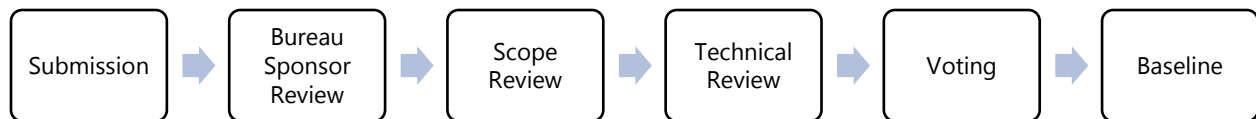
and managing the Department's network infrastructure, which includes leading the Department's IT CCB.⁹ According to IRM officials, ENM provides to the IT CCB process a Change Manager who is charged with leading the day-to-day operations of the IT CCB. For example, the Change Manager leads IT CCB management and personnel to facilitate the IT CCB process by overseeing the appointment of various reviewing officials and by approving the priority status of non-routine change requests. IT CCB management and personnel are members of the ENM office who report directly to the IT CCB Change Manager.

According to IRM officials, the IT CCB Chair works for IRM's Office of the Chief Architect within the Office of Business Management and Planning. The Chair provides high-level oversight of the IT CCB and the Change Manager. Additional IT CCB key stakeholders include Bureau Sponsors¹⁰/Voters¹¹ and Technical Reviewers¹² who work in many different bureaus and offices, including IRM.

IT CCB Configuration Change Control Process

As shown in Exhibit 2, each change request made by a bureau or post that is processed by the enterprise-wide IT CCB goes through six steps before it is approved to be implemented.

Exhibit 2: Enterprise-Wide IT CCB Configuration Change Control Process



Source: Prepared by Kearney and Company, P.C., from information obtained in meetings with IT CCB officials.

Submission

Any Department employee can submit an IT change request. All changes inherently start at the local level, within a bureau or post. Specifically, when the need for a change is identified, a system, product, or software owner will typically document the desired change in a formal document called a change request and submit the change request to the local Configuration Control Board for consideration. The local Configuration Control Board will determine if it can approve the change or if the change requires approval from the enterprise-wide IT CCB.

⁹ 1 FAM 276.1, "Enterprise Network Management Office (IRM/OPS/ENM)."

¹⁰ In general, Bureau Sponsors perform the initial review of the change request to ensure it is complete and accurate. Additional details are provided later in the Background section of this report.

¹¹ In general, Voters are responsible for considering the impact of a change request on the enterprise as a whole. Additional details are provided later in the Background section of this report.

¹² In general, Technical Reviewers perform an in-depth review of the requested change. Additional details are provided later in the Background section of this report.

If the change request is required to go through IT CCB, the employee submitting the request first contacts the Bureau Sponsor and then submits the change request using IT CCB's system for controlling change requests, the Virtual Information Technology Configuration Control Board Application (VITCCB).¹³ To submit a request in VITCCB, the employee must complete a Reviewer's Questionnaire, which includes information on the change being requested, such as licensing requirements and specifications. This information is needed to ensure that reviewers have enough data to assess the change request. The IT CCB website states that the Voluntary Product Accessibility Template (VPAT)/Section 508 Compliance documentation¹⁴ is recommended. However, in practice, IT CCB management requires change requesters to submit the VPAT/Section 508 documentation before moving a request forward in the IT CCB process.

VITCCB also includes a section for the requester to upload and retain additional supporting documentation. As shown in Table 2, the enterprise-wide IT CCB has recommended guidelines for submitting supporting documentation; however, only the Reviewer's Questionnaire and the VPAT/Section 508 documentation are required, in practice.

Table 2: IT CCB Change Request Documentation

Documentation	Description
Business Impact Analysis Documents	Documentation that predicts the consequences of a disruption of a business function and process and gathers information needed to develop recovery strategies.
Cost Information	Documentation explaining the cost information for a specific product.
Concept of Operations Documents	Document describing the characteristics of the proposed system. It communicates the quantitative and qualitative system characteristics.
Configuration Standards or Guidelines	Procedures for the product to operate effectively.
Security Plan and Network Diagrams	A proposed plan to protect and control an information system and a graphical chart of a network.
Classified Information Spillage Cleanup Procedures	Procedures that implement the security control requirements needed to respond to electronic spillage of classified national security information onto unclassified information systems or devices.
VPAT/Section 508 Compliance	An amendment to the U.S. Workforce Rehabilitation Act of 1973, a Federal mandate that all electronic and IT developed, procured, maintained, or used by the Federal Government be accessible to people with disabilities.
Additional Market Research Evidence	Research into the change's characteristics, spending needs, location, and other requirements to determine the feasibility of the change before committing substantial resources to a system.
Vendor Documentation	Documentation comparing vendor options for a product.

¹³ VITCCB allows for all individuals involved in the IT CCB process to simultaneously review supporting documentation, provide recommendations, and vote on multiple change requests at one time. It also provides a tool for documentation retention and IT CCB management oversight.

¹⁴ Section 508 requires Federal agencies to make their electronic records and IT accessible to people with disabilities. This law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

Documentation	Description
Technical Specification Documents	Document that defines a set of requirements that a product, software, or system must meet or exceed.
Administration and User Manuals	A technical communication document intended to give assistance to users of a particular system.
Evaluation Reports	Documentation determining the relevance and fulfilment of objectives, efficiency, effectiveness, impact, and sustainability of a product.
Bandwidth Impact/Requirements Statement	The difference between the upper and lower frequencies of a band of electromagnetic radiation that is passed along a communication channel in a given period of time.

Source: Prepared by Kearney & Company, P.C., from the list of recommended documentation outlined on the IT CCB website.

Once the submission is complete, VITCCB automatically assigns a Configuration Management number and generates an email to the Bureau Sponsor, initiating the start of the Bureau Sponsor review phase.

Bureau Sponsor Review

Each bureau within the Department has a sponsor assigned to it. Large bureaus, such as IRM, may have multiple IRM employees assigned as sponsors who represent IRM's interests. Smaller bureaus, such as the Bureau of the Comptroller and Global Financial Services, may have an employee from another bureau assigned as their sponsor. The Bureau Sponsor vets change requests proposed by members of its assigned bureaus or offices to ensure changes are in the best interest of the bureau and approved by management, if necessary.

The Bureau Sponsor performs an initial review of the change request to ensure the submission is complete and accurate and the business requirement aligns with organization policies and objectives, as well as Federal laws and policies. Specifically, the Bureau Sponsor should ensure the Reviewer's Questionnaire in VITCCB is complete and a VPAT/Section 508 Compliance form is included. Once the Bureau Sponsor review is complete, the Bureau Sponsor submits the change request to IT CCB management, using VITCCB.

Scope Review

The scope review is performed by a member of IT CCB management and should include a review to verify that the submission is within the scope of the IT CCB and is ready for technical review. Specifically, IT CCB management is responsible for performing a secondary check to ensure that the Reviewer's Questionnaire and the VPAT/Section 508 Compliance form has been included in VITCCB. In addition, IT CCB management should confirm the requested product has not already gone through the IT CCB process. Once the scope review is complete, IT CCB management sends the submission for technical review, using VITCCB.

Technical Review

The technical review phase involves an in-depth review of the requested product. Twenty¹⁵ Technical Reviewers representing multiple bureaus or offices throughout the Department are involved in the process. Each Technical Reviewer is responsible for a different area of focus on the basis of individual expertise. For example, a Technical Reviewer from the Bureau of Diplomatic Security is responsible for reviewing the IT security aspects of a change request and a Technical Reviewer from IRM is responsible for ensuring that the change request does not violate the Department's IT policies and procedures. Each Technical Reviewer is only responsible for reviewing issues related to a designated area and is not required to review other areas of the submission.

Technical Reviewers can provide feedback to the submitter and request additional information or documentation as needed. A Technical Reviewer who requires additional information or documentation places a "stop" on the change request, which prevents the request from proceeding to the next phase. All stops must be lifted before the change request can proceed through the process. Technical Reviewers should document a reason for a stop to allow submitters to address the concerns. In the event the change request submitter cannot satisfy the Technical Reviewer's additional request or the change request cannot be implemented, the change request submitter can withdraw the change request from the process, using VITCCB, effectively canceling the change request. If satisfied, the Technical Reviewer issues a recommendation for the submission to proceed to voting.

Voting

Once the Technical Reviewers have approved a change, VITCCB will automatically notify all IT CCB Voters¹⁶ that a change request is ready for review. Because IT change requests may interact in complex and sometimes unforeseeable ways with the Department's existing IT infrastructure, According to IT CCB management, Voters should consider the effect of a change on all Department bureaus and the enterprise as a whole, rather than only considering how a change may impact the bureau making the request. Only 12 of the total 23 Voters are required to approve a change. If the Voters cannot reach a simple majority, the IT CCB will not approve the change. Voters are not required to perform any particular level of review before casting their votes.

¹⁵ Twenty bureaus or offices, each with an appointed primary reviewer, perform technical reviews. Seventy-six individuals have the capability to perform technical reviews because many bureaus or offices have Alternate Technical Reviewers and Office Directors who could perform this function.

¹⁶ IT CCB Voters are the same people as the Bureau Sponsors.

Baseline

When approved by the Voters, IT CCB guidance states that the change should be updated in the Department's baseline.¹⁷ The baseline is a cumulative list of all changes approved for implementation and, when considered in the aggregate, should represent the current state of an organization's IT infrastructure. An accurate baseline provides the basis for introducing safely and efficiently new changes to an environment; conversely, an inaccurate or incomplete baseline can pose significant risk to an entity. Without a complete understanding of the specific hardware and software used by the organization, the entity will not be able to accurately test and control how changes may affect its existing IT infrastructure or how changes may interact with other changes.

Types of Change Requests

Change requests were once categorized as change requests, amendments, or system authorization requests.¹⁸ The most common category was change requests, a designation that is still used today. IT CCB management discontinued the amendment process during FY 2017 but stated that it plans to use the process again in the future. Therefore, this report addresses issues identified with amendments.

A change request is a formal request for a change to be performed on a component of the IT infrastructure. This includes changes to hardware, software, the network, wireless connections, and settings. A change refers to an addition, change, deletion, or termination of infrastructure components, applications, or systems that could affect the performance, security, integrity, reliability, availability, or interoperability of the infrastructure or its existing applications.

An amendment was used to classify minor revisions to a change request that had already been made. For example, an amendment would have been used to modify a version, model, configuration setting, or instructions. The amendment process was separate from the change request process. Specifically, the review process was performed manually, outside VITCCB, and did not include a review by Voters. IT CCB management retained responsibility for ensuring the change was, in fact, minor and, therefore, appropriate to be treated as an amendment. IT CCB management ensured the change was minor by sending an email with the amendment description to all IT CCB Technical Reviewers for confirmation. In the event that Technical Reviewers did not consider the change minor, the amendment was rejected and the requestor was required to submit a change request.

¹⁷ According to the IT CCB website, as of April 11, 2017, the IT CCB determines a change request to be baselined when it is added to the list of approved hardware and software. From that point, any bureau or office can reference the list of approved changes and use items included in the baseline as it sees fit, assuming an identical iteration of the hardware or software. The baseline is available on the IT CCB website.

¹⁸ According to 5 FAM 841, "System Authorization Process," the Department is required to make a security determination, called authorization, before an IT system can become operational. The IT CCB discontinued processing system authorization requests in FY 2016. Therefore, this report does not address the causes for any issues noted with this type of change request.

Priority Levels of Change Requests

When a person submits a change request, the submitter assigns a priority level for the request—routine, expedited, or emergency. Most change requests are routine. A change request is considered expedited if it is so urgent that the routine IT CCB processing time is not fast enough. A change request is considered an emergency if it involves unforeseen events that affect availability, integrity, or confidentiality of Department IT systems or networks. The IT CCB Change Manager approves the priority status of all expedited or emergency requests prior to processing. Expedited and emergency change requests are processed manually because of their status. Not all areas of focus in the technical review phase need to be reviewed for expedited and emergency change requests.

AUDIT RESULTS

Finding A: The Department of State Did Not Authorize or Test Change Requests in Accordance With Federal Requirements and Department Policy

Kearney & Company, P.C. (Kearney), found that 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. The IT CCB process is deficient in part because IRM has not implemented sufficient program management to execute the IT CCB process in accordance with Department and Federal policies. 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 VITCCB database, and training. As a result of unauthorized and untested change requests, the Department's networks, applications, and software are put at risk because of an inconsistently applied and controlled configuration control process.

Change Requests Were Not Always Authorized as Required

Kearney found instances in which change requests were not sufficiently authorized at every stage of the review process. For example, Kearney found that IT CCB management did not always maintain documentation about Bureau Sponsor reviews of change requests. In addition, Kearney found that the majority of the change requests that did not have evidence of review by Bureau Sponsors were moved on to the next phase of the process even though the requests were missing required documentation. The IT CCB management and personnel that perform the required scope reviews stated that they do not perform all the required steps to confirm that a change request needs an IT CCB review or whether the Local Configuration Control Board should instead perform the review. Furthermore, Kearney identified instances in which at least one of two items that IT CCB management said that it checks during the scope reviews was incomplete. Kearney also noted that Scope Reviewers did not always approve the priority levels of change requests as required.

Kearney also found a variety of concerns associated with Technical Reviewers and Voters. First, Kearney found that Technical Reviewers are not required to approve all change requests and do not in fact always approve them before they move forward. Instead, the process and VITCCB is designed to issue a "default proceed" on behalf of a Technical Reviewer for a change request if a Technical Reviewer does not respond within allotted timeframes. Routine requests could, in theory, be moved forward through the technical review phase even if no Technical Reviewers completed a review. Moreover, although a need for more time is not one of the reasons Technical Reviewers are allowed to "stop" the change request process, Kearney, found that some Technical Reviewers put "stops" on change requests to give themselves more time to review the request, rather than for a valid reason. In addition, Kearney found that amendments that went through a manual review process could be implemented in the Department's baseline even if no Technical Reviewers responded to a request for approval. Kearney also found that when Voters vote on change requests, they might not be approving requests on the basis of a thorough review of the request. In fact, according to IT CCB officials, Voters have never denied a change request.

Bureau Sponsor Review

According to guidance included on the IT CCB website, Bureau Sponsors should perform an initial review of a request made by someone in their assigned bureaus to ensure that the submission is complete and accurate and that the business requirements align with the organization's policies and objectives, as well as Federal laws and regulations. Specifically, Bureau Sponsors should ensure that the required Reviewer's Questionnaire and VPAT/Section 508 Compliance form are complete and included in the VITCCB.

Kearney found that IT CCB management did not always maintain documentation of Bureau Sponsor reviews of change requests. Specifically, of 78 change requests reviewed, Kearney did not find evidence that Bureau Sponsors had performed reviews for 14 (18 percent). Of the 14 change requests that did not have evidence of a Bureau Sponsor review, 12 (86 percent) advanced to the next phase of the process without evidence of a VPAT/Section 508 Compliance form and 13 (93 percent) advanced to the next phase of the process without evidence of a completed Reviewer's Questionnaire. In fact, of the 14 change requests that did not have evidence of a Bureau Sponsor review, 6 (43 percent) made it through the entire IT CCB process and were moved to the baseline even though at least 1 of 2 required pieces of documentation was missing or incomplete.

Scope Review

According to guidance included on the IT CCB website, a scope review, which is performed by IT CCB management, has two objectives. First, it is to confirm that a change request requires approval by the enterprise-wide IT CCB and cannot be processed by a Local Configuration Control Board. The second objective is to confirm that the request is not redundant with another request or with hardware or software that is already approved by the IT CCB. In addition, during a scope review, IT CCB management should confirm that the request is ready to move forward in

the process. Although the scope review should address a number of issues, according to IT CCB officials, during the scope review, the Scope Reviewer only ensures that two required documents are provided with the change request, the same two that the Bureau Sponsors should check (Reviewer's Questionnaire and VPAT/Section 508 Compliance form). IT CCB officials responsible for performing scope reviews stated that they did not always assess whether a change request required enterprise-wide IT CCB approval or whether the review should be performed by the Local Configuration Control Board. In addition, IT CCB officials responsible for the scope reviews stated that they did not always determine whether the change request was appropriate and not redundant. Further, Kearney found instances in which requests approved by the scope review to move forward in the process were missing at least one of two required items that IT CCB management said were assessed during the scope review. Specifically, of 78 change requests reviewed, 14 (18 percent) did not have either a complete Reviewer's Questionnaire or a complete VPAT/Section 508 form, as required.

In addition to assessing whether all change requests are ready to move forward in the process, during the scope review phase, IT CCB officials should¹⁹ ensure that the priority status selected by the submitter (routine, expedited, or emergency) is appropriate for the request. Of a sample of 78 change requests tested during the audit, 2 were identified as either expedited or emergency. Of these two priority change requests, one (50 percent) lacked the proper change manager approval of the status, which should have occurred during the scope review phase.

Technical Review

The technical review phase involves an in-depth review of a change request by reviewers that have expertise in key areas. For example, a Technical Reviewer from the Bureau of Diplomatic Security reviews the IT security aspect of change requests, and a Technical Reviewer from IRM ensures that change requests do not violate the Department's IT policies and procedures. According to guidance included on the IT CCB website, Technical Reviewers "perform impact analyses within their scope of authority." This policy is consistent with National Institute of Standards and Technology (NIST) guidance, which requires the evaluation of change requests prior to implementation.²⁰

Although the technical review is a vital component of the process that ensures that changes requests comply with security and IT requirements, IT CCB management stated that the technical review phase does not require Technical Reviewers affirmatively to approve all change requests before they can move forward. Instead, the process and VITCCB is designed to issue a "default proceed" on the behalf of a Technical Reviewer for a change request if a Technical

¹⁹ 5 FAH-5 H-513 (d) "IT CCB Assessment Request (AR) and Approval."

²⁰ According to NIST, Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," Section 2.3.3, "the group, which represents various perspectives from within the organization, is chosen to evaluate and approve changes to the information system. The CCB is a check and balance on configuration change activity, assuring that changes are held to organizationally defined criteria (e.g., scope, cost, impact on security) before being implemented."

Reviewer does not respond within allotted timeframes. In fact, routine requests could, in theory, be moved forward through the technical review phase even if no Technical Reviewers completed a review.²¹ In response to a customer survey,²² one change request submitter noted, “some reviewers seem to...submit proceed with no apparent review.” Of 54 change requests tested during the audit that completed the technical review phase,²³ Kearney found that 42 (78 percent) included 1 or more default proceeds. As shown in Table 3, for the 54 change requests reviewed, Kearney identified 16 Technical Reviewers with 1 or more defaults on the 54 change requests.

Table 3: Number of Default Proceeds by Technical Reviewer

Technical Review Area and Purpose	Total Default Proceeds
Privacy – To ensure personally identifiable information is appropriately protected.	0
Network Capacity – To ensure the network has the ability to handle the upgrade to or implementation of the software/application.	0
Architecture and Strategic Plan – To ensure the change request is consistent with the Department’s plan and fits in to the Department’s current architecture.	0
Application and Desktop – To ensure the change request does not harm the application or desktop.	0
Enterprise Software Licensing – To ensure the change request is appropriately licensed prior to approval.	1
Communication (Audio, Telephone) – To determine whether the change request impacts communication.	1
IT Security – To ensure the change request does not harm the Department’s network or create a higher risk environment.	1
Section 508 Compliance – To ensure the change request meets Federal requirements for technology to be accessible to disabled users.	1
IT Policies and Procedures – To ensure the change request is compliant with the Department’s IT policies and procedures	1
Helpdesk and Desktop Support Services – To identify the need for Helpdesk and Support Services upon change request implementation.	2
Messaging and Email – To determine the impact of the change request on email and messaging communication.	3
Infrastructure Development, Wireless Telephony – To determine the implications of the change request on the wireless infrastructure development.	4
Capital Planning and Financial Impact – To determine the financial impact and how the change request is reviewed for capital planning.	11

²¹ Expedited and emergency requests require that seven Technical Reviewers complete their review before the request moves forward in the process. Specifically, the seven required areas of technical review for expedited and emergency changes include privacy, technical countermeasures, IT security, Section 508 compliance, network capacity, messaging and email, and accreditation and contingency planning.

²² Appendix B provides the survey questions and results.

²³ Kearney selected a sample of 78 change requests for review. However, only 54 of those change requests completed the technical review phase. Others were suspended or removed from the process for various reasons and were not included in the count of 54.

Technical Review Area and Purpose	Total Default Proceeds
Foreign Operations/Innovation – To ensure the change request does not harm foreign operation and innovation.	12
Corporate Messaging, Collaboration and Archiving Processes, and Systems – To ensure the change request does not harm the processes established for corporate communication.	11
Accreditation and Contingency Planning – To assess the change request’s status and need for inclusion in the accreditation and authorization process, as well as its need for a contingency plan.	13
Education and Training – To identify the change request’s need for education and training prior to full implementation.	14
Advocacy for Functional Bureaus – To determine the change request’s impact and advantages for functional bureaus.	15
Global IT Modernization – To determine how the change request aligns to the Department’s effort to modernize.	36
Advocacy for Regional Posts and Foreign Missions – To determine how the change request can be used for regional posts and foreign missions.	39

Source: Prepared by Kearney from documentation obtained from IT CCB.

One Technical Reviewer who frequently “defaulted” was the Technical Reviewer for Global IT Modernization. According to the Department’s Information Technology Strategic Plan,²⁴ “the Department must adapt the network architecture to counteract increasingly sophisticated threats.” The Strategic Plan also states that the Department is “developing a modernized and secure IT infrastructure that harnesses new information delivery models [that] will enhance the Department’s voice, network, data, radio, and video capabilities, providing secure platforms for Department communications and emergency life-safety and command and control situations.” The development of a modernized and secure IT infrastructure could be put at risk if the Technical Reviewer for Global IT Modernization does not participate in the change request process.

Another Technical Reviewer who often “defaulted” was the Technical Reviewer for Capital Planning and Financial Impact, which is conducted by IRM’s Strategic Planning Office. The Strategic Planning Office is responsible for ensuring a coordinated capital planning effort across the Department. Since change requests can require significant resources, capital planning and preparation for the systems used across the Department are essential. It is accordingly important for the Strategic Planning Office to participate in the IT CCB process.

Kearney assessed some of the change requests included in its sample that had multiple default proceeds and found that some of them were high-risk change requests. For example, one change request was for a product designed to ensure that data were authenticated and remained behind the firewall on the Department’s classified system through a secure, encrypted channel. This change request received six default proceeds from Technical Reviewers, including

²⁴ Department of State, “2017-2019 Department of State IT Strategic Plan.”

the reviewers responsible for Global IT Modernization and Contingency Planning. Another change request for a software update of the secure module of the Department's inventory tracking application, housed on the Department's classified network, received five default proceeds from Technical Reviewers, including the reviewers responsible for Capital Planning and Financial Impact, Helpdesk and Desktop Services Support, and Global IT Modernization. Kearney also found widely disseminated change requests that had a significant number of default proceeds. For example, the change request that resulted in the Department-wide implementation of the Apple operating system, version 9.0, received nine default proceeds, including a default proceed from the Technical Reviewer responsible for Section 508 compliance. It is important for any change request, but especially one that is implemented agency-wide, to be reviewed to ensure that disabled employees would be able to use the product.

IT CCB management stated that default proceeds should not be considered to be an indication that the Technical Reviewer did not review a change request but instead an indication that a Technical Reviewer used the maximum allotted time and found no reason to stop the submission and had no additional input for the Voters to review. Information obtained in this audit does not support this claim. Specifically, during the audit, Kearney spoke to multiple Technical Reviewers who stated that no review was performed when a default proceed occurred. More generally, without affirmative concurrence from Technical Reviewers, it is impossible to know whether a change request was reviewed.

In addition to issues related to default proceeds, another issue identified by Kearney related to the technical review phase was that Technical Reviewers can "stop" any change request during the process. If a Technical Reviewer places a "stop" on a change request, the request will not continue in the process until the Technical Reviewer clears the "stop" in the VITCCB. Kearney found that some Technical Reviewers placed "stops" on all change requests to allow themselves more time for review. One Technical Reviewer stated that he immediately "stopped" every request that he received. Technical Reviewers have the ability to request further time for technical reviews from IT CCB management if the allotted time is not sufficient; however, Kearney found none of the 54 change requests that completed the technical review phase of the process contained a request for an extension. Although "stops" are appropriate if issues arise during the technical review phase, "stops" create inappropriate delays if they are not done for a valid reason.

In response to a customer satisfaction survey conducted by Kearney,²⁵ 22 of 38 (58 percent) respondents stated that they had at least 1 change request that had been "stopped" during the Technical Review phase. Nine of the 22 (41 percent) respondents stated that they had submitted more than 4 change requests that had been "stopped." One change request submitter commented, "Technical Reviewers need to be more specific when initiating stops. They should also initiate stops for their area of responsibility." Furthermore, one change request submitter commented, "some of the reviewers seem determined to put 'stops' on anything submitted,

²⁵ Appendix B provides the survey questions and results.

causing more delay and effort. At times, it seems that the whole process is an exercise in trying to keep customers from ever submitting anything to the IT CCB.”

Technical Reviews of Amendments

The technical review of amendments also raises concerns. An amendment was used by the IT CCB to classify minor changes to a change request that had already been made. Although IT CCB did not use this designation during FY 2017, when the audit was performed, IT CCB management stated that IT CCB plans to use this designation again in the future, and Kearney is accordingly reporting issues identified regarding approval of such amendments. According to IT CCB’s standard operating procedures, amendments were processed outside VITCCB using a manual process. IT CCB procedures stated that amendments did not include a traditional scope review.²⁶ Technical Reviewers were given the opportunity to review the amendment prior to implementation. However, rather than being notified by VITCCB, IT CCB officials would email information, including supporting documentation, to the Technical Reviewers. Technical Reviewers were asked if they had any objections to the amendment, but they were requested to respond in a shorter timeframe than the normal change request process provided. The amendment could be approved and added to the baseline even if no Technical Reviewer approved the amendment. One Technical Reviewer stated that he did not have enough time to review amendments, so he simply did not respond to any that he received.

Voting

According to guidance on the IT CCB website, Voters²⁷ provide the final approval of a change request based on recommendations from the Technical Reviewers. Voters should ensure that a change would not adversely affect the operations of applications in their bureau or affect the overall security risk of the Department’s systems or networks. Voters serve as a final quality control check on the process. Further, it is important for Voters to be aware of enterprise-wide IT changes to ensure that bureaus can take advantage of changes being made to the IT system. However, according to IT CCB officials and several Voters, Voters do not necessarily review supporting documentation or assess the Technical Reviewers’ recommendations before approving a change request. In addition, only half the Voters (12 of 23) need to approve a change, meaning that Voters can choose not to vote on a change request.

Kearney noted which bureaus participated in the voting process for 35²⁸ change requests tested. As shown in Table 4, Kearney found that 7 of 23 (30 percent) Voters voted on fewer than half the 35 change requests tested.

²⁶ IT CCB management was only required to review the amendment to ensure it was a minor change and not a major upgrade or the acquisition of new hardware or software.

²⁷ The Department’s IT CCB process includes 23 Voters.

²⁸ Of 78 change requests tested by Kearney, 54 cleared the technical review phase. Of the 54 change requests that cleared the technical review phase, 8 were not required to go through the voting stage according to IT CCB guidance. Of the 46 change requests that went to Voters, 11 did not complete the voting process at the time of audit testing.

Table 4: Number of Votes by Voter for 35 Sampled Change Requests

Bureau or Office	Number of Requests Voted On	Percentage of Change Requests Voted On
Administration	15	43
African Affairs	16	46
Consular Affairs	28	80
Diplomatic Security	34	97
East Asian and Pacific Affairs	33	94
Economic and Business Affairs	32	91
European and Eurasian Affairs/International Organizational Affairs	26	74
Foreign Service Institute	32	91
Human Resources	28	80
International Information Program/Educational and Cultural Affairs	24	69
International Narcotics and Law Enforcement Affairs	34	97
Intelligence and Research	17	49
Information Resource Management	33	94
Legal Adviser	21	60
Medical Services	32	91
Near Eastern Affairs	4	11
Office of Inspector General*	0	0
Public Affairs	23	66
Comptroller and Global Financial Services	3	3
Chief of Protocol	5	5
Executive Secretariat	26	74
International Security and Nonproliferation	19	54
Western Hemisphere Affairs	4	11

*The Office of Inspector General (OIG) is included as a Voter for the sole purpose of allowing OIG to stay informed of changes to the Department's systems and to approve certain hardware or software added to the baseline for use exclusively by OIG. OIG abstains from voting on Department hardware or software change requests to maintain its independence, as required by laws and regulations. It would not be appropriate for OIG to endorse the use of a specific hardware or software for the Department, as OIG may no longer appear to be independent regarding that hardware or software.

Source: Prepared by Kearney from its review of voting records for 35 change requests.

Kearney found that all 35 change requests tested were authorized by Voters and moved on to be baselined. For these 35 change requests, not a single Voter rejected a change request. On the basis of its review of the VITCCB database and discussions with IT CCB officials, Kearney concluded that no change request has ever been rejected during the voting phase. Moreover, statements by the Voters themselves confirm that decisions are not necessarily made on the basis of substantive analysis. For example, one Voter stated that he would never reject a change request made by another bureau because that bureau might reject one of his own change requests someday. In addition, one Voter felt unqualified to say that a change request from another bureau should not be implemented. Further, one Voter stated that, upon receipt of the voting request, he immediately casts his vote without reviewing the change request. Finally, another Voter stated that he reviews guidance on the basis of his interest in the change request.

IT CCB Process Did Not Ensure That Change Requests Were Tested

"Testing" consists of assessing the proposed change to an application in a controlled developmental area prior to releasing the product or software into the live network to ensure the change does not negatively affect the network. According to NIST standards, a properly designed configuration change control process includes "testing the proposed change for security and functional impacts. Testing confirms the impacts identified during analysis and/or reveals additional impacts." The NIST standard also states that the "impacts of the change are presented to the [Configuration Control Board]." ²⁹ Kearney analyzed 78 change requests (of which 65 went to the technical review phase and 54 cleared the technical review phase) and found 49 (63 percent) that did not have documentation for testing included in the VITCCB. Moreover, the change requests that were tested were not tested for minimum requirements to ensure that a consistent approach was applied. Some of the change requests were significant to the Department's system. For example, one network infrastructure product used for Day 0³⁰ provisioning and network monitoring was baselined without any type of testing to determine how it would affect the network.

It is possible that testing was performed on the change requests at the bureau or post level; however, that information was not readily available to Technical Reviewers or Voters, who should have that information to ensure that items that modify the Department's IT baseline will not cause significant harm if they are approved. According to Department officials, Technical Reviewers can require the requestor to provide a copy of testing results during the technical review phase, but reviewers are not required to review that information. Voters, on the other hand, are not authorized to seek additional information from the change requestor. Therefore, a Voter would not be able to obtain testing information, even if interested in the results. IT CCB management does not require testing for change requests prior to adding the hardware or software to the baseline.

Several Deficiencies Led to Issues With Change Request Approvals and Testing

The IT CCB process is deficient in part because IRM has not implemented sufficient program management to execute the IT CCB process in accordance with Department and Federal policies. Kearney also found that IT CCB management designed an IT CCB process, which was outlined on the IT CCB website, to support the change request process. However, the design of the process was inadequate. Further, Kearney found deficiencies in the manner in which Technical Reviewers and Voters are appointed, as well as with policies and procedures, the VITCCB database, and training.

²⁹ NIST, Special Publication 800-128, Section 2.3.8, "Configuration Change Control."

³⁰ A Day 0 vulnerability is an undiscovered computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers, or a network.

Insufficient Program Management

The primary reason that the Department did not authorize or test change requests in accordance with Department and Federal policies was insufficient program management. IRM is responsible for ensuring the control over change requests. However, the Department has not put into practice sufficient Chief Information Officer (CIO) authority to manage IT CCB activities, as provided for in law. In addition, as OIG has reported, the CIO was not appropriately positioned to ensure that the IT CCB process was properly managed. Further, the implementing offices within IRM have not appropriately overseen the process, leaving the change request and approval process overall without strong leadership.

Office of Management and Budget requirements³¹ state that agency “CIOs must be positioned with the responsibilities and authorities to improve the operating efficiency of their agencies.” The Office of Management and Budget further states that agency CIOs will be held accountable for lowering operational costs, terminating and turning around troubled projects, and delivering meaningful functionality at a faster rate when enhancing the security of information systems. These authorities are intended to enable CIOs to reduce the number of wasteful duplicative systems, simplify services for the American people, and deliver more effective IT to support their agency’s mission.

The Office of Inspector General (OIG) has reported, as recently as November 2016, that the CIO was not, in fact, properly positioned within the organization to carry out required roles and responsibilities. OIG has also reported that, because the CIO was not properly positioned, the CIO could not ensure that the Department’s information security program was effective.³² This overall issue also affects the CIO’s ability to ensure that the change request process is properly managed. Because the CIO reports to the Under Secretary for Management, the CIO cannot effectively compel other bureaus, offices, and posts to implement a sufficient change control process. Moreover, other bureaus, offices, and posts are able to use funds to acquire IT equipment or systems without the approval of the CIO, who also lacks the authority to effectively control the implementation of the new equipment or systems.

In practice, the lack of sufficient CIO authority increases the need for a strong, centralized oversight function to ensure that changes requested for IT systems are safe and will not damage the Department’s IT infrastructure and also to ensure consistent implementation of OMB requirements. However, the Department has not established and implemented such strong, centralized oversight controls needed for IRM to perform this role appropriately under the current organizational structure. According to the FAH,³³ ENM (an IRM office that ultimately reports to the CIO) is responsible for the configuration change control process for the Department. However, Kearney found that ENM had not effectively implemented the authority

³¹ Office of Management and Budget, Memorandum M-11-29, “Chief Information Officer Authorities,” August 8, 2011.

³² OIG, *Audit of the Department of State Information Security Program* (AUD-IT-17-17, November 2016). Because OIG has made recommendations related to this topic in other reports, it is not offering a similar recommendation in this report.

³³ 5 FAH-5 H-512, “The Information Technology Change Control Board (IT CCB).”

communicated in the FAH. Throughout the audit, IT CCB management stated that its role was to facilitate the process rather than to be the program manager of the process. These officials also stated that they did not believe that they had the authority to exert control over the IT CCB process, even though the FAH states that ENM is responsible for configuration change controls within the Department.

Of the five phases in the IT CCB process (Bureau Sponsor review, scope review, technical review, voting, and baseline announcement), IT CCB management only actively participates in two—scope review and baseline announcement. For the other three phases, IT CCB management becomes involved only when individuals engaged in the process request support. IT CCB management does not actively engage in or monitor the process to ensure it is achieving stated objectives. Strong, centralized authority, however, is needed to ensure that change requests are reviewed and approved consistently and in accordance with requirements. To facilitate the IT CCB program management role established by the Department's FAH, IT CCB management should develop and implement a detailed program plan that lays out clear goals and objectives and defines areas of authority and responsibility.

Because the CIO is not properly positioned and IRM has not implemented a strong, centralized program management process for IT change requests, the Department does not have any bureau or office ultimately responsible for ensuring that changes made to the Department's baseline are safe. Also, no bureau or office can be held ultimately accountable if issues arise, because the process is decentralized.

Issues With the Design of the IT CCB Process

The design of the IT CCB process also played a role in the deficiencies. Kearney identified issues in the design of the process related to the lack of an approved list of change request submitters, the lack of requirements for supporting documentation and testing, allowing a change request to continue in the process even when a Technical Reviewer does not authorize the request, and the lack of a quality assurance program.

Lack of Control Over Change Request Submitters

According to NIST,³⁴ an information system owner is "the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system." Only system, product, or software owners should make change requests for their systems, product, or software. However, the IT CCB process has been designed to allow anyone in the Department who has a state.gov email address to submit a change request. IT CCB management does not maintain a list of acceptable change request submitters or system, product, or software owners, and IT CCB management cannot ensure that change requests are submitted by the correct owner. The failure to ensure that a request was made by a valid system, product, or software owner has created issues in the past. For example, a change

³⁴ NIST, Special Publication 800-100, "Information Security Handbook: A Guide for Managers," Chapter 8 – Security Planning.

request submitter incorrectly labeled a request for new software. Instead of requesting the software only for the requestor's office, the requestor mistakenly requested the software be updated for the entire Department. The enterprise-wide owner of the software was unaware of the change request until after changes had been approved and implemented and was unable to control the change request, as would have been appropriate.

Lack of Required Documentation for Change Requests

The IT CCB process is also insufficient because IT CCB management does not formally require submission of any supporting documentation for a change request. Although IT CCB management has established a list of recommended documentation, the change request submitter has discretion to decide what documentation to provide. In practice (although this practice is not formalized), IT CCB management requires submitters to provide the Reviewer's Questionnaire and the VPAT/Section 508 compliance document. Because documentation is not required when the change request is submitted, Technical Reviewers often have to request the documentation during that phase of the process, outside the VITCCB, which is inefficient. Therefore, information obtained by the Technical Reviewers may not be available for Voters to review. It is essential for IT CCB management to determine what documents should be provided during the IT CCB process.

Lack of Minimum Testing Requirements

According to Federal Standards related to configuration control boards,³⁵ "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." As already noted, though, the IT CCB process does not require testing. Not only is testing not required by the IT CCB, testing documentation is not even included on the list of documents recommended to submitters. The absence of such a requirement means that the IT CCB does not comply with NIST standards related to establishing minimum requirements for the testing.

Lack of Affirmative Concurrence of All Technical Reviewers

Technical reviews are a vital component of the IT CCB process. It is essential for Technical Reviewers to perform a thorough review of change requests to ensure that changes will not harm the Department and its systems. Notwithstanding the importance of these reviews, IRM has established an IT CCB process that does not require Technical Reviewers to authorize a change request before the change request moves forward in the process. Instead, as reported in the Audit Results section of this report, the process allows a "default proceed" if a Technical Reviewer has not completed a review within the allotted time period. As discussed previously, IT CCB management expressed the belief that default proceeds do not necessarily reflect an absence of review. However, without confirmation from a Technical Reviewer, it is impossible to know whether a change request was, in fact, reviewed. That means that the IT CCB process has

³⁵ NIST, Special Publication 800-128, "Establish Configuration Control Board for Information System."

been designed to allow change requests to potentially move forward without any type of technical review. This is another way in which the design of the IT CCB process is inadequate.

Lack of Quality Assurance Program for the IT CCB Process

The FAH states that quality assurance “provides a framework from which to monitor the requirements and specifications. It helps to ensure that project guidelines, and procedures are being followed in the development of services and products.”³⁶ Although Department guidance describing change control processes stresses the importance of quality assurance, IT CCB management does not perform a quality assurance review during the IT CCB process. This is yet another way that the process is improperly designed. For example, IT CCB management does not ensure that change requests comply with the control guidelines established for the IT CCB process. Also, IT CCB management does not monitor the number of “default proceeds” or ongoing “stops” that occur during the IT CCB process. The implementation of a quality assurance process could include the review of processed “default proceeds,” evaluation of open “stops,” collection of all relevant documentation for retention, and a check to ensure all pertinent process controls occurred.

Deficiencies in the Appointment of Technical Reviewers and Voters

Kearney assessed the process to appoint and vet Technical Reviewers and Voters. Kearney determined that the controls surrounding the appointment of Technical Reviewers and Voters were insufficient to ensure that appropriate officials were assigned to these roles. Specifically, Kearney found that Technical Reviewers and some Voters were not officially appointed to the roles that they filled, Technical Reviewers and Voters were not properly vetted, and segregation of duties was not considered when assigning officials to the Technical Reviewer or Voter roles. In addition, appointments of alternative Technical Reviewers and Voters were insufficient to ensure that the IT CCB process was not delayed if someone was unavailable.

Technical Reviewers and Voters Lack Official Appointment

According to the IT CCB website, all Technical Reviewers and Voters must be appointed prior to performing their roles. Specifically, according to IT CCB guidance, Technical Reviewers require formal appointment by the Bureau’s Executive Director before they begin in the role. Kearney requested the appointment letters for all 76 Technical Reviewers in place as of January 6, 2017, and found that none of the 76 Technical Reviewers could provide official letters of appointment. Kearney also requested the appointment letters for the 76 Voters³⁷ in place as of January 6, 2017, and found that 55 (72 percent) Voters were not formally appointed.

³⁶ 5 FAH-5 H-413, “IT CCB Assessment Request (AR) and Approval.”

³⁷ A maximum of 23 votes can be cast for a change request. Both primary and alternate reviewers comprise a total of 76 Voters.

Technical Reviewers and Bureau Sponsors/Voters Are not Vetted Prior to Appointment

Kearney found no requirement to consider an employee's knowledge, skills, and abilities before an employee is appointed a Technical Reviewer or Voter. A number of Technical Reviewers and Voters stated that they began reviewing change requests as one of many duties that they were assigned upon promotion, but others were told to fulfill this role when a supervisor departed. However, their ability to perform the technical review or the voting was not considered before they were assigned. The lack of experience of some officials responsible for technical reviews or voting may limit their ability to effectively review and authorize change requests. Some officials who submit change requests noted this as an issue in response to Kearney's customer survey.³⁸ For example, one respondent stated that "the [T]echnical [Reviewer] should be someone knowledgeable of the field they are technically reviewing...most of the stops are because one doesn't understand or know about the field that they are reviewing, which sets a requester back when trying to accomplish a goal. In other words they waste time."

Lack of Segregation of Duties Across IT CCB Roles

Government Accountability Office guidance³⁹ requires management to consider "segregation of duties in designing control activity responsibilities so that incompatible duties are segregated." The Standards also state that segregation of duties "helps prevent fraud, waste, and abuse in the internal control system." Kearney found that segregation of duties is not required to be considered before appointing a Technical Reviewer or a Voter. For example, Kearney identified one official who had served as a Bureau Sponsor, a Technical Reviewer, and a Voter simultaneously during a 3-year period. This means that the same individual was responsible for both promoting and approving a particular change.

Insufficient Alternates for Technical Reviewers and Voters

Kearney also found that Technical Reviewers and Voters may not have sufficient alternates identified to ensure that the IT CCB process moves forward even when someone is unavailable. A total of 59 Primary and Alternate Technical Reviewers and 54 Primary and Alternate Voters are appointed to the IT CCB.⁴⁰ Alternate Technical Reviewers or Voters only participate when called on to do so by the Primary Technical Reviewer or Voter. Twenty designated offices are responsible for technical reviews. Of those 20 offices, Kearney found that 1 does not have an appointed primary Technical Reviewer. In addition, the Technical Reviewer appointed for the Regional Bureaus, who is responsible for focusing on how a change would affect regional bureau operations, does not have an alternate.

³⁸ Appendix B includes the survey questions and results.

³⁹ Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

⁴⁰ According to the IT CCB's list of Technical Reviewers and Voters, an additional 17 members are included in the VITCCB as Technical Reviewers and 22 as Voters. These members are not designated as primary or alternates but have titles within VITCCB such as Office Director or Managing Office Director. During the audit, Technical Reviewers and Voters stated that these members do not actively participate in the IT CCB but serve in an oversight capacity.

Furthermore, only 22 primary Voters are among the 23 bureaus with voting responsibilities. Of those 22 primary Voters, 4 (18 percent) do not have alternate Voters. One of the bureaus that does not have an alternate identified is IRM, which is the bureau that submits the largest number of change requests annually. In addition, although the Bureau of African Affairs had identified an alternate Voter, no primary Voter was appointed.

Deficiencies in Policies and Procedures

According to the Government Accountability Office, management should implement control activities through well-documented policies. Well-designed policies and procedures are needed to ensure that IT CCB requirements are consistently understood and executed, leading to requests being processed efficiently and timely. However, Kearney found that the available policies and procedures related to the IT CCB process were simultaneously inconsistent and insufficient. Throughout the audit, IT CCB management stated that the sole source of authoritative guidance on the IT CCB process is the IT CCB website. In addition to the information on its website, which the IT CCB considers to be its policy, IT CCB management has developed several tutorial guides for groups of users. These documents do not include policy guidance but instead provide information on the mechanics of implementing the different roles. Specifically, the IT CCB has developed a "Submitter's Guide,"⁴¹ a "Sponsor/Voter Guide,"⁴² and a "Reviewing Authority User Manual."⁴³

During the audit, various users of the IT CCB process mentioned a 2014 standard operating procedure issued by IT CCB management; these users stated that they relied on this 2014 document to better understand the process. IT CCB management, however, determined that the 2014 guidance should no longer be used because maintaining guidance on the website should be sufficient for IT CCB users. Although the standard operating procedure document is no longer officially in use, some users who were familiar with the document stated that they continue to refer to the document because it provides more detailed guidance than does the IT CCB website. Kearney obtained a copy of the 2014 guidance and found that it outlined the steps, roles, and responsibilities of the IT CCB for the three types of change requests allowed in 2014. Because the document was still consulted by some users, Kearney assessed the guidance that was included.

To determine whether the Department's policy was consistent with Federal and Department requirements, Kearney compared key items from NIST 800-128 and guidance from the FAM and the FAH to the 2014 IT CCB Standard Operating Procedure, as well as to guidance included on the IT CCB website. As shown in Table 5, Kearney found that IT CCB management's guidance did

⁴¹ The "Submitter's Guide" is designed to help a change request submitter prepare and submit a change request using the VITCCB.

⁴² The "Sponsor/Voter Guide" is designed to help Bureau Sponsors and Voters use the VITCCB to sponsor and vote on change request submissions.

⁴³ The "Reviewing Authority User Manual" is designed to help describe the change request process and to help Technical Reviewers perform their reviews using the VITCCB.

not always reflect guidance from NIST or the FAM and the FAH. Moreover, Kearney identified inconsistencies in IT CCB management's guidance.

Table 5: Comparison of Federal and Department Guidance to ENM Guidance

Topic Area	Federal and Department Guidance	IT CCB 2014 SOP	IT CCB Website
Change Request Testing	Every change should be tested	Local CCB tests	No provision
Bureau Sponsorship	No provision	Coordination with bureau sponsor required for submission	No provision
Technical Review	Change request process should occur within 2 weeks	No provision	Change request process should occur within 2 weeks
Authorization of Change Requests	Approval to be performed by Configuration Control Board	A majority of Voters needed for approval	A majority of Voters needed for approval
Supporting Documentation Retention	Documentation retention is required	Supporting documentation provided as needed	No provision
Quality Assurance	Required	No provision	No provision

Source: Prepared by Kearney from an analysis of available guidance.

Kearney also compared information on the IT CCB website to information included in the supplemental guides and found other inconsistencies. For example, the "Submitter's Guide" states that the change request submitter must obtain specific documentation for a request, although the website explains that all documentation is recommended but not required.

The lack of sufficient policies and procedures extends to the amendment process, which as noted, will likely be reinstituted at some point. Before the amendment process was discontinued in FY 2016, the IT CCB had no comprehensive policies and procedures to authorize amendments. The only information available on the amendment process was in the 2014 standard operating procedures, which was no longer in effect.

Deficiencies in the New Virtual IT CCB Database

IT CCB management deployed a new VITCCB for use across the Department in FY 2016. Kearney found that data were not transferred accurately and completely from the former database to the new database, which is one cause of the deficiencies identified by Kearney related to the IT CCB process. Specifically, IT CCB management decided to migrate change requests from FY 2012 through FY 2016 to the new VITCCB database and leave data from prior years in the old VITCCB database. However, IT CCB management did not validate the transferred information to ensure that the required data were indeed transferred. Kearney identified 53 change requests from FY 2012 through FY 2016 in the old database that should have been, but were not, transferred to

the new database. In addition, IT CCB management elected to copy the data from the old database to the new database rather than migrating the data; this means that some of the same records appear in both databases, which can confuse users. Furthermore, both the new and old VITCCB databases were left open to serve as a resource for Department users. Kearney also identified a duplicate change request in the system. The details of the request were the same, but each item had a different change request number.

Deficiencies in Training on the IT CCB Process and Roles and Responsibilities

Kearney found that IT CCB management did not provide training to people who could submit change requests or to officials involved in the authorization process. A number of Technical Reviewers and Voters confirmed that they had received no training or guidance from IT CCB management on their roles and responsibilities in the IT CCB process. Instead, they stated that the only guidance provided was from the individual who previously held the position. Some Technical Reviewers did not believe that training or guidance was necessary. For example, one Technical Reviewer stated that he was the subject matter expert and did not need instructions from IT CCB management on performing reviews. However, Kearney noted the inconsistent use of the “stop” function. The basic understanding of the functionality is to stop change requests upon the identification of issues; however, Technical Reviewers used the “stop” function for no identifiable reason or to gain more time. IT CCB management stated that Technical Reviewers could request further time for technical reviews, but Kearney did not obtain any evidence of a request for additional time for any change request tested.

Training is an important method to ensure key officials are aware of requirements and to ensure consistency in a process. Therefore, regular updates or training to submitters, Technical Reviewers, and Voters would be useful. In addition, once IT CCB management addresses the issues set forth in this report related to insufficient program management, ineffective process design, and lack of policies and procedures, it will be especially important for IT CCB management to develop a methodology, such as a training session, in which changes are communicated to all key officials involved in the process.

Networks, Applications, and Software at Risk

Without a well-designed or monitored change request process, the Department is at risk of introducing changes that may compromise the security, efficiency, and effectiveness of its general support systems, as well as the operational and financial applications that reside on them. Because IT CCB management believes that it only has the authority to facilitate the IT CCB process and not to manage it, the overall process is inconsistently applied, increasing the risk that improperly reviewed change requests will have detrimental effects on the Department’s network and applications.

Implementing software 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 unavailable to support the mission of the Department. For example, Kearney found that the IT CCB had

approved the installation of a device for which testing had not been completed on the Department's network. When the device was installed, it created issues with other previously installed products. Had testing for this device been completed before it was installed, the Department may well have avoided those issues.

In addition, because the IT CCB process allows routine changes to automatically proceed without the authorization of all Technical Reviewers once a predefined time limit has passed, the Department may not be considering key areas such as privacy, network capacity, IT security, and contingency planning before implementing a change to its IT baseline. For example, one change request related to the Department's approved cloud console moved forward without approval from the Technical Reviewer responsible for IT Security. As data retention within the Department moves toward virtual servers and cloud environments, a review of IT security is needed to ensure that data retain their integrity and remain protected.

The Voters, acting on behalf of their bureaus, should function as the final review of the change management process to ensure that a proposed change does not harm the bureau or the enterprise as a whole. Because Voters were not always reviewing all changes and did not consistently have sufficient information, the Department may be unknowingly exposing itself to exploitable vulnerabilities or introducing changes that compromise other bureaus or the enterprise.

Customers are not satisfied with the services provided by the IT CCB. In response to a customer survey, only 53 percent of respondents (20 of 38) stated they were either satisfied or very satisfied with the change request process.

Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a detailed program plan for the Information Technology Configuration Control Board process that includes clear goals and attainable objectives and defines areas of authority and responsibility.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a detailed program plan for the IT CCB process that includes clear goals and attainable objectives and defines areas of authority and responsibility.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management develop and implement a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. The list should be made available to users and members of the Information Technology Configuration Control Board through the Information Technology Configuration Control Board website or applicable policies and procedures outlined in Recommendation 12.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. This detail should also be made available via the IT CCB website.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management determine what documentation is needed to support a change request and modify the policies and procedures outlined in Recommendation 12 or other guidance, such as the submitters guide, provided to change request submitters to reflect the documentation that is required for a complete and accurate change request submission.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM determined what documentation is needed to support a change request and modified policies and procedures to reflect the documentation that is required for a complete and accurate change request submission.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when

OIG receives and accepts documentation demonstrating that IRM developed and implemented guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.

Recommendation 5: OIG recommends that the Bureau of Information Resource Management remove the default proceed ability for Technical Reviewers in the Virtual Information Technology Configuration Control Board application.

Management Response: IRM did not concur with this recommendation, stating that the impact of the recommendation would “be a decrease in ITCCB efficiency.” IRM also stated that “this runs counter to the OIG recommendations concerning timeliness, feedback from the Secretary’s recently accomplished listening tour, and emergent guidance from OMB concerning the need to appropriately balance business need and IT risk management. In practice, a ‘default proceed’ means a [T]echnical [R]eviewer utilized the maximum allotted time and found no reason to stop the submission. Technical [R]eviewers are equally responsible for their review, regardless if it is a ‘default’ or ‘explicit’ proceed. The net impact of this recommendation, removing the ‘default proceed,’ will be the transformation of the ‘default proceed’ into the only available alternative, a ‘default stop.’ This contradicts the recommendations to improve timeliness.” IRM also stated that its “analysis of the historical data does not identify the ‘default proceed’ as a root cause of ITCCB inefficiency and the assertions that underpin this recommendation appear to be a hypothetical as opposed to an actually observed challenge.”

OIG Reply: Because IRM did not concur with the recommendation or provide an acceptable alternative that meets the recommendation’s intent, OIG considers this recommendation unresolved. Although OIG acknowledges the need for an efficient process, IRM’s comments regarding the need to appropriately balance business need and IT risk management overlook the requirement that IT risk management should be effective in addition to efficient. OIG also notes that the analysis contained in the report does not contend that the default proceed was the “root cause of IT CCB inefficiency;” it explains instead that the use of the default proceed is a substantive flaw that can compromise the appropriateness of change request approvals. Moreover, as a factual matter, OIG does not agree that a “default proceed” means that a Technical Reviewer performed a review and found no reason to stop the submission. In fact, as detailed in the Audit Results section of this report, Technical Reviewers reported precisely the contrary to Kearney in stating that, when they allowed the system to “default proceed” on a change request, it did not necessarily mean that they had performed a full technical review on the request. OIG also questions IRM’s statement that “[T]echnical [R]eviewers are equally responsible for their review,” even if the “default proceed” is used. It is unclear how a Technical Reviewer can be “responsible” for a review when there is no documented approval to confirm that he or she actually evaluated the

request. For example, if a Technical Reviewer who did not have a back-up, was on leave during the period of time a change request was pending, this change request would be moved forward in the process using the “default proceed” feature even though the Technical Reviewer had never looked at the request. It would be impossible to hold this Technical Reviewer accountable for any problems with the implementation of the change request because the Reviewer was unavailable during the period of review. As stated in the report, IRM’s decision to allow change requests to move forward without an affirmative approval from key Technical Reviewers is putting its systems at risk.

This recommendation will be considered resolved when the IT CCB clearly demonstrates that it plans to implement this recommendation or provides an alternative solution that meets the intent of the recommendation. This recommendation will be closed when IRM provides documentation of the removal of the default proceed capability and the implementation of documentation to prove the technical review occurred to support the approval, stop, or rejection of the change request.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management formally notify all Technical Reviewers that default proceeds are no longer allowed and that all Technical Reviewers must review all change requests and either approve, stop, or reject the change request. Policies and procedures outlined in Recommendation 12 or other guidance should be updated to reflect this change to the process.

Management Response: IRM did not concur with this recommendation, stating that the impact of the recommendation would be a “decrease in [IT CCB] efficiency.” IRM also stated that “this runs counter to the OIG recommendations concerning timeliness, feedback from the Secretary’s recently accomplished listening tour, and emergent guidance from the OMB concerning the need to appropriately balance business need and IT risk management. In practice, a ‘default proceed’ means a technical reviewer utilized the maximum allotted time and found no reason to stop the submission. Technical reviewers are equally responsible for their review, regardless if it is a ‘default’ or ‘explicit’ proceed. The net impact of this recommendation, removing the ‘default proceed,’ will be the transformation of the ‘default proceed’ into the only available alternative, a ‘default stop.’ This contradicts the recommendations to improve timeliness.” IRM also stated that its analysis of “historical data does not identify the ‘default proceed’ as a root cause of [IT CCB] inefficiency and the assertions that underpin this recommendation appear to be a hypothetical as opposed to an actually observed challenge.”

OIG Reply: Because IRM did not concur with the recommendation or provide an acceptable alternative that meets the recommendation’s intent, OIG considers this recommendation unresolved. As detailed in OIG’s response to Recommendation 5, IRM’s comments regarding the need to appropriately balance business need and IT risk management overlooks the requirement that IT risk management should be effective in addition to efficient. As stated in the report, IRM’s decision to allow change requests to move forward without an affirmative approval from key Technical Reviewers is putting its systems at risk. As set forth above, the

analysis contained in the report does not contend that the default proceed was the “root cause of IT CCB inefficiency;” it explains instead that the use of the default proceed is a substantive flaw that can compromise the appropriateness of change request approvals. OIG also notes that IRM’s statement that eliminating the “default proceed” will effectively implement a “default stop” system seemingly presumes that Technical Reviewers are not, in fact, reviewing the requests. If IRM is correct that Technical Reviewers are analyzing requests and making a decision that the changes are appropriate, there seems to be no reason that requiring affirmative approval would affect timeliness in the first place. This recommendation will be considered resolved when the IT CCB clearly demonstrates that it plans to implement this recommendation or provides an alternative solution that meets the intent of the recommendation. This recommendation will be closed when IRM provides documentation demonstrating that it has notified Technical Reviewers that default proceeds are no longer allowed and policies and procedures are updated to reflect the process change.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a quality assurance assessment process for all change requests going through the enterprise-wide Information Technology Configuration Control Board. At a minimum, the quality assurance process should include periodic evaluation of open “stops,” reviews to ensure retention of all relevant documentation, and a final check prior to adding change to the baseline to ensure all pertinent process controls occurred at a minimum.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM’s concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a quality assurance assessment process for all change requests going through the enterprise-wide IT CCB.

Recommendation 8: OIG recommends that the Bureau of Information Resource Management verify, no later than 30 days after the final issuance of this report, that all Technical Reviewers and Voters that participate in the Information Technology Configuration Control Board process are formally appointed.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM’s concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM verified, no later than 30 days after the final issuance of this report, that all Technical Reviewers and Voters who participate in the IT CCB process are formally appointed.

Recommendation 9: OIG recommends that the Bureau of Information Resource Management develop and implement a process to formally appoint new Technical Reviewers and Voters who participate in the Information Technology Configuration Control Board process.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a process to formally appoint new Technical Reviewers and Voters who participate in the IT CCB process.

Recommendation 10: OIG recommends that the Bureau of Information Resource Management define the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the Information Technology Configuration Control Board process.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM defined the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the IT CCB process.

Recommendation 11: OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that Technical Reviewers and Voters have formally appointed alternatives.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a process to verify that Technical Reviewers and Voters have formally appointed alternatives.

Recommendation 12: OIG recommends that the Bureau of Information Resource Management develop and implement complete and consistent policies and procedures and supplemental guidance, such as a Submitter's Guide, for the Information Technology Configuration Control Board process. The policies, procedures, and guidance should, at a

minimum, include guidance on roles and responsibilities, detailed procedure steps for submitters, minimum testing requirements, instructions on how Technical Reviewers and Voters should conduct their review, the appropriate use of "stops," and established timelines for the process.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented complete and consistent policies and procedures and supplemental guidance, such as a Submitter's Guide, for the IT CCB process.

Recommendation 13: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically review and validate the accuracy and completeness of the data in the Virtual Information Technology Configuration Control Board database and to correct data integrity, omissions and inaccuracies existing between the new and old databases and when identified going forward. As part of this effort, the Bureau of Information Resource Management should ensure that the old database is available solely as a read-only reference resource and that new data cannot be entered into that database.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a process to periodically review and validate the accuracy and completeness of the data in the VITCCB database.

Recommendation 14: OIG recommends that the Bureau of Information Resource Management develop and implement required, periodic, training for Information Technology Configuration Control Board management and personnel, Bureau Sponsors, Technical Reviewers, Voters, and change request submitters involved in the Information Technology Configuration Control Board process.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented required, periodic training for IT CCB management and personnel, Bureau Sponsors, Technical Reviewers, Voters, and change request submitters involved in the IT CCB process.

Finding B: The Information Technology Configuration Control Board Did Not Meet Internal Deadlines for Processing Change Requests.

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 was noted 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. The IT CCB could take advantage of some of the capabilities of its VITCCB system to assist in monitoring the status of change requests. 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. As described in Finding A of this report, Kearney also found inaccurate data in the VITCCB system, which makes monitoring more difficult. In addition, the IT CCB does not have a process to periodically assess the accuracy of data in the system or to correct data issues when inaccuracies are identified. Also, as discussed in Finding A, the IT CCB did not have sufficient policies and procedures for its customers or its stakeholders. The lack of sufficient policies and procedures also affected the IT CCB's ability to meet its established deadlines for change request reviews. As a result of untimely processing of change requests, the Department could be exposed to network vulnerabilities.

IT CCB Did Not Process Many Change Requests in Accordance With Deadlines

The IT CCB has developed internal deadlines for most of the change request review phases as shown in Table 6.

Table 6: Change Request Processing Timeline

Priority	Submission	Bureau Sponsor Review	Scope Review	Technical Review	Voting	Baseline	Total Days
Routine	No Limit	No Limit	2 days	14 days	3 days	1 day	20 days
Expedited	No Limit	No Limit	1 day	3 days	1 day	1 day	6 days
Emergency	No Limit	No Limit	1 day	1 day	1 day	1 day	4 days

Source: Prepared by Kearney from information on the IT CCB website.

To determine whether the Department processed change requests in a timely manner, Kearney reviewed a sample of 65 change requests submitted to the IT CCB.⁴⁴ Kearney found that the Department had processed 38 of the 65 (58 percent) change requests in an untimely manner, either not meeting the overall deadline for processing a change request or not meeting one or more deadlines for a phase.

⁴⁴ Of the 65 sampled change requests, 52 were submitted in FY 2016 and 13 were submitted in prior fiscal years. All 13 prior fiscal year requests were listed as being open during the time of sample selection. None of the selected items was designated an emergency.

Overall Deadline

Of the 65 change requests reviewed, Kearney was only able to test the Department's adherence to the IT CCB overall deadlines for 42, because the Department discontinued 23 change requests at various process stages. As shown in Table 7, of the 42 change requests that Kearney reviewed to assess compliance with the overall deadline, Kearney found that 18 (43 percent) were not processed in the allotted number of days—20 days for routine submissions and 6 days for expedited submissions. In one instance, the IT CCB took 124 days to process a routine change request.

Table 7: Overall Processing Time

Priority	Change Requests Tested	Untimely Responses to Change Requests	Percentage of Untimely Responses to Change Requests	Average Number of Days Taken For All Requests	Average Number of Days Late for Overdue Requests
Routine	41	18	44	50	76
Expedited	1	0	0	5	0
Total	42	18	43	49	76

Source: Prepared by Kearney from testing results.

Scope Review

As shown in Table 8, of the 65 reviewed change requests that went through the scope review phase of the process, Kearney found that the scope review for 2 (3 percent) requests was not performed in the allotted number of days (2 days for routine submissions and 1 day for expedited submissions). In one instance, the scope review was 20 days late.

Table 8: Timeliness of Scope Reviews

Priority	Scope Reviews Tested	Untimely Scope Reviews	Percentage of Untimely Scope Reviews	Average Number of Days Taken For All Reviews	Average Number of Days Late for Overdue Reviews
Routine	64	2	3	1	13
Expedited	1	0	0	0	0
Total	65	2	3	1	13

Source: Prepared by Kearney from testing results.

For the two untimely scope reviews, IT CCB Management sent the change request back to the submitter requesting additional documentation or clarification, delaying the continuation to the technical review stage.

Technical Review

As shown in Table 9, of the 54 reviewed change requests that went through the technical review phase of the process,⁴⁵ Kearney found that for 24 (44 percent) the technical review was not performed in the allotted number of days (14 days for routine submissions and 3 days for expedited submissions). Kearney found one technical review that was 896 days late. In addition, Kearney found that 10 of the 24 untimely technical reviews were at least 100 days overdue.

Table 9: Timeliness of Technical Reviews

Priority	Technical Reviews Tested	Untimely Technical Reviews	Percentage of Untimely Technical Reviews	Average Number of Days Taken For All Reviews	Average Number of Days Late for Overdue Reviews
Routine	53	23	43	94 days	187 days
Expedited	1	1	100	4 days	1 day
Total	54	24	44	93 days	174 days

Source: Prepared by Kearney from testing results.

As discussed in Finding A of this report, Technical Reviewers have the ability to “stop” any change requests. If a Technical Reviewer places a “stop” on a change request, the request will not continue through the process until the Technical Reviewer clears the “stop” in the VITCCB. Kearney found that 8 of the 24 (33 percent) untimely change requests were “stopped” at some point during the technical review process.

In response to a customer satisfaction survey conducted by Kearney,⁴⁶ 22 of 38 (58 percent) respondents stated that they had at least one change request that had been “stopped” during the technical review phase. Nine of the 22 (41 percent) respondents stated that they had submitted more than 4 change requests that had been “stopped.” As discussed in Finding A of this report, the use of “stops” is not sufficiently defined and can be used for legitimate and illegitimate reasons.

⁴⁵ Of the 65 change requests reviewed, 11 were “stopped” or remained inactive as a result of unfulfilled “stop” requirements, which prevented them from moving forward in the process.

⁴⁶ Appendix B includes survey questions and results.

Voting

Of the 35 change requests reviewed that went through the voting phase of the process,⁴⁷ all were voted on in the allotted number of days, (3 days for routine submissions and 1 day for expedited submissions). Kearney found the average number of days taken to complete voting was less than one.

Baseline

As shown in Table 10, of the 42⁴⁸ change requests reviewed that went to the baseline phase of the process, Kearney found that the baseline announcement for 6 (14 percent) was not performed in the allotted number of days (1 day for all types of submissions). In one instance, Kearney found the IT CCB did not announce an approved change request to the baseline for 172 days.

Table 10: Timeliness of Baseline Announcements

Priority	Baselines Tested	Untimely Baselines	Percentage of Untimely Baselines	Average Number of Days Taken For All Baselines	Average Number of Days Late for Overdue Baselines
Routine	41	6	14	7 days	44 days
Expedited	1	0	0	0 days	0 days
Total	42	6	14	7 days	44 days

*Average number of days includes one change request that was not announced to the baseline for 172 days and another that was not announced to the baseline for 74 days. Excluding these two change requests, the average number of days taken is 1 day and the average number of days late is 5 days.

Source: Prepared by Kearney from testing results.

Four of the six change requests that the IT CCB did not announce to the baseline in a timely manner were System Authorization Requests, which require manual processing. The manual processing affected the timing of the announcement. The other two baselines announcements that were delayed were processed automatically.

⁴⁷ Of the 65 change requests reviewed, 54 were subject to the technical review phase. Of those 54 change requests, 12 did not complete the technical review process as of January 4, 2017, because of inactivity (that is, the change request was "stopped" at some point, preventing it from proceeding to voting) or withdrawal. Of the remaining 42 change requests that completed the technical review phase, 7 were not required to go through the voting process, in accordance with IT CCB policies. Therefore, a total of 35 change requests were subject to the voting phase of the IT CCB process.

⁴⁸ Although only 35 change requests were voted on, the 7 that were exempt from voting still required a formal baseline announcement; therefore, they are included in the total change requests that were fully processed to the baseline announcement.

ITCCB Lacked Monitoring Procedures, Accurate Data, and Sufficient Policies and Procedures

One reason that the IT CCB did not always meet its timeliness metrics was that it has not developed and implemented sufficient monitoring procedures. The IT CCB could take advantage of some of the capabilities of its VITCCB system to assist in its monitoring activities. 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 deadlines were met. As reported in Finding A of this report, Kearney also found inaccurate data in the VITCCB system, which makes monitoring more difficult. In addition, the IT CCB does not have a process to periodically assess the accuracy of data in the system or to correct data issues when identified. Further, as discussed in Finding A of this report, the IT CCB did not have sufficient policies and procedures for its customers or its stakeholders. The lack of sufficient policies and procedures also affected the IT CCB's ability to meet its established deadlines for change request reviews.

Lack of Monitoring Procedures

According to Government Accountability Office guidance,⁴⁹ management should "establish and operate monitoring activities." The guidance goes on to state that ongoing monitoring should be "built into the entity's operations, performed continually, and responsive to change." Kearney found that change requests were not always processed in a timely manner in part because the IT CCB had not designed or implemented a process to monitor the status of those requests. The IT CCB needs monitoring procedures to effectively prioritize requests, manage workloads, and ensure timeliness.

Although IT CCB officials explained that they sometimes perform impromptu searches using VITCCB to view the status of requests, the officials also stated that they do not use routine VITCCB reports that show the status of each change request currently in process. As the Government Accountability Office guidance⁵⁰ states, "ongoing monitoring may include automated tools, which can increase objectivity and efficiency" However, Kearney found that, in some cases, the VITCCB is not designed to assist in the monitoring process, and in other cases, it is not being effectively used by IT CCB officials. For example, Kearney found that the VITCCB does not include a routine process to alert the appropriate IT CCB stakeholders when a request is approaching the established deadlines for that phase. In addition, the VITCCB does not notify all stakeholders when an event occurs in the system that may affect the timeliness of a request, such as a request being "stopped" by a Technical Reviewer.⁵¹ IT CCB officials do not track the status of stopped requests. IT CCB officials stated that, although VITCCB can track and report information that would be useful for monitoring the process, such as status related metrics, this function is not being used. Without effective monitoring procedures, change requests may remain open or stopped for significant periods of time without accountability. As reflected in the

⁴⁹ GAO, "Standards for Internal Control in the Federal Government", GAO-14-704G, (September 2014).

⁵⁰ Ibid.

⁵¹ Only the Requestor is notified when a Technical Reviewer "stops" a change request.

responses to a customer service satisfaction survey, the IT CCB needs better oversight to hold Technical Reviewers accountable for actions and to decrease processing times.

In addition, Kearney found that, although the IT CCB has set timeliness metrics for each phase of the change request review process, it does not have a process to track and report whether those standards are met. Maintaining a scorecard to track metrics is a way to evaluate and communicate performance. This type of reporting would be useful for both IT CCB officials and those who request changes.

Unreliable Request Status Data

As described in Finding A of this report, Kearney also found inaccurate data in the VITCCB system, which makes monitoring more difficult. In addition, the IT CCB does not have a process to periodically assess the accuracy of data in the system or to correct data issues when inaccuracies are identified. According to the Government Accountability Office guidance,⁵² management should “use quality information to achieve the entity’s objectives.” Therefore, to effectively monitor the timeliness of individual change requests, IT CCB officials need to have accurate and readily available data reflecting the status of each open request. However, Kearney found that information in the VITCCB was not always accurate. For example, Kearney found instances in which the VITCCB was not updated when the status of change requests changed. Kearney reviewed 13 change requests that were initiated prior to FY 2016 but remained open in VITCCB at the time of the audit. Although these change requests were still shown as open in VITCCB, Kearney found that a completion date was not listed. In fact, although no completion date was included, Kearney confirmed that none of the 13 requests remained open. Some of the requests had been withdrawn and others were stopped during the process and were not resumed by the requester. Kearney determined that IT CCB officials did not have a sufficient process in place to assess the accuracy of the data in VITCCB or to correct data deficiencies. Without accurate data on the status of active requests, the IT CCB’s ability to effectively identify and prioritize requests will be limited. The recommendation for this deficiency is included in Finding A of this report.

Insufficient Policies and Procedures

As detailed in Finding A of this report, Kearney also found that the IT CCB did not have sufficient guidance for the IT CCB process, which is another factor affecting the IT CCB’s ability to process requests in a timely manner. Well-designed policies and procedures are needed to ensure that IT CCB requirements are understood and executed, which could lead to requests being processed efficiently and promptly. The recommendation for this deficiency is included in Finding A of this report.

⁵² GAO-14-704G.

Untimely Processing Introduces Risk

The untimely processing of change requests submitted to the IT CCB could expose the Department to network vulnerabilities. If a change request that is needed to protect a system or application from a vulnerability is submitted, the excess time spent on the review could lead to increased risks. For example, Kearney found one change request related to wireless security that took 71 days to process, 57 days longer than the allotted timeframe. If security-specific changes do not deploy when expected, system failures could occur, increasing the potential for Department threats.

Untimely processing of change requests can also lead to customer dissatisfaction. Twelve of 48 (25 percent) respondents to a customer satisfaction survey performed by Kearney⁵³ included negative responses to at least one subjective survey question directly related to the length of time that it took for a change request to go through the process. For example, one respondent stated that Technical Reviewers initiate “stops” without an apparent need. Additionally, as shown in Table 11, a number of respondents to the customer satisfaction survey were dissatisfied with the timeliness of one or more phases of the process.

Table 11: Timeliness Survey Results

Processing Stage	Number of Dissatisfied Survey Responses	Number of Very Dissatisfied Survey Responses
Bureau Sponsor(s)	5	0
Technical Reviewer(s)	8	3
IT CCB Voters	3	2
IT CCB Management	2	3

Source: Prepared by Kearney from results of customer survey.

Recommendation 15: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a request is nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM’s concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and implemented a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a request is

⁵³ Appendix B includes survey questions and results.

nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.

Recommendation 16: OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to hold officials accountable for failure to meet established deadlines in the Information Technology Configuration Control Board change request process. Once completed, the policies, procedures, and supplemental guidance discussed in Recommendation 12 should be updated.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented policies and procedures to hold officials accountable for failure to meet established deadlines in the IT CCB change request process.

Recommendation 17: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers in addition to appropriate bureau officials.

Management Response: IRM concurred with the recommendation.

OIG Reply: On the basis of IRM's concurrence with the recommendation, OIG considers this recommendation resolved pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM developed and implemented a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers, in addition to appropriate bureau officials.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a detailed program plan for the Information Technology Configuration Control Board process that includes clear goals and attainable objectives and defines areas of authority and responsibility.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management develop and implement a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. The list should be made available to users and members of the Information Technology Configuration Control Board through the Information Technology Configuration Control Board website or applicable policies and procedures outlined in Recommendation 12.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management determine what documentation is needed to support a change request and modify the policies and procedures outlined in Recommendation 12 or other guidance, such as the submitters guide, provided to change request submitters to reflect the documentation that is required for a complete and accurate change request submission.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.

Recommendation 5: OIG recommends that the Bureau of Information Resource Management remove the default proceed ability for Technical Reviewers in the Virtual Information Technology Configuration Control Board application.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management formally notify all Technical Reviewers that default proceeds are no longer allowed and that all Technical Reviewers must review all change requests and either approve, stop, or reject the change request. Policies and procedures outlined in Recommendation 12 or other guidance should be updated to reflect this change to the process.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a quality assurance assessment process for all change requests going through the enterprise-wide Information Technology Configuration Control Board. At a minimum, the quality assurance process should include periodic evaluation of open "stops," reviews to ensure retention of all relevant documentation, and a final check prior to adding change to the baseline to ensure all pertinent process controls occurred at a minimum.

Recommendation 8: OIG recommends that the Bureau of Information Resource Management verify, no later than 30 days after the final issuance of this report, that all Technical Reviewers and Voters that participate in the Information Technology Configuration Control Board process are formally appointed.

Recommendation 9: OIG recommends that the Bureau of Information Resource Management develop and implement a process to formally appoint new Technical Reviewers and Voters who participate in the Information Technology Configuration Control Board process.

Recommendation 10: OIG recommends that the Bureau of Information Resource Management define the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the Information Technology Configuration Control Board process.

Recommendation 11: OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that Technical Reviewers and Voters have formally appointed alternatives.

Recommendation 12: OIG recommends that the Bureau of Information Resource Management develop and implement complete and consistent policies and procedures and supplemental guidance, such as a Submitter's Guide, for the Information Technology Configuration Control Board process. The policies, procedures, and guidance should, at a minimum, include guidance on roles and responsibilities, detailed procedure steps for submitters, minimum testing requirements, instructions on how Technical Reviewers and Voters should conduct their review, the appropriate use of "stops," and established timelines for the process.

Recommendation 13: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically review and validate the accuracy and completeness of the data in the Virtual Information Technology Configuration Control Board database and to correct data integrity, omissions and inaccuracies existing between the new and old databases and when identified going forward. As part of this effort, the Bureau of Information Resource Management should ensure that the old database is available solely as a read-only reference resource and that new data cannot be entered into that database.

Recommendation 14: OIG recommends that the Bureau of Information Resource Management develop and implement required, periodic, training for Information Technology Configuration Control Board management and personnel, Bureau Sponsors, Technical Reviewers, Voters, and change request submitters involved in the Information Technology Configuration Control Board process.

Recommendation 15: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a

request is nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.

Recommendation 16: OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to hold officials accountable for failure to meet established deadlines in the Information Technology Configuration Control Board change request process. Once completed, the policies, procedures, and supplemental guidance discussed in Recommendation 12 should be updated.

Recommendation 17: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers in addition to appropriate bureau officials.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Office of Inspector General (OIG) for the Department of State (Department) initiated this performance audit to determine whether the Department's enterprise-wide Information Technology Configuration Control Board (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. An external audit firm, Kearney & Company, P.C. (Kearney), acting on behalf of OIG, performed this audit.

Kearney conducted fieldwork for this performance audit from December 2016 to May 2017 in the Washington, DC, metropolitan area. The scope of this audit was FY 2016 enterprise-wide ITCCB activity.^{1,2} Kearney conducted this audit in accordance with the Government Accountability Office's, *Government Auditing Standards*, 2011 revision. Those standards require that Kearney plan and perform the audit to obtain sufficient, appropriate audit evidence to provide a reasonable basis for findings and conclusions based on the audit objectives. Kearney believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on audit objectives.

To obtain background information for this audit, Kearney researched and reviewed the National Institute of Standards and Technology's (NIST) publications, the Federal Information Processing Standards, the Department's Foreign Affairs Manual (FAM), the IT CCB Standard Operating Procedures, and the Department's internal IT CCB webpage. Kearney also interviewed IT CCB management and personnel from the Bureau of Information Resource Management (IRM) to gain an understanding of the IT CCB's policies, organization, and framework from which it operates. In addition, Kearney met with officials from the Bureau of Diplomatic Security and the Bureau of Consular Affairs who support the IT CCB change management process through participation as Bureau Sponsors, Technical Reviewers, and Voters.

Kearney used a risk-based approach to review the IT CCB change requests. Kearney identified risks associated with the audit objective to determine if the Department authorized and tested change requests in compliance with FAM and NIST requirements and to determine if the change requests were processed in a timely manner that was consistent with the IT CCB's internal deadlines. Additionally, Kearney identified the controls in place to address those risks. To assess the design and operating effectiveness of these controls, Kearney performed process walkthroughs and obtained relevant supporting documentation for a sample of change requests. Kearney then performed procedures to test and verify that the change requests were authorized and tested in accordance with FAM and NIST requirements and were processed in a timely manner that was consistent with the IT CCB's internal processing deadlines.

¹ The activity included change requests that were initiated, completed, withdrawn, or ongoing in FY 2016.

² As explained in the report itself, Local Configuration Control Boards can approve change requests that affect only local networks. This audit did not review change requests approved by Local Configuration Control Boards.

Kearney also conducted a survey to assess change request submitter's levels of satisfaction with the change request services provided by the IT CCB. Information on the methodology used to develop and distribute the survey is included in the "Detailed Survey Methodology" section of this report.

Work Related to Internal Controls

Kearney performed steps to assess the adequacy of internal controls related to the audit objectives. Kearney gained an understanding of controls relating to the authorization, documentation, and testing of change requests. This included an assessment of centralized controls performed by IRM, as well as controls performed by appointed bureau participants. Kearney tested the implementation of key controls. Weaknesses in internal controls that were identified during the audit are detailed in the "Audit Results" section of this report.

Use of Computer-Processed Data

Kearney used computer-processed data from the Department during this audit. Kearney requested that IT CCB management provide a list of all change requests that contained FY 2016 activity. According to IT CCB management, it manually compiled the list. The IT CCB uses a database to track change requests.³ Using the databases, Kearney generated a similar list of in-scope change requests. Kearney used information from both the old and new databases. To assess the reliability of the data, Kearney compared the FY 2016 change request list provided by IT CCB management to the Kearney-generated list. Kearney found discrepancies between the lists, as noted in the "Population Review" section of this appendix. A test for the completeness of this data could not be accomplished because the IT CCB compiles this list manually and change requests cannot be separately accounted for. Further, Kearney was unable to gain comfort over the completeness of the listing because IT CCB management was unaware of changes that may have bypassed the IT CCB or changes that required IT CCB review but nonetheless were addressed through the Local CCB process. Given Kearney's assessment of the data, including the discrepancies and lack of completeness test, for the purposes of this audit, the Kearney-generated listing was considered sufficiently reliable for sampling.

In addition to using the database to identify change requests subject to sampling, Kearney also used the information in the database to assess the timeliness of change request processing. Specifically, Kearney used the "Review Start Date" and "Decision Date" fields to assess the timeliness of the change request. Kearney used sample documentation and a timeliness report of sampled change requests to confirm the accuracy and reliability of the date fields. Kearney used the IT CCB baseline of approved products in the database to determine whether approved products were consistently added to the baseline. Kearney noted change requests in which the

³ The IT CCB transitioned to a new database in August 2016. IT CCB management stated that data from FY 2012 to FY 2016 were moved to the new database and that the old database was no longer used after August 2016. However, as reported in the Audit Results section of this report, Kearney found that not all data were actually moved and that, in some cases, the old database continued to be used after August 2016. As a result of the discrepancies identified by Kearney and the fact that not all historical information was transferred to the new database, Kearney considered information included in both databases.

date fields were inconsistently used, but did not find evidence to show that the data in the fields, when used, were inaccurate. Issues with the data have been included in Finding A.

Detailed Sampling Methodology

Kearney's sampling objectives were to determine if change requests active in FY 2016 were authorized and tested in compliance with Federal and Department guidelines and processed in a timely manner.

Population Review

To determine the universe of change requests active in FY 2016, Kearney requested that the IT CCB provide a list of all change requests submitted to the IT CCB from October 1, 2015, through September 30, 2016, by network.^{4,5} Table A.1 summarizes the information provided by the IT CCB.

Table A.1: Change Request Data Provided by IT CCB Management

Network	Number of Change Requests
OpenNet ^a	159
ClassNet ^b	62
Other ^c	14
Total Requests	235

^a The Department's unclassified general support system.

^b The Department's classified general support system.

^c Networks that do not meet the OpenNet or ClassNet categorization.

Source: Prepared by Kearney from information provided by IT CCB management.

To validate the reliability of the information provided by IT CCB management and to obtain a population for sampling, Kearney obtained data on change requests that were active during FY 2016 from the IT CCB's databases. Specifically, Kearney obtained a list of all change requests processed by the IT CCB and included on either the old or the new databases (Kearney did not limit the data collection to the scope period). Kearney removed duplicate change requests⁶ and categorized each change request according to the network (OpenNet, ClassNet, or Other). As shown in Table A.2, Kearney identified 2,286 unique change requests that were included in the IT CCB's databases.

⁴ Kearney requested IT CCB management identify whether the change request was for OpenNet, ClassNet, or other network.

⁵ Kearney asked how the list was prepared. IT CCB management stated that it could not provide this information because the individual who prepared the list separated from the Department and did not respond to inquiries from IT CCB management.

⁶ When Kearney combined information from both databases, it identified some items that had the same change request number. Kearney considered these items to be duplicates and removed one of the two items to ensure that the list included only unique change requests.

Table A.2: Change Requests in IT CCB Databases by Network Type

Network	Number of Change Requests in the Old Database	Number of Change Requests in the New Database	Remove Duplicates	Total Number of Change Requests
OpenNet	1,320	2,676	2,449	1,547
ClassNet	646	794	764	676
Other	54	83	86	51
Network not Specified	0	72	60	12
Total Requests	2,020	3,625	3,359	2,286

Source: Prepared by Kearney from analysis of the information included in the new and old IT CCB databases.

Kearney analyzed the 2,286 change requests to determine whether each request was related to the audit scope—that is, active during FY 2016. Kearney considered any change request that was initiated, approved, or withdrawn in FY 2016 to be active, as well as change requests that were initiated in a prior fiscal year but remained open in FY 2016. To make this determination, Kearney primarily used the “Decision Date” and “Review Status” fields in the databases. However, 214 change requests did not contain enough identifying information within the databases to determine whether the request was active during FY 2016. For these 214 items, Kearney required the IT CCB officials to determine the status of the change request. On the basis of documentation provided by the IT CCB, Kearney determined that 60 of the 214 change requests were outside the scope of the audit. The remaining 154 change requests were included in the testing population because they were active during FY 2016. The IT CCB withdrew many of these 154 items from the database after Kearney’s inquiries because the change requests were old and no longer being actively reviewed. However, because these change requests were technically open in the database in FY 2016, Kearney included them in the population subject to sampling. Table A.3 summarizes Kearney’s analysis of information from the two IT CCB databases.

Table A.3: Change Request Scope Analysis

Category Based on Analysis	Total Number of Change Requests
Total number of unique items from the databases	2,286
Less: Change requests completed prior to 10/1/2015	1,726
Less: Change requests withdrawn prior to 10/1/2015	106
Less: Change requests initiated after 9/30/2016	22
Less: Change requests that did not include identifying information in the database that Kearney found were completed prior to 10/1/2015 or initiated after 9/30/2016 per follow-up inquiry*	60
Total Change Requests That Were Active In FY 2016	372

*This line is a subset of the 214 items for which the database fields did not provide sufficient information for Kearney to determine if they were in scope. These items were not included in the prior exclusions that were made on the basis of the information in the database.

Source: Prepared by Kearney from analysis of information in the IT CCB databases.

Table A.4 summarizes the change request sampling population by network.

Table A.4: Change Request Sampling Population by Network

Network	Change Requests That Were Active in FY 2016
OpenNet	263
ClassNet	89
Other	20
Total	372

Source: Prepared by Kearney from information provided by the IT CCB management and an analysis of information in the IT CCB databases.

Kearney compared the population it created using the IT CCB databases with the list provided by IT CCB officials. The list provided by IT CCB included 235 items, and Kearney's list included 372 items. Upon review, Kearney determined that the IT CCB list did not include change requests that were initiated in a prior fiscal year but that were still open in FY 2016. Additionally, the IT CCB's list did not include change requests that were withdrawn during FY 2016.

Kearney also identified nine change requests included in the IT CCB list that were not included in the list Kearney developed using the IT CCB databases. IT CCB officials could not explain why the nine change requests were in the databases but could not be seen by Kearney using Kearney's access information. IT CCB officials could see the data when they logged into the databases. Kearney included these nine items in the population sampling list.

Sample Design

The population of IT CCB change requests subject to sampling is 381. Kearney grouped all change requests in the final population by the status of the request. Kearney categorized 381 change requests into 5 sampling categories further broken down by OpenNet, ClassNet, and Other Network change requests. The categorization established the change requests status as of FY 2016. Table A.5 summarizes the number of change requests by request status and network.

Table A.5: Sampling Category Population Breakdown by Network

Request Status	OpenNet Change Requests	ClassNet Change Requests	Other Network Change Requests	Total Change Requests
Requests with a High-Risk Status*	1	0	0	1
Requests that were initiated in FY 2016	23	19	5	47
Requests that were completed in FY 2016	208	49	12	269
Requests that were withdrawn in FY 2016	16	6	1	23
Requests initiated prior to FY 2016 and not completed or withdrawn as of 9/30/2016	21	18	2	41
Total	269	92	20	381

* The review status for this request indicated that the requested change was made but the actual change request was never approved; therefore, Kearney considered it high-risk.

Source: Prepared by Kearney from information provided by the IT CCB and information in IT CCB databases.

Kearney determined that a non-statistical sample size of 78 change requests was appropriate on the basis of industry guidance for control testing.⁷ Kearney chose to select a sample of 78 change requests. To gain adequate coverage over all request statuses and networks, Kearney allocated the sample size across each of the categories. First, Kearney allocated 3 samples to each category for a total of 34 samples.⁸ Kearney then weighted each category and allocated the remaining 44 samples on the basis of the weight of each category. The weighted average was calculated by taking the number of change requests in each category and network and dividing it by the total number of change requests in the remaining population subject to sampling. Once the sample size for each category was determined, Kearney selected a random sample using IDEA® sampling software. Table A.6 provides details of the samples selected by category and network.

⁷ American Institute of Certified Public Accountants Audit Guide, "Audit Sampling," (2017).

⁸ If fewer than three items existed for a category, all the items for that category were selected.

Table A.6: Sample Selection

Sampling Category	OpenNet Change Requests	ClassNet Change Requests	Other Network Change Requests	Total Change Requests
Requests with a High-Risk Status	1	0	0	1
Requests initiated in FY 2016	6	5	3	14
Requests completed in FY 2016	29	9	4	42
Requests withdrawn in FY 2016	5	3	1	9
Requests initiated prior to FY 2016 and not completed or withdrawn in FY 2016	5	5	2	12
Total Change Requests Sampled	46	22	10	78

Source: Prepared by Kearney from information provided by IT CCB management and information on the IT CCB website.

Detailed Survey Methodology

Kearney initiated a customer satisfaction survey. The primary objective of the survey was to obtain change request submitters' opinions regarding the services the IT CCB provided. The survey consisted of 27 questions related to customer satisfaction. Appendix B includes survey questions and results.

Identification of Change Request Submitters and Distribution

For the 381 change requests identified as having FY 2016 activity, Kearney reviewed the information in the old and new IT CCB databases to identify the change request submitter. One hundred forty-nine individuals submitted the 381 change requests. Kearney emailed the questionnaire with instructions for completion to the 149 change request submitters. In two instances, Kearney received an error message indicating that the submitters were no longer employees of the Department.

Survey Results

Kearney obtained responses to the survey from 49 individuals. Kearney requested that survey respondents provide their email address in question 1. Kearney used this information to validate that only those sent the survey responded. Kearney noted that one individual who was not a change request submitter responded to the survey. This response was excluded from the analysis of the survey results. The survey was also set up in a manner that prevented individuals from responding more than once. Kearney analyzed 48 completed surveys. These 48 responses, of 147 surveys successfully sent, represent a 33-percent response rate. The survey questions and results are presented in Appendix B.

APPENDIX B: SUMMARY OF RESPONSES TO A CUSTOMER SURVEY

To obtain change request submitters' opinions regarding the services provided by the Information Technology Configuration Control Board (IT CCB), Kearney & Company, P.C., surveyed 147 individuals who had change requests active in FY 2016 to determine their satisfaction with the process. In total, 48 responses were received, which is a 33-percent response rate.¹ Information on the number (and percentage) of respondents is provided for each question.² Questions requiring a narrative response are included, but the responses to these questions are not provided.

Survey Questions and Responses

1. Please enter your Department of State email address. This information will be used to confirm that only those contacted are completing the survey. **(Answered: 48)**
2. Are you a system owner?
 - a) **[(20) 42%]** Yes
 - b) **[(28) 58%]** No

If not, please provide the name and title of the individual who requested you to submit a change request to the Enterprise-wide IT CCB.

Of the 28 respondents who answered "no," 16 respondents provided contact information for another Department official.

3. Please indicate how many change requests you submitted through the Enterprise-wide IT CCB change management process in FY 2016 for each request status. *(Please select one answer for each change request status).* **(Answered: 48)**

¹ Appendix A: Purpose, Scope, and Methodology provides additional details on the survey process.

² The number of respondents may be different for each question, because not all people surveyed provided a response for each question. Percentages may not total 100 percent due to rounding.

Table B.1: Responses to Survey Question 3

Type	None	One	Two	Three	Four	More than Four
Routine	(6) 13%	(13) 27%	(8) 17%	(3) 6%	(1) 2%	(17) 35%
Expedited	(37) 77%	(7) 15%	(2) 4%	(0) 0%	(0) 0%	(2) 4%
Emergency	(45) 94%	(1) 2%	(0) 0%	(0) 0%	(1) 2%	(1) 2%

Source: Prepared by Kearney from survey responses.

4. When was your most recent change request submitted? *(Estimate date as needed)*
(Answered: 48)

Table B.2: Responses to Survey Question 4

Date	Number (Percent) of Submissions*
Before 2016	5 (10%)
1/1/2016 – 3/31/2016	7 (15%)
4/1/2016 – 6/30/2016	8 (17%)
7/1/2016 – 9/30/2016	6 (13%)
10/1/2016 – 12/31/2016	4 (8%)
2017	18 (38%)

*Sum of percentages does not foot to 100% due to rounding.

Source: Prepared by Kearney from survey responses.

5. Did you obtain guidance for submitting a change request on the IT CCB website?
(Answered: 48)
- a) [(31) 65%] Yes
b) [(17) 35%] No
6. Other than the IT CCB website, where did you obtain guidance for submitting a change request to the Enterprise-wide IT CCB? (Answered: 16, Skipped: 32)
- Sixteen respondents indicated that they used guidance outside the IT CCB website. For example, respondents reported that they used guidance from their own personal experience or self-training, colleagues who had previously used the IT CCB process, or other control boards, such as the Local Configuration Control Boards.
7. Generally, the guidance provided on the IT CCB website regarding the IT CCB change management process is clear. (Answered: 46, Skipped: 2)

- a) [(3) 7%] Strongly Agree
- b) [(16) 35%] Agree
- c) [(11) 24%] Neither Agree nor Disagree
- d) [(10) 22%] Disagree
- e) [(6) 13%] Strongly Disagree

*Sum of percentages does not total 100% due to rounding.

8. Generally, the instructions provided on the IT CCB website for completing the IT CCB change request questionnaire are clear. **(Answered: 43, Skipped: 5)**

- a) [(3) 7%] Strongly Agree
- b) [(16) 37%] Agree
- c) [(13) 30%] Neither Agree nor Disagree
- d) [(9) 21%] Disagree
- e) [(2) 5%] Strongly Disagree

9. Overall, I am satisfied with the virtual forms provided on the IT CCB website, such as the questionnaire and change request form. **(Answered: 43, Skipped: 5)**

- a) [(5) 12%] Strongly Agree
- b) [(12) 28%] Agree
- c) [(12) 28%] Neither Agree nor Disagree
- d) [(5) 12%] Disagree
- e) [(9) 21%] Strongly Disagree

*Sum of percentages does not total 100% due to rounding.

10. The guidance provided on the IT CCB website assisted me in submitting IT CCB change request questionnaire(s). **(Answered: 43, Skipped: 5)**

- a) [(4) 9%] Strongly Agree
- b) [(15) 35%] Agree
- c) [(16) 37%] Neither Agree nor Disagree
- d) [(3) 7%] Disagree
- e) [(5) 12%] Strongly Disagree

11. Please provide information on what steps or guidance included in the IT CCB website could be improved. **(Answered: 43, Skipped: 5)**

12. Did you submit your change request(s) to the Enterprise-wide ITCCB using the Virtual IT CCB Database application? **(Answered: 43, Skipped: 5)**

- a) [(33) 77%] Yes
- b) [(10) 23%] No

13. Other than the Virtual IT CCB Database application, how did you submit a change request(s) to the Enterprise-wide IT CCB? **(Answered: 10, Skipped: 38)**

The 10 respondents indicated that they had submitted requests through the IT CCB website or through their local IT CCB.

14. Generally, the process for submitting a change request(s) to the enterprise-wide IT CCB via the Virtual IT CCB Database is easy. **(Answered: 43, Skipped: 5)**

- a) **[(4) 9%]** Strongly Agree
- b) **[(14) 33%]** Agree
- c) **[(13) 30%]** Neither Agree nor Disagree
- d) **[(6) 14%]** Disagree
- e) **[(6) 14%]** Strongly Disagree

15. Generally, the Virtual IT CCB Database contained up-to-date information on the status of my change requests. **(Answered: 38, Skipped: 10)**

- a) **[(6) 16%]** Strongly Agree
- b) **[(15) 39%]** Agree
- c) **[(14) 37%]** Neither Agree nor Disagree
- d) **[(2) 5%]** Disagree
- e) **[(1) 3%]** Strongly Disagree

16. The Virtual IT CCB Database met my needs as a change request submitter. **(Answered: 38, Skipped: 10)**

- a) **[(5) 13%]** Strongly Agree
- b) **[(13) 34%]** Agree
- c) **[(12) 32%]** Neither Agree nor Disagree
- d) **[(4) 11%]** Disagree
- e) **[(4) 11%]** Strongly Disagree

*Sum of percentages does not total 100% due to rounding.

17. Please provide information on how the Virtual IT CCB Database application (used to submit change requests) could be improved. **(Answered: 38, Skipped: 10)**

18. Please indicate your general level of satisfaction or dissatisfaction with each of the following: **(Answered: 38, Skipped: 10)**

Table B.3: Responses to Survey Question 18

Category	Very Satisfied	Satisfied	Neither Satisfied nor Dissatisfied	Dissatisfied	Very Dissatisfied	Not Applicable (I do not have experience with this item)
Enterprise-Wide IT CCB change management	(4) 11%	(16) 42%	(10) 26%	(5) 13%	(3) 8%	(0) 0%
Enterprise-wide IT CCB website*	(4) 11%	(14) 37%	(11) 29%	(6) 16%	(3) 8%	(0) 0%
Virtual IT CCB Database	(4) 11%	(16) 42%	(10) 26%	(5) 13%	(3) 8%	(0) 0%

*Sum of percentages for the category does not total to 100% due to rounding.

Source: Prepared by Kearney from survey responses.

19. Overall, please indicate your level of satisfaction or dissatisfaction with your interactions with the following groups during the Enterprise-wide IT CCB change management process. (Answered: 38, Skipped: 10)

Table B.4: Responses to Survey Question 19

Category	Very Satisfied	Satisfied	Neither Satisfied nor Dissatisfied	Dissatisfied	Very Dissatisfied	Not Applicable (I do not have experience with this item)
Bureau Sponsor(s)*	(8) 20%	(14) 37%	(11) 29%	(2) 5%	(0) 0%	(3) 8%
Technical Reviewer(s)*	(2) 5%	(17) 45%	(5) 13%	(8) 20%	(3) 8%	(3) 8%
IT CCB Voting Representatives (Final Approvers)*	(3) 8%	(16) 42%	(10) 26%	(5) 13%	(1) 3%	(3) 8%
IT CCB Management*	(5) 13%	(17) 45%	(8) 20%	(3) 8%	(3) 8%	(2) 5%

*Sum of percentages for the category does not total to 100% due to rounding.

Source: Prepared by Kearney from survey responses

20. Overall, please indicate your level of satisfaction or dissatisfaction with the timeliness of services provided by the following groups during the Enterprise-wide IT CCB change management process. (Answered: 38, Skipped: 10)

Table B.5: Responses to Survey Question 20

Category	Very Satisfied	Satisfied	Neither Satisfied nor Dissatisfied	Dissatisfied	Very Dissatisfied	Not Applicable (I do not have experience with this item)
Bureau Sponsor(s)	(7) 18%	(14) 37%	(9) 24%	(5) 13%	(0) 0%	(3) 8%
Technical Reviewer(s)	(4) 11%	(14) 37%	(6) 16%	(8) 20%	(3) 8%	(3) 8%
IT CCB Voting Representatives (Final Approvers)*	(2) 5%	(18) 47%	(10) 26%	(3) 8%	(2) 5%	(3) 8%
IT CCB Management	(7) 18%	(14) 37%	(9) 24%	(2) 5%	(3) 8%	(3) 8%

*Sum of percentages for the category does not total to 100% due to rounding.

Source: Prepared by Kearney from survey responses.

21. While processing your most recent change request, did any of the following groups request information or supporting documentation regarding your request that was not originally required in the change request submission? **(Answered: 38, Skipped: 10)**

Table B.6: Responses to Survey Question 21

Category	Yes	No
Bureau Sponsor(s)	(10) 26%	(28) 74%
Technical Reviewer(s)	(20) 53%	(18) 47%
IT CCB Voting Representatives (Final Approvers)	(8) 20%	(30) 80%

Source: Prepared by Kearney from survey responses.

22. Please describe what additional information reviewers requested that was not originally required in the change request submission. If none was requested, please note N/A. **(Answered: 38, Skipped: 10)**

Generally, respondents indicated that Bureau Sponsors and Technical Reviewers requested additional information or clarification outside the required documentation, such as change control testing results.

23. How many of your change requests were stopped during the technical review phase in FY 2016? **(Answered: 38, Skipped: 10)**

- a) **[(16) 42%]** None
- b) **[(7) 18%]** One

- c) [(2) 5%] Two
- d) [(1) 3%] Three
- e) [(3) 8%] Four
- f) [(9) 24%] More than Four

24. Were any change requests stopped without an explanation of why the request was stopped? **(Answered: 22, Skipped: 26)**

- a) [(3) 14%] Yes
- b) [(19) 86%] No

25. If any change requests were stopped without an explanation, please provide information on the situation and the feedback received regarding the stoppage. If none, please note N/A. **(Answered: 22, Skipped: 26)**

26. For your most recent stopped change request, did IT CCB Management facilitate the resolution of the stoppage between you, the change request submitter, and the Technical Reviewer(s)? **(Answered: 22, Skipped: 26)**

- a) [(9) 41%] Yes
- b) [(13) 59%] No

27. Please provide any additional comments concerning the Department's Enterprise-wide IT CCB IT change management process, including any information that you think is important or pertinent given the context of this survey. *(If you choose to respond, please type in the box provided, which will expand to accommodate the size of your response.)* **(Answered: 38, Skipped: 10)**

APPENDIX C: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE




UNCLASSIFIED

United States Department of State

Washington, D.C. 20520

September 15, 2017

TO: OIG/AUD – Norman P. Brown
FROM: IRM/PDCIO – Karen E. Munnaw, Acting 
SUBJECT: Draft Report - Audit of the Department of State's Information
Technology Configuration Control Board

Attached is the Bureau of Information Resource Management's response to the Draft Report on the Audit of the Department of State's Information Technology Configuration Control Board, Recommendations 1-17.

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

Attachment

Audit of the Department of State's Information Technology
Configuration Control Board (ITCCB)
AUD-IT-17-XX

Recommendation 1: OIG recommends that the Bureau of Information Resource Management develop and implement a detailed program plan for the Information Technology Configuration Control Board process that includes clear goals and attainable objectives and defines areas of authority and responsibility.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management develop and implement a process to establish and periodically update a list of system, product, or software owners who will be authorized to make change requests for their system, product, or software. The list should be made available to users and members of the Information Technology Configuration Control Board through the Information Technology Configuration Control Board website or applicable policies and procedures outlined in Recommendation 12.

Management Response (September 2017): IRM concurs with the recommendation. During the exit interview the audit team clarified the recommendation. It is in reference to versioning control of baselined products.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management determine what documentation is needed to support a change request and modify the policies and procedures outlined in Recommendation 12 or other guidance, such as the submitters guide, provided to change request submitters to reflect the documentation that is required for a complete and accurate change request submission.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement guidance for change requests to require and include: (a) minimum testing standards for change requests, (b) instructions that testing be performed in advance of the change request being submitted and that the testing documentation be submitted as part of the change request process, and (c) a clearly defined technical review of the testing documentation that is submitted to verify the documentation complies with minimum standards.

Management Response (September 2017): IRM concurs with the recommendation.

UNCLASSIFIED

UNCLASSIFIED

Audit of the Department of State's Information Technology
Configuration Control Board (ITCCB)
AUD-IT-17-XX

Recommendation 5: OIG recommends that the Bureau of Information Resource Management remove the default proceed ability for Technical Reviewers in the Virtual Information Technology Configuration Control Board application.

Management Response (September 2017): IRM does not concur with this recommendation. The impact of the OIG recommendation would be a decrease in ITCCB efficiency. This runs counter to the OIG recommendations concerning timeliness, feedback from the Secretary's recently accomplished listening tour, and emergent guidance from the OMB concerning the need to appropriately balance business need and IT risk management. In practice, a "default proceed" means a technical reviewer utilized the maximum allotted time and found no reason to stop the submission. Technical reviewers are equally responsible for their review, regardless if it is a "default" or "explicit" proceed. The net impact of this recommendation, removing the "default proceed", will be the transformation of the "default proceed" into the only available alternative, a "default stop". This contradicts the recommendations to improve timeliness. Further, our analysis of the historical data does not identify the "default proceed" as a root cause of ITCCB inefficiency and the assertions that underpin this recommendation appear to be a hypothetical as opposed to an actually observed challenge. Significant historical precedents and customer feedback support the OIG's recommendation to improve timeliness.

Recommendation 6: OIG recommends that the Bureau of Information Resource Management formally notify all Technical Reviewers that default proceeds are no longer allowed and that all Technical Reviewers must review all change requests and either approve, stop, or reject the change request. Policies and procedures outlined in Recommendation 12 or other guidance should be updated to reflect this change to the process.

Management Response (September 2017): IRM does not concur: the impact of the OIG recommendation would be a decrease in ITCCB efficiency. This runs counter to the OIG recommendations concerning timeliness, feedback from the Secretary's recently accomplished listening tour, and emergent guidance from the OMB concerning the need to appropriately balance business need and IT risk management. In practice, a "default proceed" means a technical reviewer utilized the maximum allotted time and found no reason to stop the submission. Technical reviewers are equally responsible for their review, regardless if it is a "default" or "explicit" proceed. The net impact of this recommendation, removing the "default proceed," will be the transformation of the "default proceed" into the only available alternative, a "default stop." This contradicts the recommendations to improve timeliness. Further, our analysis of the historical data does not identify the "default proceed" as a root cause of ITCCB inefficiency and the assertions that underpin this recommendation appear to be a hypothetical as opposed to an actually observed challenge. Significant historical precedents and customer feedback support the OIG's recommendation to improve timeliness.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a quality assurance assessment process for all change requests going through the enterprise-wide Information Technology Configuration Control Board. At a minimum, the quality assurance process should include periodic evaluation of open "stops," reviews to ensure retention of all relevant documentation, and a final check prior to adding change to the baseline to ensure all pertinent process controls occurred at a minimum.

Management Response (September 2017): IRM concurs with the recommendation.

UNCLASSIFIED

UNCLASSIFIED

Audit of the Department of State's Information Technology
Configuration Control Board (ITCCB)
AUD-IT-17-XX

Recommendation 8: OIG recommends that the Bureau of Information Resource Management verify, no later than 30 days after the final issuance of this report, that all Technical Reviewers and Voters that participate in the Information Technology Configuration Control Board process are formally appointed.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 9: OIG recommends that the Bureau of Information Resource Management develop and implement a process to formally appoint new Technical Reviewers and Voters who participate in the Information Technology Configuration Control Board process.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 10: OIG recommends that the Bureau of Information Resource Management define the roles, responsibilities, and technical skillsets for each technical review and voting area and develop and implement a vetting process to verify Technical Reviewers and Voters have the knowledge, skills, and abilities to perform their assigned duties related to the Information Technology Configuration Control Board process.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 11: OIG recommends that the Bureau of Information Resource Management develop and implement a process to verify that Technical Reviewers and Voters have formally appointed alternatives.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 12: OIG recommends that the Bureau of Information Resource Management develop and implement complete and consistent policies and procedures and supplemental guidance, such as a Submitter's Guide, for the Information Technology Configuration Control Board process. The policies, procedures, and guidance should, at a minimum, include guidance on roles and responsibilities, detailed procedure steps for submitters, minimum testing requirements, instructions on how Technical Reviewers and Voters should conduct their review, the appropriate use of "stops," and established timelines for the process.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 13: OIG recommends that the Bureau of Information Resource Management develop and implement a process to periodically review and validate the accuracy and completeness of the data in the Virtual Information Technology Configuration Control Board database and to correct data integrity, omissions and inaccuracies existing between the new and old databases and when identified going forward. As part of this effort, the Bureau of Information Resource Management should ensure that the old database is available solely as a read-only reference resource and that new data cannot be entered into that database.

Management Response (September 2017): IRM concurs with the recommendation.

UNCLASSIFIED

UNCLASSIFIED

Audit of the Department of State's Information Technology
Configuration Control Board (ITCCB)
AUD-IT-17-XX

Recommendation 14: OIG recommends that the Bureau of Information Resource Management develop and implement required, periodic, training for Information Technology Configuration Control Board management and personnel, Bureau Sponsors, Technical Reviewers, Voters, and change request submitters involved in the Information Technology Configuration Control Board process.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 15: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to (a) monitor the status of all change requests throughout each stage of the change request process and (b) notify stakeholders when a request is nearing the end of a deadline or when an event occurs that may affect the deadline for a change request.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 16: OIG recommends that the Bureau of Information Resource Management develop and implement policies and procedures to hold officials accountable for failure to meet established deadlines in the Information Technology Configuration Control Board change request process. Once completed, the policies, procedures, and supplemental guidance discussed in Recommendation 12 should be updated.

Management Response (September 2017): IRM concurs with the recommendation.

Recommendation 17: OIG recommends that the Bureau of Information Resource Management develop and implement a formal process to periodically gather, assess, and report on its change request review process timeliness metrics and to make those results available to its stakeholders and customers in addition to appropriate bureau officials.

Management Response (September 2017): IRM concurs with the recommendation.

UNCLASSIFIED

ABBREVIATIONS

CIO	Chief Information Officer
ENM	Enterprise Network Management Office
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
IRM	Bureau of Information Resource Management
IT CCB	Information Technology Configuration Control Board
NIST	National Institute of Standards and Technology
VITCCB	Virtual Information Technology Configuration Control Board Application
VPAT	Voluntary Product Accessibility Template

UNCLASSIFIED



HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926

[OIG.state.gov/HOTLINE](https://oig.state.gov/HOTLINE)

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
OIGWPEAOmbuds@state.gov

oig.state.gov

Office of Inspector General • U.S. Department of State • P.O. Box 9778 • Arlington, VA 22219

UNCLASSIFIED