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

Summary of FY 2004 Information Systems Security Issues

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

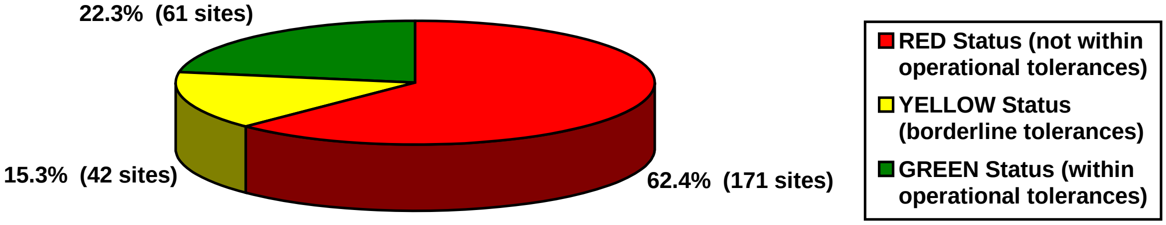
The inspections of FY 2004 uncovered systems security issues that cross regional and bureau boundaries, allowing OIG to suggest several areas for improvement Department-wide. The Information System Security Officer (ISSO) program is struggling at several posts. Patch management procedures and other essential emergency planning and recovery documentation are missing or inadequate. Several local change control boards (CCB) at posts are noncompliant with Department regulations. At the root of these and other problems, management's guidance and oversight of IT security practices needs improvement.

OIG found that the ISSO program is struggling to reach its full potential at many locations. Roughly a third of the inspections conducted by the OIG reported shortcomings in the ISSO program. Deficiencies in the ISSO program were generally in two areas: (1) a lack of trained information systems security personnel, and (2) insufficient prioritization, guidance, oversight and accountability from senior and middle management.

Recent statistics from the Enterprise Network Management Office's patch bulletin website indicate a majority of posts are not installing patches, thus leaving Department systems vulnerable, as shown in figure 1.

The fieldwork for this report was conducted by the Office of Information Technology Audits in FY 2004. This is an unclassified summary of a full inspection report, which receives limited official distribution.

Figure 1: Patch Management at 274 Department Sites



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

Documenting procedures is a vital step in proper information systems management. Often, having a recovery plan in place can reduce downtime from days to hours or less in the event of a system failure. Documentation is also necessary for budgeting and staffing reasons. Key documents include, but are not limited to, the following: contingency plans; information systems security plans; and IT budget plans. During its inspection, OIG found many of the required post-specific documents were either incomplete or nonexistent. Overall, nearly half of the inspections uncovered problems within documentation.

The local CCB provides a forum for IT staff and regional security officers to discuss whether or not to allow new software or hardware onto the post's IT systems. Posts are required to inform the Department regularly of their CCB decisions. Though most posts have a local CCB, OIG found many were not fully cognizant of their role.

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

Office of Inspector General

The Office of Inspector General's (OIG) mission is to assess Department of State and Broadcasting Board of Governors (BBG) operations and recommend ways to strengthen their integrity, effectiveness, and accountability. OIG's Office of Information Technology provides systematic and independent evaluations of the information management and information security operations of the Department of State, its posts abroad and the BBG.

March 29, 2005