however, are not required to communicate information security risks to IRM. In 2015, OIG recommended that the Department review the organizational placement of the CIO to address this decentralized risk-reporting structure.[108] The Department acknowledged the need for enhancements to information security across the Department, but it determined that the CIO's position within IRM was sufficient to implement an effective agency-wide information security program. The Department stated that it had instead made efforts to improve the effectiveness of its information security program by drafting a new approach to managing information system-level security risks. As a result, the CIO is still not organizationally placed to address information security program issues effectively.

A recent report illustrates the flaws in this organizational structure. In particular, OIG reported that insufficient program management was one reason that the Department did not authorize or test IT change requests in accordance with Department and Federal policies. The report explained that, although IRM is responsible for ensuring control over change requests, the CIO, who is located within IRM, does not have sufficient authority to manage activities of the Information Technology Configuration Control Board, as provided for in law. This relative lack of authority increases the need for a strong, centralized, oversight function within IRM 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 Office of Management and Budget requirements. The Department, however, has not established and implemented such an oversight function to allow IRM to perform this role appropriately under the current organizational structure. To the contrary, IRM management stated that IRM's role was to facilitate the change request process rather than to act as a program manager for the process.[109]

Conclusion

Each of the management challenges described in this report has an effect on the Department's ability to perform its mission and to safeguard taxpayer resources while doing so. As such, each challenge independently warrants ongoing attention.

OIG notes as well the unique vulnerabilities that emerge when these challenges interact with one another. They do not exist in isolation; rather, many overlap with and exacerbate one another. For example, operating in contingency and critical environments amplifies the Department's weaknesses in managing contracts and grants. The already challenging task of overseeing and monitoring a complex foreign assistance program becomes even more challenging when the Department cannot put oversight staff on the ground where a particular program is being implemented. An additional example pertains to information security, where weaknesses can have a broad effect on the Department and worsen challenges such as financial management. In particular, IT security weaknesses can affect the integrity of financial applications, which, in turn, increases risks that sensitive financial information could be accessed by unauthorized individuals, that financial transactions could be accidentally or intentionally altered, or, more basically, that the Department will be unable to report financial data accurately. OIG accordingly encourages the Department to consider the ways that these challenges compound each other and how it can address these problems systematically rather than in a piecemeal fashion.

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926

OIG.state.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Ombudsman
to learn more about your rights:

WPEAOmbuds@stateoig.gov

[108] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-16-16, November 2015).

[109] AUD-IT-17-64, September 2017.