These deficiencies manifested themselves in various ways, and OIG found concerns in both domestic and overseas operations. For example, OIG detailed ongoing difficulties in monitoring and overseeing the antiterrorism assistance program in Pakistan. In particular, OIG reported that DS had no staff in Pakistan responsible for verifying satisfactory contractor performance or monitoring whether required reports were submitted. Furthermore, the bureau had not adopted a meaningful way to measure progress toward program goals.[47] In another example, an audit of a contract for monitoring services in Iraq reported that the Department did not adequately monitor funds available under contract line item numbers.[48] OIG's inspection reports also highlighted posts where Contracting Officers Representatives served without proper training or without proper designation, which could affect their ability to ensure proper oversight of contractors.[49] Domestically, OIG reported that CA's Office of Consular Systems and Technology contract files did not have all required documentation and that contractor monthly status reports were missing for each contract reviewed.[50]

OIG acknowledges that conditions on the ground can have significant effect on the Department's ability to perform oversight. For example, OIG found that difficulty in obtaining visas from the Government of Pakistan was a contributing factor in the Department's flawed oversight and monitoring of the antiterrorism assistance program there.[51] Even in such situations, however, OIG identified specific, practical actions the Department could take to improve oversight, including developing and implementing procedures to verify compliance with contract reporting requirements. In other situations, Department bureaus responsible for administering contracts and foreign assistance should better ensure compliance with contract reporting requirements and should develop and implement monitoring and evaluation systems that measure contractor performance.

3 Information Security and Management

Like all large organizations, the Department depends on information systems and electronic data to carry out its mission. The security of these systems and networks—cybersecurity—is vital to protecting national and economic security, public safety, and the flow of commerce. These same information systems, however, are subject to serious threats, including exploitation and compromise of the information being processed, stored, and transmitted. These threats, in turn, can harm the Department's operations and assets. As described below, OIG's reports have emphasized a number of these risks. OIG also notes that, as discussed in the separate section addressing coordination and the need for clear lines of authority, these issues are affected by the organizational placement of the Chief Information Officer (CIO).

Strengthening Cybersecurity Practices

Overall, during FY 2017, OIG reported that the Department did not have an effective information security program guided by risk-based decision-making, as evidenced by security weaknesses in key IT metrics, including risk management, configuration management, identity and access management, continuous monitoring, incident response, and contingency planning.[52] OIG FY 2017 reports identified various areas where the Department could strengthen its cybersecurity performance. These include Information Systems Security Officer duties, the cybersecurity assessment process, the configuration change control process, and IT contingency planning.

Information Systems Security Officers (ISSO) are responsible for implementing the Department's information systems security program and for working closely with system

[47] OIG, *Management Assistance Report: Challenges Remain in Monitoring and Overseeing Antiterrorism Assistance Program Activities in Pakistan* (AUD-MERO-17-37, May 2017).

[48] AUD-MERO-17-41, May 2017.

[49] *See, e.g.*, ISP-I-17-07A, January 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[50] AUD-CGI-17-38, May 2017.

[51] AUD-MERO-17-37, May 2017.

[52] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-17-17, November 2016).