7 Promoting Accountability Through Internal Coordination and Clear Lines of Authority

Promoting accountability through careful, internal coordination and clear, well-defined lines of authority is crucial. OIG, however, has identified program management weaknesses associated with a lack of coordination and dispersed authority as a serious challenge facing the Department. This is a concern that is reflected in a wide range of OIG's reports. OIG has included this as a management challenge because of its significant implications for the Department's ability to implement its programs and operate efficiently and effectively. Moreover, as described below, unclear lines of authority and a lack of coordination have particular consequences for both physical and IT security.

OIG acknowledges that, in some areas, the Department has made efforts to address these concerns. To take just one example, OIG's inspection of NEA discussed the ways that the bureau worked across "complex lines of authority" to address a range of crises in its area of operations and noted that it complied with Department guidance requiring it to serve "as the single focus of responsibility for leadership and coordination" of government activities in "its area of assignment." In the same report, OIG highlighted the effective coordination work of two NEA offices—the Office of Iranian Affairs and the Office of Maghreb Affairs. OIG, however, identified other areas where coordination was not effective, noting, for example, that NEA did not fully engage with the Bureau of Conflict and Stabilization Operations, although the two bureaus had overlapping responsibilities in some areas.[103]

Moreover, in other specific program areas, challenges regarding coordination and clear lines of authority persisted. For example, OIG identified ineffective administration of the armored vehicle program that resulted, in part, from a lack of documentation and understanding regarding the relative roles of DS and the Bureau of Administration.[104] Confusion over its role in the program contributed to DS's failure sufficiently to oversee the program and strategically plan the allocation of armored vehicles at overseas posts.

Another area of concern is the lack of coordination between OBO and DS, both of which have responsibilities for physical security of diplomatic facilities. Although OBO and DS collaborate on a number of working groups, OIG has long pointed out the implications of this overall lack of coordination and encourages complete implementation of its recommendation for these bureaus to work together to develop formal, standardized processes to prioritize physical security-related deficiencies at posts by category.[105] One recent example of the consequences of a lack of coordination concerns a gap OIG identified in the security certification process. In particular, OIG found that the improper alterations on security doors were overlooked, in part, because the security certification process did not include a follow-up inspection by DS to confirm that OBO's actions to address identified physical security deficiencies were in accordance with physical security standards.[106]

OIG has also identified concerns regarding overlapping and poorly defined information security responsibilities between DS and IRM.[107] The Federal Information Technology Acquisition Reform Act enhanced the CIO's authority and responsibility for the implementation of an agency's information security program. According to Department policies, however, both IRM and DS have responsibilities for information security, even though the Department's CIO, who is the head of IRM, should have this role. Furthermore, the Department's current organizational risk-reporting structure requires the CIO and DS separately to report to the Under Secretary for Management; DS and other bureaus or offices reporting to the Under Secretary for Management,

[103] *Ibid*.

[104] AUD-SI-17-21, February 2017.

[105] OIG, *Compliance Follow-up Audit of the Process To Request and Prioritize Physical Security-Related Activities at Overseas Posts* (AUD-ACF-16-20, December 2015); OIG, *Management Assistance Report: Department Attention Needed to Address Overdue Responses on Selected Open Recommendations* (AUD-ACF-17-55, July 2017).

[106] AUD-MERO-17-28, March 2017.

[107] *See, e.g.*, OIG, *Audit of the Department of State's Efforts to Detect and Address the Use of Unapproved Portable Devices* (AUD-IT-17-61, September 2017) and AUD-IT-17-17, November 2016.