Congress of the United States
U.S. House of Representatives
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515–0315

Memorandum

To:	Members, Committee on Small Business
From:	Committee Staff
Date:	July 10, 2017
Re:	Hearing: "Help or Hindrance? A Review of SBA's Office of the Chief Information Officer"

On Wednesday, July 12, 2017 at 11:00 a.m., the Committee on Small Business will meet in Room 2360 of the Rayburn House Office Building for the purpose of examining whether the Small Business Administration's Office of the Chief Information Officer is operating efficiently and effectively.

I. The Office of the Chief Information Officer is Subject to Several Laws

The Small Business Administration (SBA) established the Office of the Chief Information Officer (OCIO) on December 1, 1998.[1] According to SBA, the OCIO's mission "is to foster an environment in which information and technology are used to support and enhance business decisions and Agency operations."[2] Congress has acted several times over the past few years to improve information technology (IT) investments and protect IT security systems across the federal government. These are some of the more significant laws to which the SBA's OCIO is subject.

A. Clinger-Cohen Act

Partially in response to the Clinger-Cohen Act passed in 1996, SBA created the OCIO.[3] The Clinger-Cohen Act required an agency's Chief Information Officer (CIO) to oversee IT investments for the agency and advise the head of the agency on those investments.[4] According

[1] U.S. Small Bus. Admin., About the Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio/about-us (last visited July 6, 2017).
[2] U.S. Small Bus. Admin., Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio (last visited June 28, 2017).
[3] The Small Business Administration created the Office of the Chief Information Officer on December 1, 1998. U.S. Small Bus. Admin., About the Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio/about-us (last visited July 6, 2017).
[4] Clinger-Cohen Act of 1996, §5125(b) and (c). The law requires, in part, the CIO to "monitor the performance of information technology programs of the agency, evaluate the performance of those programs on the basis of the applicable performance measurements and advise the head of the agency regarding whether to continue, modify, or terminate a program or project." §5125(c)(2).

to SBA, its CIO is "responsible for strategic execution and management of Agency-wide functions" related to IT as prescribed by the Clinger-Cohen Act.[5] The CIO also chairs the Business Technology Investment Council—composed of senior SBA officials—which acts as SBA's IT investment review body and corporate advisory board for SBA's IT investment portfolio.[6]

B. Federal Information Technology Acquisition Reform Act (FITARA)

Congress passed the Federal Information Technology Acquisition Reform Act (FITARA) on December 19, 2014 to reform how federal agencies purchase and manage IT assets.[7] According to the Government Accountability Office (GAO), the federal government will spend approximately $89 billion on IT investments in FY 2017.[8] Historically, the projects supported by these IT investments have incurred "multi-million dollar cost overruns and years-long schedule delays."[9] FITARA establishes a long-term framework through which federal IT investments can be tracked, assessed, and managed, to help reduce wasteful spending and improve project outcomes. Some of the SBA OCIO's responsibilities include to develop and "implement IT performance and design efficiency" and "review systems integration, performance and design efficiency."[10]

C. Federal Information Security Modernization Act (FISMA)

The Federal Information Security Modernization Act (FISMA) requires that each agency head—through the agency's CIO—protect agency information systems in accordance with federal requirements, including establishing an agency information security program.[11] SBA acknowledges that the OCIO is also responsible for maintaining SBA's security and information privacy program.[12]

II. The Office of the Chief Information Officer Faces Management Challenges

Over the years, SBA's Office of the Chief Information Officer has struggled to fulfill its most important functions: to conduct effective oversight over the agency's (1) IT investments, and (2) IT security. Government watchdogs have issued numerous reports outlining the OCIO's

---

[5] U.S. Small Bus. Admin., About the Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio/about-us (last visited July 6, 2017).
[6] *Id.*
[7] The National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. 113-291 (Dec. 19, 2014).
[8] *OMB and Agencies Need to Focus Continued Attention on Implementing Reform Law: Hearing Before the Subcomm. on Gov't Ops. and Subcomm. on Information Tech. of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. (May 18, 2016) (Testimony of David A. Powner, Director, Information Technology Management Issues, U.S. Gov't Accountability Office).
[9] U.S. GOV'T ACCOUNTABILITY OFFICE, ADDITIONAL ACTIONS AND OVERSIGHT URGENTLY NEEDED (June 10, 2015) (GAO-16-675T), *available at* http://www.gao.gov/assets/680/670745.pdf.
[10] U.S. Small Bus. Admin., About the Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio/about-us (last visited July 6, 2017).
[11] Federal Information Security Modernization Act, 44 U.S.C. §3541.
[12] U.S. Small Bus. Admin., About the Office of the Chief Information Officer, https://www.sba.gov/offices/headquarters/ocio/about-us (last visited July 6, 2017).

many failures and flaws. Despite efforts to respond to these watchdogs' recommendations, the OCIO has struggled to meet its legislative and regulatory requirements.

A. A high turnover rate at the Chief Information Officer position has undermined the OCIO's ability to make lasting improvements

The CIO position has endured substantial turnover over the past several years. Since 2005, there have been 8 different CIOs.[13] The current CIO, Maria Roat, is the eighth CIO. Before her arrival in October 2016, the post had been vacant since July 2015. Further, the OCIO has often lacked a deputy CIO and sustained turnover at other key positions.[14]

The SBA Office of Inspector General's (OIG) *Report on the Most Serious Management and Performance Challenges in Fiscal Year 2017* described the OIG's concerns about SBA's IT leadership.[15] The OIG determined that SBA needed to strengthen its IT leadership so that it can address operational risks and challenges.[16] The turnover and repeated vacancies have affected SBA's ability to improve IT investments and security.[17] The OIG emphasized that "continuity in these positions is critical to ensuring open vulnerabilities are corrected, operational issues are quickly resolved, current guidance adopted and implemented, and IT expenditures (maintenance and capital investment) are vetted and monitored."[18] Notably, Maria Roat was hired as CIO just as OIG released its report.[19]

B. The OCIO needs to continue to improve oversight over SBA's IT investments

The OCIO has still not fully implemented FITARA-mandated controls to protect IT investments. According to a recent OIG evaluation, SBA's Office 365 cloud email migration had multiple risk areas that needed to be addressed.[20] Due to lack of planning and oversight, SBA experienced significant delays without deploying a system that meets the Office of Management and Budget's (OMB) deadlines and guidance.[21]

---

[13] GOV'T ACCOUNTABILITY OFFICE, SMALL BUSINESS ADMINISTRATION: LEADERSHIP ATTENTION NEEDED TO OVERCOME MANAGEMENT CHALLENGES (Sept. 2015) (GAO-15-347), *available at* http://www.gao.gov/assets/680/672648.pdf.

[14] In a welcome break from the recent past, SBA currently has a Deputy Chief Information Officer, Guy Cavallo.

[15] U.S. SMALL BUS. ADMIN. OFFICE OF INSPECTOR GEN., REPORT ON THE MOST SERIOUS MANAGEMENT AND PERFORMANCE CHALLENGES IN FISCAL YEAR 2017 (Oct. 14, 2016) (17-02), *available at* https://www.sba.gov/sites/default/files/oig/FY_2017_-_Management_Challenges_-_10_14_16_7.pdf [hereinafter OIG Risk Management Report for FY 2017].

[16] *Id.* at 4.

[17] *Id.*

[18] *Id.*

[19] U.S. Small Bus. Admin., "SBA Appoints Maria Roat as Chief Information Officer," https://www.sba.gov/about-sba/sba-newsroom/press-releases-media-advisories/sba-appoints-maria-roat-chief-information-officer (last visited July 7, 2017).

[20] U.S. SMALL BUS. ADMIN. OFFICE OF INSPECTOR GEN., WEAKNESSES IDENTIFIED DURING SBA'S OFFICE 365 CLOUD EMAIL MIGRATION (June 7, 2016) (16-16), *available at* https://www.sba.gov/sites/default/files/oig/Audit_Report_16-16_Office_365_Cloud_Migration.pdf.

[21] *Id.*

Further, in its management challenge report, the OIG criticized SBA's organizational structure for potentially undermining IT investment oversight.[22] Currently, the CIO reports to the Deputy Chief Operating Officer. Meanwhile, the Chief Digital Officer (CDO), who heads a digital services teams, reports directly to the Chief Operating Officer. The CDO's stated role is to transform SBA's "existing technology using the right mix of modern technology development and management approaches."[23] The OIG determined that the CDO's role may be duplicative and conflict with the CIO's role—who is responsible for recommending modification, termination, or pause of IT projects or initiatives.[24] The Committee has learned that SBA is requesting to reorganize the OCIO so that the Chief Digital Officer falls within the CIO's chain of command.

C. The OCIO needs to continue to improve its controls over its information security

SBA's IT security controls continue to face significant vulnerabilities. In light of recent government security breaches, these vulnerabilities are heightened.[25] The SBA OIG reported last October that there were 39 open recommendations related to IT security, some dating back to fiscal year 2011.[26] The recommendations focus on the need for continuous monitoring that requires validation of compliance with security requirements, risk management, and configuration management.[27]

More recently, the OIG issued a report finding FISMA-related vulnerabilities.[28] In addition to the 28 open FISMA recommendations, the OIG made 9 new recommendations.[29] For example, the OIG recommended that OCIO document policies and procedures regarding the organizational risk management strategy.[30] Further, OCIO needs to align its definitions for SBA's significant risks, mitigation measures, risk tolerances and processes with the National Institute of Standards and Technology standards.[31] Ultimately, a lack of management oversight, resources, and formalized processes have weakened SBA's IT security.

III. Conclusion

The OCIO plays an integral role at SBA. It necessarily touches on all aspects of SBA through its IT investment oversight and IT security oversight. Lapses in those vital areas waste taxpayer dollars and weaken IT security. SBA needs to continue to strengthen its IT leadership so that the OCIO is empowered to fulfill its mission.

---

[22] OIG Risk Management Report for FY 2017 at 4.
[23] *Id.*
[24] *Id.*
[25] *See, i.e.*, the Committee's hearing memorandum for its hearing *Small Business and the Federal Government: How Cyber Attacks Threaten Both: Hearing Before the H. Comm. on Small Business,* 115th Cong. (April 18, 2016), *available at* https://smallbusiness.house.gov/uploadedfiles/4-20-16_hearing_memo.pdf.
[26] *Id.* at 5.
[27] *Id.*
[28] U.S. SMALL BUS. ADMIN. OFFICE OF INSPECTOR GEN., WEAKNESSES IDENTIFIED DURING THE FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW (June 15, 2017) (17-14), *available at* https://www.sba.gov/sites/default/files/oig/SBA_OIG_Report_17-14.pdf.
[29] *Id.*
[30] *Id.* at 3.
[31] *Id.*