FY 2018 Annual Cybersecurity Risk Management Assessment

Office of Government Ethics

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Office of Government Ethics (OGE) budgeted for an IT refresh in FY 2018 to replace major infrastructure components and introduce new technology. For example, OGE is migrating our data center from Virtual Desktop Infrastructure (VDI) to Hyper-Converged Infrastructure (HCI).

However, due to the FY 2018 budget continuing resolution, the procurement process was delayed by several months. This delay resulted in our FY 2018 independent security assessment review being conducted simultaneously with our IT refresh implementation. This will have a negative impact on the "findings" reported by the independent security assessors.

Nevertheless, the OGE is committed to the goal of enhancing its performance security metrics and implementing policies and procedures to protect its IT assets. OGE has taken substantial steps to assess its cybersecurity systems and align its practices to better manage risks.

OGE conducts its risk management process in conjunction with a number of external partners. High and medium risk vulnerabilities are assessed and mitigated in a timely manner, whether identified by an independent security assessment, an eternal partner, or OGE staff. When necessary, OGE implements its risk acceptance process to formally document and justify the acceptance of a known deficiency and the compensating control. OGE requires that a compensating control (or sufficient justification) is defined in order to obtain full approval for a risk acceptance. OGE's risk acceptance process is the result of intense collaboration among the system manager, system administrators and developers, the system owner, the CIO, the authorizing official, and the Senior Agency Official (SAO) for Risk Management.

The OGE Cybersecurity Program provides a level of risk commensurate to the risk as determined by risk assessments conducted by the CIO in collaboration with senior leadership.

Independent Assessment

In FY 2018, the U.S. Office of Government Ethics (OGE) engaged an independent evaluator to assess the status of its information technology cybersecurity program in accordance with NIST SP 800-37 Revision 1, NIST SP 800-53, Revision 4, and NIST SP 800-53A, Revision 4. The independent evaluator identified 62 deficiencies (representing 20% of OGEN security controls). Of the 62 deficiencies identified, the assessor rated 17 as low risk, 44 as moderate risk, and 1 as high risk. Each deficiency has been documented, assigned an ID, and will be tracked until mitigated or accepted by the Authorizing Official (AO). The OGE CIO has written a Plan of Action and Milestones (POAM) document for each deficiency. Each document will be signed by the CIO and the AO to indicate either closure or risk acceptance. However, OGE did not have their independent assessor use IG metrics. Consequently, the IG assessment section is marked "Not Applicable" (NA). The Office of Government Ethics will modify the task order for the FY 2019 independent assessment to include the evaluation of FISMA IG metrics in order to achieve compliance.