Initial Performance Summary

Office of Government Ethics

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	1
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	2
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**3**

CIO Self-Assessment

In FY 2021, OGE engaged assessors from the Enterprise Services Center, Information Security Assessment Group, Federal Aviation Administration, to conduct an independent assessment of the OGE Network using FY 2021 FISMA Chief Information Officer (CIO) metrics. Twenty-nine (29) moderate findings were identified by the assessor. No "very high" or "high" findings were identified. Nine (9) of the findings are covered by signed risk acceptances. For three (3) of those weaknesses, the assessor downgraded the residual risk from "Moderate" to "Low." Consequently, the OGE Chief Information Officer (CIO) will write sixteen (16) Plans of Action and Milestones (POAMs) and three (3) Risk Acceptances (RAs) to address outstanding moderate findings. Each finding will documented, assigned an ID, and monitored until mitigated or accepted by the Authorizing Official (AO). Each POAM will be signed by the CIO and the AO to indicate either closure or risk acceptance.

Also in FY 2021, OGE engaged assessors from the U.S. Department of the Interior to conduct an independent assessment of its information security program using FY 2021 FISMA Inspector General (IG) reporting metrics. The purpose of this audit was to determine the effectiveness of the agency's information security program and practices. This was OGE's third annual audit against these requirements. Previous audits created a solid baseline from which OGE was able to work. FY2021's audit results showed continuous improvement, even in the face of challenges placed upon OGE by new requirements and the COVID-19 pandemic. For purposes of the Audit, FY2021 IG FISMA Reporting Metrics and NIST Cybersecurity Framework identified five domains. These domains are measured against five maturity model levels: ad hoc, defined, consistently implemented, managed

Independent Assessment

The scope of this audit covers the Office of Government Ethics. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of Information Security Continuous Monitoring, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other areas as required by the FY2021 IG FISMA reporting Metrics. The results of the assessment were used to measure the maturity of the agency's information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels in which OGE implements an information security program, develops, and disseminates sound policies and procedures, deploys automated mechanisms in support of risk management and data protection, and trains its personnel to maintain and institutionalize good security practices.

Upon completion of the audit, it is apparent that OGE has gone through extensive efforts in securing the organization GSS environment and has complied with most security control requirements tested during the security assessment of the OGE information security program and information systems. The OGE information security program was found to be Managed and Measurable; notwithstanding, the 1 discrepancy described in section 6.

and measurable, and optimized. The high-level result of OGE’s FY 2021 IG FISMA Metrics Audit was “Managed and Measurable” in all domains.