Cybersecurity Performance Summary

Office of Government Ethics

Chief Information Officer Assessment

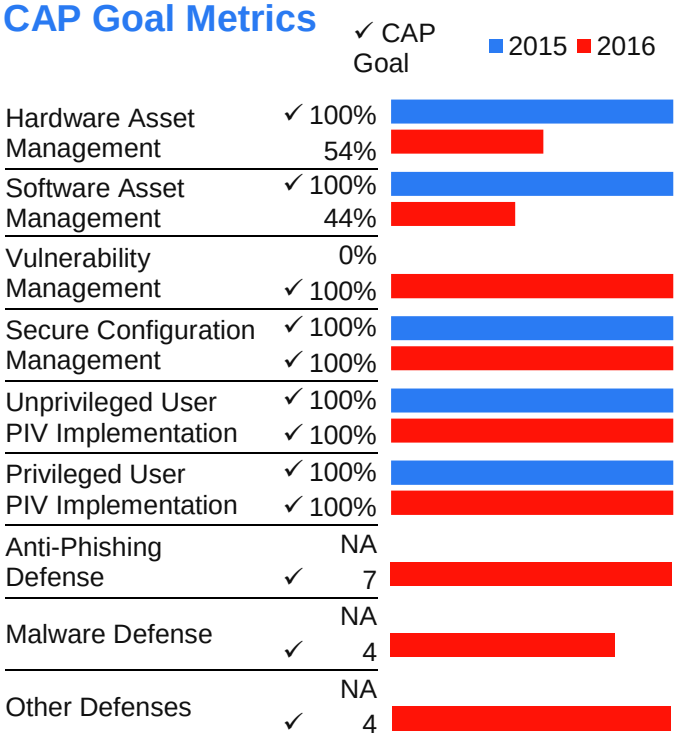
The Office of Government Ethics (OGE) remains committed to maintaining an information technology (IT) security program that takes a risk-based approach to protect the confidentiality, integrity, and availability of OGE systems and data. No major incidents occurred during this reporting period. OGE IT security program highlights are as follows: OGE was one of the first agencies to fully implement the Managed Trusted Internet Protocol Service (MTIPS), which plays an active role in protecting the agency's network; it was also one of the first agencies to fully implement Internet Protocol version 6 (IPv6) in accordance with Office of Management and Budget (OMB) mandates; OGE's private network is scanned for vulnerabilities on a weekly basis by the National Cybersecurity Assessment and Technical Services (NCATS) team at the Department of Homeland Security (DHS); OGE is participating as a charter member of the Continuous Diagnostics and Mitigation (CDM) Program managed by DHS, and actively participates in meetings, conference calls, and the ongoing procurement process; OGE has fully deployed Personal Identity Verification (PIV) card authentication on the agency's network; and OGE's IT specialists continuously monitor the security of the agency's information technology resources. Two-factor authentication is required to access the OGE network locally and remotely. Additionally, OGE conducts annual cybersecurity awareness classes.

Independent Assessment

Identify	NA
Protect	NA
Detect	NA
Respond	NA
Recover	NA

An independent evaluation of the status of the Federal Information Security Modernization Act (FISMA) program for OGE was performed for FY 2015. An independent assessment was not performed in FY 2016, so this section is marked "Not Applicable" (NA). OGE performed a self assessment in FY 2016 using the same network vulnerability tool used by the independent evaluator. OGE collaborated with the independent assessor to configure the tool using the same configuration used by the independent evaluator. OGE runs the tool on a monthly basis. As a result, OGE's internal network is scanned for known vulnerabilities on a monthly basis instead of annually, allowing OGE to be more proactive in the mitigation of vulnerabilities found. Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. OGE will explore contracting with an independent assessor in FY 2017.

CAP Goal Metrics



US-CERT Incidents by Threat Vectors

Total Number of Incidents: 0

Attrition	0
Email	0
External/ Removable Media	0
Impersonation	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Threat Vectors	0