UNITED STATES OFFICE OF
GOVERNMENT ETHICS

Information Technology Strategic Plan
Fiscal Years 2019-2022

Information Technology Division

Table of Contents

OGE's MISSION

The U.S. Office of Government Ethics, established by the Ethics in Government Act of 1978, provides overall leadership and oversight of the executive branch ethics program which is designed to prevent and resolve conflicts of interest. OGE's mission is part of the very foundation of public service. The first principle in the Fourteen Principles of Ethical Conduct for Government Officers and Employees is, "Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain."

As the statutorily established "supervising ethics office" for the executive branch, OGE ensures that the ethics program remains an effective prevention mechanism to guard against conflicts of interest and violations of ethical standards. Each day, some part of the ethics program is at work in every agency in the executive branch. The program ensures that ethics is a top priority for Presidential appointees as they begin government service. It ensures that public servants at all levels remain free from conflicts of interest and even the appearance of conflicts of interest, as they carry out the responsibilities the American people have entrusted to them. It ensures that employees who are seeking to leave the government avoid conflicts of interest, and, after they leave, it ensures that they do not exercise undue influence over their former agencies on behalf of others. Above all, it is working to protect the public's trust in government.

IT MISSION, VISION, AND GOALS

Our Mission

Our mission is to provide the cost-effective information technology infrastructure and services necessary to support the agency's mission while implementing appropriate security controls to protect the confidentiality, integrity, and availability of the agency's data and information systems. Our support of the agency's mission includes planning, developing, testing, implementing, securing, and delivering technology-based business solutions and services. In doing so, we will exceed customer expectations for enabling OGE staff to improve work processes, increase productivity, and enhance OGE operations.

Our Vision

Our vision is to create an environment where we earn respect throughout the agency as a team that demonstrates value. Looking through the eyes of our customers will enhance our vision.

Our Goals and Objectives

1. We are committed to customer service. We strive to overcome obstacles and get things done.
2. We will implement best practices in the management of the agency's information technology.
3. We will provide the information technology services necessary to improve work processes and enhance OGE operations.
4. We will collaborate with executives and other customers to identify the information technology needs of the agency in support of its mission.

RESPONSIBILITIES

Assistant Director for Information Technology

The Assistant Director for Information Technology is responsible for coordinating, documenting, and monitoring the linkage of OGE's strategic and performance plans with the Agency's Information Technology Strategic Plan. The Information Technology Division (ITD) is responsible for providing the technology infrastructure necessary to support the Agency's mission. This includes the planning, developing, testing, implementing, securing, and supporting of technology-based business solutions.

Chief Information Officer

The OGE Director designated the Assistant Director for Information Technology as the Chief Information Officer (CIO) for the U.S. Office of Government Ethics. The Chief Information Officer is responsible for the full range of information technology services including local area network design and support, software and hardware installation, application development, cybersecurity, and network customer support.

Division Heads

OGE's Division Heads are responsible for collaborating with the CIO to identify program activities that will benefit from information technology enhancements, participating with ITD staff and contractors in the development of applications and systems, supporting OGE cybersecurity programs, and supporting ITD staffing and resource requirements (in balance with other Agency funding priorities).

MANAGEMENT OBJECTIVES

OGE's Strategic Plan includes an internal Management Objective to continuously enhance OGE's information systems and processes. OGE will prioritize its activities to continuously enhance and secure its information systems and processes. OGE will provide for the systematic, ongoing oversight and evaluation of the Agency's operations, with a particular focus on (a) reducing or eliminating unnecessary paperwork to enhance productivity agency-wide and (b) utilizing internal and external feedback to identify ways to improve internal operations.

See **Strategic Plan** (below).

REGULATORY COMPLIANCE

A. The Clinger-Cohen Act, also known as the Information Technology Management Act of 1996, defines the role of CIO and requires agencies to tie IT investment to agency accomplishments and establish integrated systems architectures.

B. The Federal Information Security Modernization Act requires agencies to assess the security of automated systems.

C. The Government Paperwork Elimination Act (GPEA) requires agencies to conduct transactions electronically and maintain records electronically when practicable.

D. The Government Performance and Results Act (1993) requires agencies to set standards for measuring their performance. It requires agencies to develop multi-year strategic plans, performance plans, and annual performance reports.

E. Section 508 of the Rehabilitation Act Amendments (1998) requires agencies to allow access to electronic information and information technologies by people with disabilities, including web site navigation.

INFORMATION TECHNOLOGY INVESTMENTS

Federal Information Technology Acquisition Reform Act (FITARA)

The Federal Information Technology Acquisition Reform Act (FITARA) was enacted on December 19, 2014, and outlines specific requirements related to:

- CIO authority enhancements
- Enhanced transparency and improved risk management in IT investments

OMB's intent is to strongly support CIOs in implementing the authorities within FITARA. OGE management strongly supports its CIO's role in implementing the authorities within FITARA. For example:

- OGE developed and incorporated a FITARA Acquisition Tracker form into its automated acquisition system. All IT acquisitions are routed to the CIO for review and approval. As part of the approval process, the CIO must complete the FITARA Acquisition Tracker Form. The Contracting Officer requires this form as a part of the procurement request package. This process ensures that the CIO is aware of and is onboard with all proposed IT requirements.

- The CIO and OGE management have established management practices that align IT resources with agency missions, goals, programmatic priorities, and statutory requirements;

- OGE has established an alignment for roles, responsibilities, and authorities of the CIO and the roles and responsibilities of other applicable Senior Agency Officials in managing IT as a strategic resource;

- OGE has enabled the CIO's role with respect to the development, integration, delivery, and operations of any type of IT, IT service, or information product to enable integration with the capabilities they support wherever IT may affect functions, missions, or operations;

- OGE has strengthened the CIO's accountability for the agency's IT cost, schedule, performance, and security;

- OGE has established an inclusive governance process that enables effective planning, programming, budgeting, and execution for IT resources;

- OGE provides transparency on IT resources across agency programs; and

- OGE has provided appropriate visibility and involvement of the CIO in the management and oversight of IT resources across the agency to support the successful implementation of cybersecurity policies to prevent interruption or exploitation of program services.

Technology Business Management (TBM)

TBM is a set of best practices for running IT like a business to effectively and consistently communicate the cost of IT along with the business services IT provides. The primary goal of TBM is to provide the ability of IT and business leaders to have data-driven discussions about cost and value of IT to best support business goals.

OGE has established an alignment for roles, responsibilities, and authorities of the agency CIO and the roles and responsibilities of other applicable Senior Agency Officials in managing IT as a strategic resource. This alignment is consistent with the goals and objectives of TBM:

- **Transparency**: Building trust, promoting accountability, & revealing opportunity
- **Cost Optimization**: Maximizing IT asset utilization & return on investment
- **Communication**: Creating a common language bridging IT and business, and enabling better conversations about value vs. cost
- **Business Value**: Augment investment decision making process

STRATEGIC PLANS

The OGE Information Technology Strategic Plan fully aligns with and supports the OGE Strategic Plan and is reviewed annually alongside the Annual Performance Plan Reviews (as required by the GPRA Modernization Act) to determine if there are any performance gaps or changes to mission needs, priorities, or goals. The IT Strategic Plan is updated to align with Agency Strategic Plans as specified in OMB Circular No. A-11. The IT Strategic Plan describes how information resources management activities help accomplish agency missions. The Plan is updated annually and made publicly available on the OGE website.

As stated in the OGE Strategic Plan, Management Objective 5.3 (Continuously Enhance OGE's Information Systems and Processes), OGE prioritizes its activities to continuously enhance and secure its information systems and processes. These systems and processes include OGE's executive branch-wide electronic financial disclosure filing system, Integrity.gov, as well as numerous internal applications, policies, and operating procedures. OGE will also maintain a strong, secure IT infrastructure, which is necessary to mitigate risk and to allow OGE to conduct its mission-critical work.

Evaluating Progress

Examples of potential measures and indicators for Management Objective 5.3:

- Percent of downtime of Integrity, OGE's network, and website
- Results of Cybersecurity Risk Management Assessment
- Feedback from Integrity and public website users

MANAGEMENT IMPROVEMENT INITIATIVES AND POLICIES

Capital planning and investment control
OGE's budget estimates reflect its commitment to information technology (IT) investments that directly support agency missions as identified in the agency's Information Technology Strategic Plan and are consistent with the CIO role and CIO review described in OMB Memorandum M-15-14, "Management and Oversight of Federal IT" and the Federal IT Acquisition Reform Act (FITARA).

Agency budget estimates reflect a comprehensive understanding of OMB security policies such as OMB Circular A-130, and National Institute of Standards and Technology (NIST) guidance, including compliance with the Federal Information Security Modernization Act, and OMB Memorandum M-17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements."

CLOUD MIGRATION

OGE's budget implements a four-year IT refresh cycle that supports continuous enhancements to information systems and processes. In FY 2020, OGE will initiate a readiness assessment by investigating the feasibility of moving the OGE network into a FedRAMP cloud environment in FY 2022.

SECURITY

OGE cybersecurity policies and procedures reflect a comprehensive understanding of OMB security policies such as OMB Circular A-130, and National Institute of Standards and Technology (NIST) guidance, including compliance with the Federal Information Security Modernization Act, and OMB Memorandum M-17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements."

OGE implements established guidelines for the preparation of security plans for applications and systems processing CUI information. All applications inherit security from the OGE network (classified as a general support system), and are subject to an independent risk-based review annually, or whenever there is a significant change. At a minimum, these reviews identify and assess IT assets, threats, vulnerabilities, controls, other protective measures. Annual reviews are performed in accordance with NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

OGE has implemented and will continue to pursue the implementation of strong cybersecurity protocols. OGE was one of the first agencies to fully implement Managed Trusted Internet Protocol Service (MTIPS), which plays an active role in protecting the agency's network. OGE's

Internet connectivity is compliant with the Trusted Internet Connections (TIC) initiative. All Internet traffic traverses the MTIPS connection.

OGE was one of the first agencies to fully implement Internet Protocol Version 6 (IPv6) in accordance with OMB mandates.

OGE's network perimeter is scanned for vulnerabilities on a weekly basis by the Department of Homeland Security (DHS), National Cybersecurity Assessments and Technical Services (NCATS).

OGE is collaborating with the Department of Homeland Security to implement the Continuous Diagnostics and Mitigation (CDM) Program (Task Order 2F). Full deployment is anticipated by the end of FY 2019.

OGE fully deployed personal identity verification (PIV) card authentication on the OGE network.

In addition, OGE's IT specialists scan the network for vulnerabilities on a regular basis to identify and mitigate risk.

OGE conducts mandatory annual cybersecurity awareness and privacy classes.

Security Operations Centers

OGE plans to move the OGE Network to a "moderate" FedRAMP cloud environment with multiple processing sites. We plan to implement and manage vulnerability and asset management; threat intelligence and assessment; security monitoring; analysis and detection; incident management and response; and situational awareness services from the cloud service provider, a compatible shared service provider, or through a non-SOC organization internal to the agency.

Continuous Diagnostics and Mitigation (CDM)

The Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. OGE participates in CDM Task Order 2F, Continuous Monitoring as a Service (CMaaS). As required by OMB Memo M-19-02, OGE has a CDM-specific line item in its budget and has built CDM requirements into its budget plans from FY 2018 and beyond.

High Value Asset (HVA) Modernization

In alignment with OMB Memo M-19-03, OGE’s budget submission accounts for the modernization of its HVAs to implement corrective action attributed to obsolete or unsupported technology as well as critical deficiencies in the solution architecture.

Identity, Credential, and Access Management (ICAM)

OGE has implemented 2-factor authentication using for network authentication using personal identity verification (PIV) cards via participation in the GSA HSPD-12 Managed Service Office's (MSO) USAccess program. In alignment with OMB Memo M-19-17, OGE’s budget submissions include funding for OGE’s identity management program (logical access) and its physical access and control program.

Coordinated Vulnerability Disclosure

OGE leverages private sector best practices to manage, modernize, and secure its information and information systems to stay abreast of and incorporate successful industry-backed methods to improve the security of its information systems. The Chief Information Officer aligns agency resources to more effectively and expeditiously identify, manage, and remediate critical and high vulnerabilities in support of the agency's approach to enterprise risk management.

IT RESOURCE STATEMENTS

In compliance with OMB Circular No. A-11, IT Resource Statements are updated and submitted whenever OGE submits updates to its agency IT Portfolio Summary:

1. The OGE CIO collaborates with the Senior Agency Official for Privacy (SAOP), the Chief Financial Officer (CFO) and the budget officer on IT Budget submissions to ensure that IT budget data is consistent with the agency's budget submission

2. The CIO reviews and has significant input in approving IT investments included in the agency budget request. For example, OGE developed and incorporated a FITARA Acquisition Tracker form into its automated acquisition system. All IT acquisitions are routed to the CIO for review and approval. As part of the approval process, the CIO must complete the FITARA Acquisition Tracker Form. The Contracting Officer requires this form as a part of the procurement request package. This process ensures that the CIO is aware and onboard with all proposed IT requirements.

3. OGE has developed and implemented a plan to ensure that all common baseline FITARA responsibilities are in place, including the consideration of risk management and internal controls.

LIST OF PLANNED PROJECTS

OGE's budget implements a four-year IT refresh cycle that supports continuous enhancements to information systems and processes. OGE designs, implements and maintains a dynamic, stable and secure network environment in support of its mission.

A. PLANNED FY 2019 PROJECTS

OGE Website

- OGE will refresh the design of its public website.

Cybersecurity

- OGE will procure an independent assessment of its cybersecurity program using FISMA CIO metrics.
- OGE will procure an independent assessment of its cybersecurity program using FISMA IG metrics.

B. PLANNED FY 2020 PROJECTS

Cybersecurity

- OGE will procure an independent assessment of its cybersecurity program using FISMA CIO metrics.
- OGE will procure an independent assessment of its cybersecurity program using FISMA IG metrics.
- OGE will designate a Deputy Chief Information Security Officer with cybersecurity credentials.

OGE Network

- OGE will initiate a readiness assessment to investigate the feasibility of moving the OGE network to a FedRAMP cloud.

OGE Website

- OGE will implement functional enhancements.

OGE Web Applications

- OGE will update existing web applications

C. PLANNED FY 2021 PROJECTS

Cybersecurity

- OGE will procure an independent assessment of its cybersecurity program using FISMA CIO metrics.
- OGE will procure an independent assessment of its cybersecurity program using FISMA IG metrics.
- OGE will complete its readiness assessment to investigate the feasibility of moving the OGE network to a FedRAMP cloud.

D. PLANNED FY 2022 PROJECTS

OGE Network

- OGE will replace its desktop environment and may move its network infrastructure to a FedRAMP cloud service provider, pending the results of the readiness assessment initiated in FY 2020.

Cybersecurity

- OGE will procure an independent assessment of its cybersecurity program using FISMA CIO metrics.
- OGE will procure an independent assessment of its cybersecurity program using FISMA IG metrics.