UNITED STATES OFFICE OF
GOVERNMENT ETHICS

May 28, 2020

The Honorable Richard Shelby
Chairman
Committee on Appropriations
United States Senate
S-128, The Capitol
Washington, DC 20510

The Honorable Patrick Leahy
Ranking Member
Committee on Appropriations
United States Senate
S-146A, The Capitol
Washington, DC 20510

The Honorable John Kennedy
Chairman
Subcommittee on Financial Services
and General Government
Committee on Appropriations
United States Senate
136 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Christopher Coons
Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
United States Senate
125 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Shelby, Ranking Member Leahy, Subcommittee Chairman Kennedy, and Subcommittee Ranking Member Coons:

The U.S. Office of Government Ethics (OGE) writes to request authorization[1] to use $33,434 of its fiscal year 2019 unobligated balance[2] for expenditures in fiscal year 2020, to enhance OGE's internal network, based on risk-mitigation recommendations.

OGE provides overall leadership and oversight of the executive branch ethics program designed to prevent and resolve conflicts of interest. OGE's network facilitates its mission-critical work and the value of OGE's network is even more apparent during the pandemic while virtual access is necessary and public trust matters most.

In fiscal year 2019, OGE engaged an independent auditor to assess the status of its network using Federal Information Security Modernization Act (FISMA) Inspector General (IG) metrics. While the audit had no "critical" or "high" risk findings, the auditor determined that OGE did have opportunities for network improvement and identified thirty-five (35) "moderate" risk findings. The auditor noted that "automated tools are required to effectively address these deficiencies identified in the assessment. Deployment of automated toolsets in select focus areas is presently not feasible due to budgetary constraints."

[1] OGE requests this authorization pursuant to Pub. L. No. 116-6, § 609, 133 Stat. 182 (2019). OGE only has one budget account, so its request to use 50% of OGE's unobligated balance of fiscal year 2019 appropriations in fiscal year 2020 will not cross budget accounts.

[2] The unobligated balance of OGE's fiscal year 2019 Salaries and Expense appropriation, as of May 27, 2020, was $66,869, half of which is $33,434. OGE is requesting authorization to use $33,434 of the available carryover balance.

OGE's intent is to purchase software, at a cost of $33,434, which will enable OGE to address risk findings. For specific details regarding the risks and how the selected tool will address those risks, please see the table below.

Enhancing OGE's Internal Network *Assessor's recommendations and how the selected tool will address identified risks*	
Assessor's Recommendation to Address Risk	**How Tool Addresses Risk**
Deploy automated mechanisms for reviewing and analyzing the OGE Network's audit records for inappropriate or unusual activity.	The selected tool allows for automatic alerting and audit of common privilege abuse pathways; detects events such as suspected credential theft, unmanaged privileged access, and service account abuse.
(1) Deploy automated mechanisms to document and maintain current baseline configurations of the OGE Network. (2) Provide evidence that the configuration management policy and procedures are reviewed at least annually.	The selected tool allows OGE to monitor and control all access to configuration management systems and ensure that there is audit and accountability for all related activity.
Deploy automated mechanisms to assist with the timely remediation of legitimate vulnerabilities.	The selected tool helps to protect the integrity of vulnerability scanning systems by ensuring that only those with authorized privileged credentials can gain access to these systems. A detailed log is kept so that OGE will have a complete record.
(1) Deploy automated mechanisms supporting and/or implementing information system monitoring capability. (2) Define monitoring objectives to detect attacks and indicators of potential attacks on the information system.	The selected tool allows for automatic alerting and audit of common privilege abuse pathways such as credential theft, unmanaged privileged credentials, and escalation of permissions.
Deploy automated mechanisms that implement, monitor, and/or control information system configuration settings; automated mechanisms that identify and/or document deviations from established configuration settings.	The selected tool helps maintain baseline configurations and supports the implementation of oversight of configuration change control by ensuring that only authorized users can gain access to system configurations.
Deploy automated mechanisms for developing, reviewing, updating and/or protecting the contingency plan.	The selected tool will help OGE to design a contingency plan that is compliant with audit requirements, and ensure that only authorized users can gain access.
Deploy automated mechanisms to assist with the timely remediation of legitimate vulnerabilities.	The selected tool will help to protect the integrity of vulnerability scanning, ensuring that only those with authorized privileged credentials can gain access to these systems. A detailed log is kept so that organizations will have a complete record of scan requests.

OGE appreciates your favorable consideration of this request for important improvements to its network. If you or your staff needs additional information or have any questions about this request, please contact Diana Veilleux, Chief, Legal, External Affairs and Performance Branch at (202) 482-9203. An identical request is being sent to the House of Representatives Appropriations Committee and its Subcommittee on Financial Services and General Government.

Sincerely,

SHELLEY FINLAYSON

Digitally signed by SHELLEY FINLAYSON
Date: 2020.05.28 14:53:54 -04'00'

Shelley K. Finlayson
Chief of Staff and Program Counsel