HOUSE OVERSIGHT AND REFORM SUBCOMMITTEE ON GOVERNMENT OPERATIONS "FITARA 14.0"
JULY 28, 2022

<u>Questions for the Record Submitted by Chairman Gerald E. Connolly</u>

1. How is your office working with the login.gov team to ensure that the platform can scale up to meet the requirements of government agencies?

RESPONSE: Login.gov is a top priority of GSA. GSA's Technology Transformation Services (TTS) and the Login.gov team have operational responsibility for the development and build out of the Login.gov platform and the underlying supporting infrastructure. GSA IT, through the Office of the Chief Information Security Officer, is focused on ensuring development and delivery of a highly scalable, resilient, and security and privacy compliant solution, to meet the demands of our broader governmentwide partners. Key focus areas ensuring that the platform can scale to meet the requirements of government agencies include:

- **Amazon Web Services (AWS) Infrastructure**
  - Login.gov utilizes the Federal Risk and Authorization Management Program (FedRAMP) authorized Amazon Web Services (AWS) and rapid auto scaling design principles to meet current and future capacity needs.
  - GSA IT is providing security oversight and guidance for upcoming reliability, security, and scalability improvements to the platform. There are rapid developments and evolving threats within the identity verification and authentication space. Login.gov is able to keep the pace by continually innovating and increasing its capabilities. GSA IT works closely with Login.gov to ensure the requisite processes and controls are in place, which both enables Login.gov to timely respond to these developments and maintain the high standards required of a federal system.

- **Staffing and Support**
  - GSA IT has dedicated Information Security System Officers and will provide embedded development, security, and operations resources to the Login.gov team to ensure compliance and security activities keep pace with rapid growth and change. The overall security is overseen by a System Level Information System Security Manager as well as the GSA IT FedRAMP Program Manager.

- **Security Stack**
  - Login.gov integrates with the GSA Enterprise Security Operation Center (SOC), which provides not only the 24x7x365 operation monitoring, but also deploys more advanced Artificial Intelligence and Machine Learning (AI/ML) capabilities

to quickly identify and respond to security threats, and structured and unstructured Threat Hunting.

- **Security and Privacy Compliance**
  - GSA IT and Privacy staff partner with the Login.gov team to ensure compliance with the FedRAMP control baseline and additional privacy controls. Additionally GSA IT provides the automated testing of security controls, as well as management of Public Vulnerability Disclosure and Bug Bounty programs.

2. How will the General Services Administration (GSA) make certain that Login.gov ensures equitable access for historically underrepresented communities in the United States?

RESPONSE: Ensuring equitable access for historically underrepresented communities in the United States to government benefits and services is paramount for Login.gov. Login.gov is focused on expanding its capabilities as well as being judicious in what technologies it rolls out and how they are deployed.

Today, Login.gov's identity verification process is completely online, optimized for mobile devices, and fully self-service. A significant portion of the $187 million investment from the Technology Modernization Fund (TMF) is targeted to increase alternate channels for identity verification to increase coverage and access, which will benefit, in particular, historically underrepresented communities. For example, Login.gov is working to develop remote supervised identity proofing (live online support) and in-person identity proofing, and is leveraging other existing government identity sources such as the American Association of Motor Vehicle Administrators.

GSA is aware that ensuring equitable access for all, in particular historically vulnerable populations, comes with the responsibility of offering a shared service to government agencies that the public can rely on. Equitable access is a fundamental pillar of our mission of providing simple, secure access to government services.

3. How is GSA allocating the $187 million Technology Modernization Fund investment for Login.gov?

RESPONSE: The TMF investment is being used in three primary areas. The first is establishing additional identity verification capabilities to ensure equitable access. For example, remote supervised identity proofing (live online support), in-person identity proofing, and leveraging other existing government identity sources.

The second is increasing cybersecurity and anti-fraud capabilities by enhancing its security operations. This includes ensuring the requisite team provides 24/7 security coverage. In addition, Login.gov is launching an anti-fraud operations team to combat fraudulent actors and provide redress mechanisms for legitimate users caught by those controls. Lastly, the TMF investment is being used to accelerate agency adoption.

4. The Internal Revenue Service (IRS) recently announced that it will begin using the Login.gov service in 2023. Will Login.gov be able to support the IRS's needs next year?

RESPONSE: Login.gov is continually engaging with agency partners to provide the best experience to serve its growing user population and implement protections to keep pace with the evolving security landscape.

Key items on the Login.gov roadmap that are essential for nationwide scale and will benefit all agency partners are currently underway. Examples include:

- Ensuring scalability of the platform for increased traffic, including an increase in contact center support staff, hours, and services;
- Providing anti-fraud control and robust redress mechanisms to legitimate users; and
- Increasing identity verification service coverage by improving its current fully remote and self-service identity verification process as well as providing additional channels to complete identity verification.

5. How is GSA helping agencies implement multi-cloud capabilities?

RESPONSE: Implementing a properly governed and secured multi-cloud infrastructure is a complex challenge. As agencies across the federal government mature their cloud offerings, new and more intricate resources are required. GSA offers support and shared services in the compliance, security, acquisition, and technology realms. These combined efforts serve to accelerate the adoption of cloud technologies across the government. GSA supports agencies in implementing multi-cloud capabilities in a number of ways:

1. To enable the government-wide, safe implementation of cloud technologies, the GSA Federal Risk and Authorization Management Program (FedRAMP) promotes the adoption of secure cloud services by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP eliminates duplicative efforts by providing a common security framework. Agencies review their security requirements against a standardized baseline. A Cloud Service Provider (CSP) goes through the authorization process once. After achieving authorization for their Cloud Service Offering (CSO), the CSO is listed in the FedRAMP Marketplace, and pertinent security artifacts are stored in FedRAMP's secure repository where federal agencies can request access to the materials as a way of facilitating reuse of the CSO. FedRAMP enables the federal government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a government-wide scale.

2. GSA delivers multiple offerings to support the acquisition of cloud services, primarily via the Technology Purchasing Programs & the Information Technology Category. The Technology Purchasing Programs provides government-wide acquisition contracts (GWACs) like Alliant 2, Polaris, and Blanket Purchase Agreements (BPAs) to accelerate and standardize cloud service acquisition. Additionally, GSA regularly hosts training events to include the *Think Cloud Think GSA* event as well as monthly webinars designed to educate federal IT buyers on how to buy cloud. The Cloud Information Center is a robust hub for resources and information that agencies need to efficiently and effectively buy cloud and related services. GSA's Assisted Acquisition Service fosters adoption across the federal government by facilitating procurement best practices and FAR compliance in cloud acquisition.

3. GSA also sponsors several Cloud Adoption Communities of Practice to share best practices and lessons learned across the federal government. For example, GSA's Office of Governmentwide Policy sponsors the Cloud and Infrastructure Community of Practice. Additionally, the Information Technology Category collaborated with the Acquisition and Cloud Adoption Centers of Excellence to stand-up an Emerging Technology Acquisition Community of Practice.

4. The Technology Transformation Services works directly with partner agencies to facilitate multi-cloud implementation by utilizing GSA shared services and industry best practices.

5. The Centers of Excellence Cloud Adoption and Infrastructure Optimization centers currently support six agencies across the federal government (OPM, GAO, NICHD, STB, USDA, EPA). Their work can vary based on the partner agency's maturity level and specific needs. Still, they strive to always assist the agency in moving forward in their cloud adoption journey.

6. GSA IT, as a professional courtesy to other IT organizations across the federal enterprise, shares its experiences and best practices in IT modernization and transformation through playbooks as well as through direct conversations and information sharing.

By providing agencies with the necessary resources via numerous avenues to meet the complex challenges of acquiring, operationalizing, and securing multi-cloud environments, GSA remains a force for the adoption of emerging technology in the federal government.

Questions for the Record Submitted by Ranking Member Jody Hice

1. The description accompanying the Scorecard category titled "Enhanced Transparency and Improved Risk Management" says, "FITARA requires OMB to publicize detailed information on federal IT investments and requires agency CIOs to categorize their major IT investments by risk." GSA scored 85 percent on this category.

a. Please explain how GSA defines “risk” and a “major IT investment.”
b. Does GSA’s grade mean that 85 percent of its major IT investments are at risk? Please explain the significance of GSA’s grade in this category.
c. What percentage of GSA’s entire IT investment portfolio is comprised of “major IT investments”?

RESPONSE: a. GSA defines “major IT investment” based on OMB guidance (A-11, Section 55) and our own internal criteria. Major IT investments are those Information Technology systems operated by GSA with a defined life cycle (e.g., development, deployment, maintenance, sunsetting) that meet at least one of the following criteria:

- Requires special management attention because of the initiative’s importance to agency mission or function of GSA as defined in GSA IT’s Strategic Plan or the agency strategic plan;
- Has high-level executive visibility from the Office of the Administrator as a result of direction related to White House or Congressional initiatives;
- Is for financial management (internal agency applications tracking financial obligations, outlays, fund balances, and reporting capabilities) and spends more than $2 million annually;
- Has development, operating, or maintenance costs of $10 million or more in each of the past three consecutive years and is budgeted to maintain spending levels for the coming fiscal year; or
- Is primarily funded through methods other than established or permanent funds; such a method could be fee-for-service or funding received from other agencies.

GSA classifies its major investments’ risk ratings as Red/Yellow/Green—depending on how critical these investments are to agency operations and the impact to operations if they were unavailable. An investment will receive a rating of Yellow if it meets at least two of the following criteria:

- The investment is a Shared Services/eGov Initiative, a Security Investment, a High Visibility Initiative, or High Value Asset;
- Its development, modernization, and enhancement (DME) budget is more than $5 million, or if DME makes up more than 50% of total spending;
- The Program Manager does not have the required level of project management certification;
- There are pending financial obligations or funding risks; or
- There are three or more significant active risks recorded in the reporting system, Folio.

b. GSA assigns a risk classification to an investment based on organizational risk and how critical these investments are to our operations and the impact to operations if they were unavailable. In the July 2022 FITARA scorecard, 85% of our major investment dollars were allocated to investments rated yellow.

c. Of GSA’s total IT spending, 32.8% is associated with Major IT Investments. Out of 108 total investments, 24 (22%) are classified as Major IT Investments.

2. During the hearing, Rep. Andrew Clyde asked you to provide an estimate of the resources required of the agency to put together the data feeding into this Scorecard. In providing the Committee with that response, please provide as much information as possible relative to the time, money, and staff it takes to collect and assemble the data for GSA's data submissions for the Scorecard.

RESPONSE: As part of our work, GSA IT measures performance across multiple spectrums. All of the data required for the FITARA scorecard metrics is captured outside of the FITARA process and shared out in multiple public forums.

The data underlying the scorecard metrics are captured through the work of approximately 7 FTE from across GSA who provide data for the IT Dashboard, PortfolioStat, EIS reporting, responses to Congressional inquiries, and the IG FISMA Audit. This work is performed throughout the entire year.

3. Are there categories not included in the Scorecard that could or should be added to better measure GSA's information technology and cybersecurity posture?

RESPONSE: Yes, we think that there are categories that can be added to the Scorecard. Any new categories should consider the following: 1) automation in data collection to minimize burden on the CIO community; 2) focusing on data that is already available; 3) waiting until data matures before adding new initiatives to the Scorecard; and 4) avoiding publishing sensitive internal information about an agency's cybersecurity posture.

With those considerations in mind, new categories for the Scorecard could include analysis of security and accessibility features for websites (source: U.S. Web Design System, DAP), individual agency's assessment of IT modernization progress (source: Agencies), and assessment of agency maturity on digitization of email and electronic records (source: NARA).

To better measure cybersecurity posture, we recommend focusing on cyber operations and resiliency, not just on compliance. To improve alignment, the scorecard could reflect both the OIG *annual* assessment determinations AND Agency CIO *quarterly* FISMA assessment in scoring. The latter is more operational, outcome oriented, and focused on the capabilities that are fundamental in ensuring cyber resiliency.