September 1, 2021

The Honorable Gerald E. Connolly
Chairman
Subcommittee on Government Operations
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

The Honorable Jody Hice
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Connolly and Ranking Member Hice:

Below are my responses to your post hearing questions submitted to the official record for the hearing that was held on Wednesday, July 28, 2021, titled "FITARA 12.0."

1. **In March of 2020, the Small Business Administration (SBA) discovered a problem with the Economic Injury Disaster Loans (EIDL) system that resulted in a data breach involving information from nearly 8,000 applicants to EIDL. What vulnerabilities in the system led to the breach, and what steps has SBA taken to address those vulnerabilities and prevent future breaches?**

   The incident referenced occurred while making multiple system changes in the middle of the night. In such a short time, a mistake was made in one of the system's configurations, which inadvertently exposed personally identifiable information (PII) data for some individuals. There was no known loss or exfiltration of data from the system. Within three hours, SBA discovered that exposure and quickly addressed it. SBA followed standard procedures for dealing with a PII exposure, which includes immediately reporting it to US CERT. SBA went further to mitigate the potential risk of those individuals whose data may have been exposed and offered these individuals free credit monitoring services.

2. **SBA is one of three agencies to earn an "A" for the Modernizing Government Technology Act IT Working Capital Fund metric. How have you leveraged your Working Capital Fund to improve the information technology position of SBA? Could you provide examples of projects the Working Capital Fund has allowed you to undertake?**

   The IT working capital fund (IT WCF), established in 2019, has allowed SBA to rapidly accelerate SBA's IT modernization plans. We have funded a variety of modernization efforts

such as some of the Certify improvements, Entrepreneurial Development Management Information System – Next Generation (EDMIS-NG) development, the implementation of SBA Connect, SBA's single-sign on solution leveraging Login.gov, and continuing enhancements for the SBA.gov infrastructure. Specifically:

- SBA.gov: SBA.gov used the IT WCF to continue the sunset of a legacy Content Management System (CMS) and launch most of its replacement in anticipation of full replacement and a version upgrade next year. In addition, SBA.gov's production environment migrated to a serverless architecture in January 2021 resulting in an advanced cybersecurity posture, cost savings through on-demand scalability, greater flexibility in the development process, and reduced operational costs.

- EDMIS-NG: The Office of Entrepreneurial Development (OED) depends on EDMIS-NG to report on the effectiveness of its programs. EDMIS-NG is a modern cloud-based system that provides innovative capabilities that allows interfaces into the variety of user systems, such as Neoserra, Salesforce, CenterIC, Outcome Tracker, and MySQL. The solution gives OED program offices, SBA resource partners and the agency's field offices the ability to key in or upload information on training and counseling activities. Starting with the business and business owner data collected by EDMIS-NG, SBA is continuing to define methods of enriching this data with additional demographic datasets, with the goal of harmonizing and deeply understanding the program's reach into underserved communities, small business and informing program equity goals. These innovations and enhanced flexibilities give us better tools to analyze entrepreneurial development data, providing us with the intelligence needed to improve the performance management of OED programs.

- SBA Connect: SBA Connect is SBA's single sign-on user authentication enterprise service that utilizes the government-wide Login.gov shared service. SBA is phasing out its legacy authentication technology as it integrates SBA Connect enterprise-wide. SBA Connect was integrated into the Office of Disaster Assistance (ODA) Disaster Loan Application Portal in January 2021. This modern service enables identify proofing for the disaster loan applicants thereby helping reduce potential fraud. SBA Connect was also integrated into EDMIS-NG in May 2021. SBA Connect continues to be optimized for efficient integration into new applications.

Insight: Integration of new tenant application for OCA for the Loan Forgiveness Program is underway.

3. **How was your agency able to establish a Modernizing Government Technology Act IT Working Capital Fund?**

The SBA received authority in the FY 2018 National Defense Authorization Act to establish a Modernizing Government Technology Act IT Working Capital Fund (ITWCF). The CIO partnered closely with the Chief Financial Officer (CFO) to formally establish the fund in the Agency's financial system. The Agency identified IT modernization targets with SBA senior leadership and the Office of Management and Budget (OMB) where the ITWCF would be utilized. Following coordination with OMB and the Appropriations Committees, SBA received an additional transfer authority in the annual appropriations bill, authorizing SBA to reprogram resources into the fund to spend on IT modernization activities. IT modernization initiatives often require sustained commitment over several years, and the ITWCF enables repurposing of annual

funds in the Salaries and Expenses account as well as the Business Loan Programs account into a three-year ITWCF account.

4. **On the FITARA 12.0 Scorecard, SBA received a "D" in the Enterprise Infrastructure Solutions metric, having only transitioned 33.8% of its services off expiring contracts. Could you elaborate on some of the barriers or challenges SBA is having with this transition?**

As a result of the pandemic, agency resources massed around supporting the shift to virtual work and the CARES Act support. The dedicated support for EIS transition was displaced and the transition effort stalled. This was actually an aid to the agency as we have been able to revisit and refocus, and we have reengaged GSA to leverage their tools and support. We anticipate being completely transitioned to EIS by the end of calendar year 2022.

5. **The transition off of the General Services Administration's expiring telecommunications contracts provides agencies a chance to make transformative technology changes at their agency. Some agencies, however, may simply use the corresponding metric on the FITARA Scorecard as a check-the-box exercise instead of taking time to migrate to services that improve mission and service delivery. How is SBA using the transition off of expiring telecommunications contracts to improve the agency's operations?**

The SBA has made significant advancements with transitioning voice services, represents the largest portion of SBA's use of GSA WITS/TOPS contracts. As a result of SBA's gradual transition from expiring telecommunications contracts, the Agency has significantly improved its operations by enhancing its voice, video, and office productivity collaboration capabilities.

The SBA's transition was not a like-for-like replacement. The network modernization concept involves software defined network and zero-trust services. The initial EIS Task Order includes initial phases of designing and deploying these architectures.

6. **In 2020, there was a significant increase in identity theft reports that involved government benefit applications. What has SBA done to tighten its processes to prevent fraud?**

The Office of Disaster Assistance (ODA) Disaster Credit Management System (DCMS) has moved to using the SBA Connect platform that provides identity validation and proofing with GSA's Login.gov as the primary Identity proofing/Identity verification (IDP/IDV) provider. There are several identity verifications steps which are taken to help reduce identity fraud. These steps include:

   a. Copy of front and back of State issued ID is submitted by the applicant to verify the identity of the applicant.
   b. Login.gov verifies the state issued ID and social security number of the applicant against either issuing or authoritative data sources.
   c. Login.gov verifies the authenticity and validity of all identity attributes from the state-issued ID.
   d. Login.gov utilizes authoritative telecommunication data sources to verify an applicant's address when a user is an account holder on their personal phone plan.
   e. If the telephone number is not registered under applicant's name, applicant's address is verified by sending them a verification code on their postal mailing address

f. Email address provided by the applicant is verified to ensure that the email address is a valid email address, and the applicant has access to the email address provided

g. Telephone number provided by the applicant is verified to ensure that the telephone number is a valid telephone number, and the applicant has access to the telephone number provided.

h. Multi-factor authentication is used to login to the system to make it difficult for an unauthorized person to access the system.

i. Strong 12 characters long password is used to help prevent an unauthorized person to access the system.

j. Separate from Login.gov, previous years' tax returns are verified directly with IRS.

For the traditional loan programs, SBA continues to rely on lenders performing due diligence.

For the last round of Paycheck Protection Program (PPP), SBA implemented the pre-fund analysis process that relies on public and private data sources to verify the borrower and business ownership.

For the Restaurant Revitalization Fund (RRF) and the new COVID-EIDL program, SBA implemented the GAO risk management framework. The framework leverages the pre-fund analysis process and lessons learned to enhance execution of the Know Your Business and Know Your Customer processes. RRF and COVID-EIDL also leverage a key commercial control to validate bank routing and account numbers. This allows the loan applicant to authenticate and real-time validate the bank account information – ensuring the funding vehicle for the loan is valid, active, and aligned to the business owner and account holder.

7. **How does SBA verify the identities of loan applicants?**

SBA is taking multiple steps to verify the identity of the loan applicants using GSA's Login.gov which include the following:

a. Copy of front and back of State issued ID is submitted by the applicant to verify the identity of the applicant.

b. Login.gov verifies the state issued ID and social security number of the applicant against their database from states.

c. Login.gov verifies that the address provided is a valid address and it's checked with USPS address database

d. Login.gov verifies that the telephone number is registered under applicant's name by checking their database.

e. If the telephone number is not registered under applicant's name, applicant's address is verified by sending them a verification code on their postal mailing address

f. Email address provided by the applicant is verified to ensure that the email address is a valid email address, and the applicant has access to the email address provided

g. Telephone number provided by the applicant is verified to ensure that the telephone number is a valid telephone number, and the applicant has access to the telephone number provided.

h. Multi-factor authentication is used to login to the system to make it difficult for an unauthorized person to access the system.

i. Strong 12 characters long password is used to help prevent an unauthorized person to access the system.

For the traditional loan programs, SBA continues to rely on lenders performing due diligence.

For the last round of PPP, SBA relied on information from public and private data sources to verify identity.

For the RRF and new COVID-EIDL program, SBA implemented the GAO risk management framework. The framework leverages information from Treasury and public data sources to verify identity.

8. **Has SBA sought any assistance from Credential Service Providers certified against NIST800-63-3?**

The SBA utilizes the GSA's USAccess for its PIV credentialing (identity provider and authenticator provider). And the SBA utilizes both OMB MAX and Login.gov (federated authentication providers).

Traditionally, SBA guaranty loans are entered by SBA lenders. Borrowers do not directly enter guaranty loans into the SBA system. All borrowers must contact an SBA lender and an SBA lender has credentials to the SBA system.

SBA relies on each lender being vetted through the lending agreement process. After a lender receives an agreement, the lender receives a location id that is linked to the agreement. Lenders are then required to set up an authorizing official who approves access for their internal employees and partners to originate loans in the SBA system.

Credential Service Providers (CSP) offer a great benefit to confirming digital identities. Ideally, SBA would like to implement a CSP solution that would require all lenders to obtain credentials with a third party. SBA's lending community ranges from Fintech providers to rural community lenders. The diversity of SBA's lending ecosystem and their access to CSPs has been a hurdle to SBA requiring all lenders to use a CSP to originate SBA loans.

To implement a CSP requirement will require all SBA lenders of all sizes and in all communities to make a financial commitment to obtain credentials. The requirement may reduce the number of small community and rural lenders offering SBA services which would limit SBA products to more tech savvy and/or commercial lenders. SBA is sensitive to the needs of underserved communities and is reviewing options to reduce fraud while remaining accessible to all lending partners.

9. **What is the status of SBA's implementation of the 21st Century Integrated Digital Experience Act? Who within SBA is responsible for implementing the requirements of the Act?**

The SBA has made progress in a variety of the areas under the 21st Century IDEA Act. The Act calls for several focus areas that SBA is working towards but has yet to call complete. Specifically, SBA continues its routine modernizing and upgrading its SBA website to ensure the best possible initial digital experience with the SBA including an ongoing effort to digitize services and forms. This is a work in progress. SBA has been using the various legislative programs to upgrade to digital forms and wireframes when possible. The agency has been conducting extensive analysis on accelerating the adoption of easier to use e-signature systems to replace widely used digital signature utilities that do not offer an optimal customer experience. Finally, the Office of Field Operations was identified as a High Impact Service Provider and has been leading the agency's effort to develop a one-touch unified experience for all customers. The

agency has current efforts underway to decide on and adopt a standardized Customer Relationship Management platform for the entire agency that will enable improved customer experience across the board.

10. **Please highlight any recent successes in improving customer experience or any areas where SBA has made improvements that align with the goals of the 21st Century Integrated Digital Experience Act.**

The SBA launched several initiatives that address the overarching goals established under the 21st Century Integrated Digital Experience Act.

Modernize websites: SBA has modernized SBA.gov which is SBA's primary portal to the world. This modernization has included improvements to page layout, page design, navigation, currency of information, search capability, etc. New websites are responsively designed thereby enabling improved customer experience when these sites are accessed via mobile devices. Further, these new websites use SBA Connect, SBA's enterprise single sign-on solution so that citizens/customers do not need to remember multiple user ids and passwords. In response to the COVID-19 economic recovery initiatives, SBA launched several new websites such as the Lender Gateway, Find a Lender, Recovery Hub, etc. In the recent past, SBA also launched the Disaster Loan Upload Form, The Learning Center, beta Certify, EDMIS-NG, Open Data System, Developer Resources Site, Public Status Site, etc.

Digitize services and forms: SBA has several initiatives underway to digitize services and forms across various Program Offices. As an example, the Office of Human Resources Solutions is launching a new system for onboarding/offboarding employees with digital versions of a variety of forms and processes.

Standardize and Transition to Shared Services: SBA increased the adoption and use of enterprise shared services such as login.gov, a shared service provided by the General Services Administration (GSA) to enable SBA's enterprise wide single sign-on capabilities.

Finally, SBA has commissioned a United States Digital Services (USDS) team to conduct an assessment of the customer experience for all CARES Act related loan and grant programs. The wide-ranging assessment will yield a recommendation to unify this experience in the best way possible while digitally funneling incoming customer requests to the right services areas and enabling digital acceleration through process improvement, leveraging artificial intelligence, or implementing robotic process automation or chatbots to reduce human touch labor and to improve the entire experience.

11. **How is SBA leveraging technology investments to address the equity and inclusion gaps we are seeing in disadvantaged communities' ability to access and navigate SBA services and resources?**

To better reach small businesses, the SBA is launching the Community Navigator Pilot Program that will strengthen outreach to underserved businesses by partnering with organizations with established relationships and experience within their communities. The Community Navigator Pilot Program is designed to provide high quality support and assistance with pandemic relief programs and recovery services to small businesses and entrepreneurs. Programming will also focus on supporting communities that represent the top ten (10) languages spoken within the United States.

The support solution will provide a cloud-based software-as-a-service (SaaS) that will be pivotal for the proposed Community Navigator Information Management System (COMNAVS) solution simply because cloud services are much more cost efficient and scalable as compared to on-premises services. The new SaaS will meet the short time constraints of delivery, cloud-based services and meets the federal goal, provide a stable environment for Operation & Maintenance (O&M), and developer pool can accommodate for hiring to meet the short development timeline.

The COMNAVS is a data collection and management application that external stakeholders, including the SBA, will rely on to report on the effectiveness of its programs. When complete, COMNAVS will be a centralized web-based reporting system that embraces the hub-and-spoke "Navigator" Model. In addition, its database will serve to harmonize and homogenize data from a diverse cross-section of government and nonprofits regarding small and underserved business communities.

Starting with the business and business owner data collected by the COMNAVS system, we are defining methods of enriching this data with additional demographic datasets, with the goal of harmonizing and deeply understanding the program's reach into underserved communities and informing program equity goals.

Our data enrichment strategies are considering additional datasets from other SBA programs, datasets from other agency sources like the Census Bureau, Department of Labor, and SAM.gov, as well as external 3rd party datasets. Successful methods for enriching demographic data piloted by this project will be considered for other SBA programs, and for interagency data enrichment projects.

When policy and legislation permit, SBA sets aside funding for disadvantaged communities to ensure access to small lending products. SBA's current financial systems have ample capabilities to establish dedicated funding for equity or inclusion gaps.

I appreciate the opportunity to provide additional information about SBA's information security, its ability to establish and use an MGT Act-authorized IT Working Capital Fund, protection against fraud, and other issues. If you and your staff have further questions, please feel free to contact Kevin Wheeler in our Office of Congressional and Legislative Affairs at (202) 941-5869.


Sincerely,

Keith Bluestein
Chief Information Officer