IT Acquisition Advisory Council (IT-AAC)
904 Clifton Drive, Alexandria, VA 22308
(703) 768-0400 (v) (703) 765-9295 (f)

IT Acquisition Advisory Council

January 25, 2022

Mr. Charles P. Rettig
Commissioner
United States Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

RE: IT-AAC Concerns about IRS Forcing Citizens to Engage with a For-Profit Commercial Entity for Identity Verification & Online Access to IRS & Associated Security & Privacy Risks

Dear Commissioner Rettig:

I am reaching out to you today on behalf of the leadership of the Information Technology Acquisition Advisory Council (IT-AAC) to express serious concerns about a decision by the United States Internal Revenue Service to increase the risk to American's personal information by requiring citizens to engage with a commercial for-profit entity in order to complete an identity verification process necessary to gain access and interact with the IRS. Not only does this decision create an unprecedented personal privacy issue, but it also allows for the potential of personally identifiable information being harvested and then utilized for commercial for-profit purposes.

The difference between requiring citizens to provide personal information that is housed and maintained by a government entity versus requiring citizens to provide such critical information to a for-profit commercial enterprise is potentially consequential. In addition, the reported requirements for completing the identity verification process would seem to potentially disadvantage many citizens who may not own or have access to the required advanced technology.

https://krebsonsecurity.com/2022/01/irs-will-soon-require-selfies-for-online-access/

https://www.fastcompany.com/90714538/irs-login-makes-you-take-a-selfie-for-this-security-company-youve-never-heard-of

https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper

Citizens should be able to rely on United States Government departments and agencies to execute the highest level of protection against exploitation and identity theft by deploying secure, proven methodologies for access and engagement. Given the well publicized growth of security compromises, with reported breaches at multiple federal departments and agencies, including the IRS, the decision to require citizens to engage with a commercial for-profit company to verify identity, including a "selfie" as

a condition for gaining access to engage with the IRS is most troubling. As you are aware, there are those that question the reliability and dependability of facial recognition technology for identity verification purposes.

It is particularly concerning when the IRS has the current option to utilize a government sponsored Identity Verification Platform, (www.login.gov) that is available and currently utilized by multiple federal departments that engage directly with citizens and have custodial responsibility for protecting personally identifiable information. What would possibly cause the IRS to make a decision to deploy an option that requires citizens to provide sensitive information to a 3rd party for-profit commercial enterprise when a government established platform is available raises questions that are worthy of much greater scrutiny and investigation. The public deserves answers to this legitimate question particularly when login.gov is a viable option currently being utilized and a platform where the government is the steward of the personal information that citizens provide as opposed to a 3rd party commercial for-profit company. The public relies on government to affirm trust and confidence. Privacy and protection of personal information is paramount to a secure engagement.

By the way, and as you are likely aware, many of these same questions have been raised for some time when it was revealed that ID.ME was the beneficiary of a series of sole source contract awards in several states to provide fraud detection and prevention capabilities associated with applicants seeking eligibility for unemployment insurance benefits claims that surged during the pandemic. Disappointing results have been reported in a number of those states, including some of the issues raised in this letter.

The failure by states to follow requirements for full and open competition in the procurement process that obligates taxpayer funds has prompted the United States Department of Labor to pursue a more comprehensive approach on behalf of all states that leverages capabilities from established and proven providers of identity verification services. That process was conducted in a full, open, and transparent manner that leveraged market-driven innovation and best value solutions and that values security and privacy on behalf of all impacted stakeholders.

In a number of those states, the same issue of the requirement for benefit applicants to establish accounts directly with ID.ME, a 3rd party, commercial for-profit company, rather than with a government sponsored site, thereby providing ID.ME with access to the personally identifiable information of many vulnerable citizens applying for unemployment insurance benefits. There are currently ongoing reviews at the state and federal level as to performance, capability, and security as well as the issue of harvesting personal information provided by citizens that may then be utilized for commercial purposes.

https://californiaglobe.com/articles/monetizing-data-the-edd-id-me-and-the-unemployed-of-california/

https://shop.id.me/

IT-AAC (www.it-aac.org) is a non-profit, public-private partnership that was established in 2007 at the urging of members of the United States Congress and senior leadership at the Department of Defense and is broadly recognized as an honest broker "do tank" that has been instrumental in helping federal departments and agencies across the defense, intelligence, and civilian communities solve some of the most difficult challenges facing government.

IT-AAC and its team of experienced senior executive professionals from government and industry operate in the public interest to support and assist federal departments and agencies identify and meet the challenging issues of IT modernization, digital transformation, cloud computing implementation, acquisition reform, cybersecurity protection and resilience, supply chain risk management, and much more. A foundational component of the IT-AAC effort is to insure that the government adheres to the requirements for full and open competition in procurement at the federal and state level of government. Avoidance of vendor bias or directed procurement outcomes to the exclusion of other qualified, eligible, and capable providers is an essential measure of maintaining public trust, while also providing end users with access to market-driven innovation and best value solutions that support the mission, the end user, and the American taxpayer.

The referenced matter appears to be an egregious violation of public trust by creating serious security and privacy risk, disenfranchising a significant number of citizens, and failing to leverage existing capabilities such as login.gov, opting instead to proceed with a single commercial for-profit provider who may in fact exacerbate security and privacy challenges. There are also many questions about the acquisition selection process itself that appears to have been a sole source contract award that did not provide an opportunity for established and proven providers with a track record of success in identity verification along with online fraud detection and prevention to even be considered through a full and open competition process as required by federal law, regulation, and executive branch guidance.

Accordingly, there are a number of questions that arise when reviewing available information.

- Why was a decision made by leadership at the IRS / Treasury to utilize a 3rd part commercial for-profit company as the access gateway for US citizens desiring to engage with the IRS as opposed to utilizing an already existing access gateway created by the government that utilizes innovative technology to provide the plumbing for the site while the government maintains the stewardship of the personal information provided, www.login.gov and states on the home page:

  # The public's one account for government.

  Use one account and password for secure, private access to participating government agencies.

- What was the process utilized to select ID.ME as a 3rd party commercial for-profit access gateway for the IRS? What contractual instrument was used? When was that contract solicited? Was the contract RFP competed with full and open competition? Was the solicitation publicized and shared across the community of proven identity verification and fraud prevention

organizations? Was there a published set of technical requirements that were researched and vetted by security professionals? Was there a technology bake-off to allow for an evaluation of capabilities across the identity verification and fraud prevention community of providers who may have been qualified and eligible to fulfill the technical and operational requirements established?

- Why did the IRS not consider offering citizens the option to utilize the government-sponsored login.gov site for access and engagement? Given that the United States Social Security Administration offers login.gov as an option for citizens, it is difficult to fathom why the IRS would not at least provide that option for citizens.

- What restrictions are contractually articulated and legally enforceable that would prevent the 3rd party commercial for-profit provider from reusing the acquired personally identifiable information that is required when establishing an account that is a prerequisite for access, not just the biometric, for commercial use? This is especially relevant as ID.ME has previously confirmed that their business model includes use of such accumulated personal data for commercial and profit making purposes.

  This becomes particularly relevant when the ID.ME CEO publicly states that the company loses money on contracts with government. That should raise an immediate red flag to understand and identity the alternate source of revenue necessary to maintain profitability. A for-profit company is not in business to lose money.

  The Privacy Statement itself raises questions as it establishes conditions for sharing the personally identifiable information that will be collected and stored for up to 7 years, including:

  We may share your information with Authorized Third Party Service Providers.

  We provide certain services and products of the Website through Third-Party service providers. These "Third-Party Service Providers" perform functions on our behalf, such as sending out and distributing our administrative and promotional emails. We may share your Personally Identifiable Information with such Third-Party Service Providers to remove repetitive information on customer lists, analyze data, provide marketing assistance, provide search results and links, process credit card payments, operate the Website, troubleshoot, and provide customer service. We may also collect personal information from individuals and companies ("Affiliates") with whom we have business relationships and may share your information with Third-Party Service Providers to accomplish our administrative tasks. However, we do not grant these entities any rights to use, and contractually restrict them from using, any information for any purpose other than providing services to us and to you. ID.me shall never sell your information to any entity for any reason.

Since this matter has become public information, IT-AAC recognizes that a number of interested parties have publicly expressed concerns about these serious issues. Those parties have included Members of Congress, information security professionals, the ACLU, other privacy advocates, and even private citizens that have attempted to utilize ID.ME.

The IT-AAC leadership recommends that the leadership at the United States Internal Revenue Service and the United States Department of the Treasury promptly review these matters and take prompt and decisive steps to advance a course correction to better ensure security, privacy, and the protection of citizen's personal information while also insuring a process that provides reasonable and predictable access for all citizens and is not dependent on access to advanced technology. In addition, the selection of providers to support mission activities should rely on a fair, open, and transparent acquisition process that adheres to requirements in federal law, regulation, and executive branch guidance for full and open competition necessary to maintain public trust.

The IT-AAC leadership applauds the efforts at IRS to join with other federal departments and agencies to address the challenges of online fraud with a robust identity verification process. The development of www.login.gov is a creative approach to leveraging innovation and best practices to provide access in a trusted manner that advances public confidence in its engagement with government across all departments and agencies. With login.gov, the government collects, own, controls, and protects the personal information provided by citizens. The IRS should immediately consider leveraging www.login.gov as the preferred approach for citizens to interact with the IRS.

Thank you in advance for your consideration of this outreach. Please do not hesitate to contact us if you have any questions or require additional information. Given the timing and urgency of this matter, we look forward to hearing back from you as expeditiously as possible and hopefully within the next two weeks at least. Please do confirm receipt of this correspondence.

Sincerely,

Robert B. Dix, Jr.
Senior Vice President- Strategy & Public Policy
Information Technology Acquisition Advisory Council

bob.dix@it-aac.org
703-975-6633

cc.

Mr. Richard Delmar
Deputy Inspector General
United States Department of the Treasury

Mr. J. Russell George
Treasury Inspector General for Tax Administration
United States Department of the Treasury

The Honorable Robin Carnahan
Administrator
United States General Services Administration

Ms. Nancy Sieger
Chief Information Officer
United States Internal Revenue Service

Mr. Tony Arcadi
Chief Information Officer
United States Department of the Treasury

Ms. Jessica Lucas-Judy
Director
United States General Accountability Office

Ms. Dawn B. Simpson
Director
United States General Accountability Office

Mr. David Hinchman
Acting Director
United States General Accountability Office

The Honorable Ron Wyden
Chairman
United States Senate Committee on Finance

The Honorable Mike Crapo
Ranking Member
United States Senate Committee on Finance

The Honorable Sheldon Whitehouse
Chair
Subcommittee on Taxation & IRS Oversight
United States Senate Committee on Finance

The Honorable John Thune
Ranking Member
Subcommittee on Taxation & IRS Oversight
United States Senate Committee on Finance

The Honorable Richard Neal
Chairman
Committee on Ways & Means
United States House of Representatives

The Honorable Kevin Brady
Ranking Member
Committee on Ways & Means
United States House of Representatives

The Honorable William Pascrell
Chairman
Subcommittee on Oversight
Committee on Ways & Means
United States House of Representatives

The Honorable Mike Kelly
Ranking Member
Subcommittee on Oversight
Committee on Ways & Means
United States House of Representatives