American Bankers Association. BETTER IDENTITY COALITION U.S. Chamber of Commerce Technology Engagement Center CHIME College of Healthcare Information Management Executives Cybersecurity Coalition

eta ELECTRONIC TRANSACTIONS ASSOCIATION ITRC IDENTITY THEFT RESOURCE CENTER naphsis TECHNET THE VOICE OF THE INNOVATION ECONOMY SIIA

June 12, 2023

To: Kemba Walden, Acting Director, Office of the National Cyber Director
Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology

Dear Ms. Walden and Ms. Neuberger:

We were thrilled to see the Biden-Harris Administration's new National Cybersecurity Strategy (Strategy) flag digital identity as an area where further government action is needed to stem the tide of identity-related cyber attacks. The Administration's attention to this issue is welcome and appreciated. We write today to offer our thoughts on how the White House can address America's digital identity challenges in the implementation plan for the Strategy.

Our organizations represent a diverse array of interests and views, but we are united in our resolve that concrete action is needed to address deficiencies in digital identity infrastructure. Year after year, we have seen the same organized criminals and hostile nation-states exploiting the same core weaknesses in digital identity infrastructure to steal billions not just from governments, but also banks, health care, retailers, fintech services, and cryptocurrency exchanges. It is an anomaly when a major cybersecurity incident happens and a compromise of identity does not provide the initial attack vector; these attacks have impacted nearly every critical infrastructure sector.

As the strategy rightly noted:

> *Today, the lack of secure, privacy-preserving, consent-based digital identity solutions allows fraud to flourish, perpetuates exclusion and inequity, and adds inefficiency to our financial activities and daily life. Identity theft is on the rise, with data breaches impacting nearly 300 million victims in 2021 and malicious actors fraudulently obtaining billions of dollars in COVID-19 pandemic relief funds intended for small businesses and individuals in need. This malicious activity affects us all, creating significant losses for businesses and producing harmful impacts on public benefit programs and those Americans who use them. Operating independently, neither the private nor public sectors have been able to solve this problem.*

With nearly 300 million victims of identity theft, that means the majority of Americans have been victimized, with nation-state sponsored hackers and organized crime rings benefitting. The Administration recognized the need for enhanced protections and identity crime victim support in its March 2, 2023, *Pandemic Anti-Fraud Proposal,* which focused on fraud in government benefits. Now is the time to build on that with a broader proposal which can protect Americans from identity-related cybercrime in every sector and ensure that those who are victimized can get direct assistance.

One issue that has failed to get enough attention: identity not only provides the initial attack vector in cybersecurity incidents, but identity is also what enables adversaries to monetize most attacks. In that the primary target of many attacks – personal data – can be easily monetized by adversaries because of our long reliance on systems where knowledge of personal data allows an adversary to impersonate an individual, allowing adversaries to steal money and launch additional attacks. Often, the individuals whose identities have been compromised are unaware their personal information has been misused, leaving them with few resources to learn the scope of the crime as well as recover and restore their identities.

By shifting to more robust digital identity solutions, America can prevent future identity-driven attacks and sharply curtail the ability of adversaries to monetize stolen data – thus removing a key incentive for those adversaries to launch attacks.

In 2016, the bipartisan Commission on Enhancing Cybersecurity flagged this issue, and proclaimed that *"the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021."* Sadly that date has come and gone, but there is no time like the present to address this problem. As the Administration now turns to the implementation plan for the Strategy, we urge you to embrace three priorities:

1. **Launch a White House Task Force to accelerate the availability of tools that can guard against identity-related cybercrime.**

   As the Strategy notes, *"The Federal Government will encourage and enable investments in strong, verifiable digital identity solutions that promote security, accessibility and interoperability, financial and social inclusion, consumer privacy, and economic growth."*

   The most impactful thing the Federal government can do here is to launch a "timeboxed" effort to coordinate activities among authoritative issuers of identity credentials to help all issuers create digital counterparts to the paper and plastic credentials that they issue today.

   White House leadership is essential here, in that authoritative issuers of identity are split between the Federal, state, and local level in the U.S. – and without an effort to coordinate a standardized approach among all those issuers, progress will lag and we will miss a key opportunity to guide all issuers toward solutions that set a high bar for security, accessibility, interoperability, and privacy.

   Voluntary solutions could take the form both of new digital credentials, such as mobile Driver's Licenses (mDLs), digital passports, and birth certificates, as well as attribute validation services that provide a "yes/no" answer as to whether identity data submitted to a party matches what is on file. The latter is particularly helpful in stopping synthetic identity fraud, as well as in helping improve inclusion.

   The benefits of digital credentials are straightforward: rather than force Americans to go through a new online process that replicates the in-person identity proofing process they already went through to get a driver’s license or state ID card, Americans should instead be given the opportunity to reuse a high assurance credential they already have.

A number of states have started to introduce mDL apps that allow someone to effectively prove their identity with a digital app rather than a plastic ID card. Congress passed a law in 2020 giving physical and digital IDs legal equivalency under the REAL ID Act. However, early use cases are focused on in-person applications such as proving identity to the Transportation Security Administration (TSA) at airports, whereas the most urgent problems mDLs can solve are in the digital world.

The Biden Administration has driven tremendous cybersecurity improvements in the “authentication layer” of identity, by introducing new requirements in the Federal Zero Trust Strategy for agencies to use possession-based authentication rather than knowledge-based authentication. Solving online identity proofing will require the same shift – getting people away from knowledge-based solutions to ones that create a digital equivalent to the secure plastic ID cards they have in their wallets.

We believe that a new White House task force which brings in key stakeholders from Federal, state, and local agencies, as well as industry and civil society, can craft an approach to close the gap between physical and digital credentials over a one-year period.

Key duties for the task force should include:

- Developing a plan of action for Federal, State, and local agencies to close the gap between physical and digital identity credentials through the development of digital versions of existing physical identity credentials, in a way that is secure, protects privacy, prioritizes equity and accessibility, and is interoperable.

- Determine whether there are any restrictions with respect to the abilities of agencies to offer new digital identity solutions, as well as whether any changes in statutes, regulations, or policies are needed to address these restrictions.

- Identify what funding or other resources will be needed to support agencies at all levels of government to support the rollout of digital credentials, and recommend funding models such as grants, fee-based models, or other approaches.

- Determine what standards and best practices are needed to ensure that any new solutions here set a high bar for security, privacy, equity, and inclusion.

- Explore ways to ensure that the emergence of robust digital identity solutions does not exacerbate existing inequities with people who are not able to easily get a physical ID today.

- Identify the role that industry solutions can continue to play in a digital identity market that features enhanced government offerings – including hybrid models where Americans may choose to leverage private sector digital wallets or other offerings, as well as ways in which industry solutions can address other components that are not inherently governmental.

2. **Prioritize work at the National Institute of Standards and Technology (NIST) on identity and attribute validation services – with a focus on developing a Digital Identity Framework of standards and best practices to help agencies at all levels of government establish attribute validation and other digital identity services in a way that is standardized, and sets a high bar for security, privacy, and equity.**

   As the Strategy noted, last year's CHIPS and Science Act directed NIST to expand its work in digital identity to also include new guidance to Federal, State, and local governments seeking to provide identity and attribute validation services.

   This is a new work area for NIST; today NIST Digital Identity Guidelines (SP 800-63) tell government agencies how to determine if someone is who they claim to be online, but they do not help agencies that want to stand up their own digital identity services that might let an individual ask an agency who already issued them a credential to vouch for them in the online world.

   This latter type of service is incredibly important as we look to close the gap between the nationally recognized, authoritative credentials that are issued today in the physical world and the lack of any counterpart to them online.

   Note that NIST recently published a draft Identity and Access Management Roadmap that outlines some of its plans at a high level, but the roadmap does not include any dates or deadlines.

   With authoritative government issuers of identity divided between across Federal, State and local agencies, it will be important to ensure that every agency playing a role in digital identity services follows standards that set a high bar for security and privacy, and ensure interoperability of solutions. NIST should be tasked with developing and periodically updating a Framework of standards, methodologies, procedures, and processes as a guide for Federal, State, and local governments to follow when providing services to support digital identity or attribute validation. We believe one year is an appropriate deadline.

   As part of this, we suggest that the White House directs NIST to more specifically address language in the Strategy concerning mDLs. The Strategy was oddly neutral on this topic, stating *"Acknowledging that States are piloting mobile drivers' licenses, we note and encourage a focus on privacy, security, civil liberties, equity, accessibility, and interoperability."*

   We believe that mDLs, if appropriately designed, may be the single best way to give Americans tools that they can use to protect themselves from identity thieves. However, we believe it is important that privacy, security, civil liberties, equity, accessibility, and interoperability are not only "encouraged," but that the government takes proactive steps to ensure they are all achieved.

Specific direction to NIST to address these issues in the context of mDLs and other identity and attribute validation services is the best way to get there. We note that NIST's National Cybersecurity Center of Excellence (NCCoE) has announced its intentions to launch a project to "Accelerate Adoption of Digital Identities on Mobile Devices" – this project can serve as the basis of this task.

3. **Launch an effort to document the ways that investments in digital identity infrastructure can generate budget savings.**

   In his 2023 State of the Union Address President Biden noted, *"For every dollar we put into fighting fraud, taxpayers get back at least ten times as much."*

   We wholeheartedly agree – but there has not been any formal effort to estimate the budgetary impact of investments in digital identity infrastructure, and the lack of any formal documentation of potential cost savings has held back legislative and executive branch efforts to improve digital identity.

   That said, there are some notable studies and figures that make clear that digital identity investments not only pay for themselves, but will generate notable economic benefits:

   - A 2019 McKinsey study estimated that the United States could unlock the economic value of 4% GDP with investments to drive digital ID adoption – driven by a combination of reductions in cybercrime and increased efficiency, as well as the ability of American businesses and government to offer new, high-trust services online.

   - A 2013 NIST study showed that the IRS alone could save northward of $300 million annually with improved digital identity solutions.

   In support of the Strategy's plans to *"encourage and enable investments in strong, verifiable digital identity solutions that promote security, accessibility and interoperability, financial and social inclusion, consumer privacy, and economic growth,"* the White House should launch an effort to formally document the estimated potential savings and overall economic benefit of investments in digital identity infrastructure.

We appreciate the Administration's consideration of our request, and offer our organizations' collective expertise should assistance be helpful as the implementation plan is crafted.

Sincerely,

American Bankers Association (ABA)
Better Identity Coalition
College of Healthcare Information Management Executives (CHIME)
Cybersecurity Coalition
Electronic Transactions Association (ETA)

Identity Theft Resource Center (ITRC)
National Association for Public Health Statistics and Information Systems (NAPHSIS)
Software & Information Industry Association (SIIA)
TechNet
U.S. Chamber of Commerce Technology Engagement Center (C_TEC)