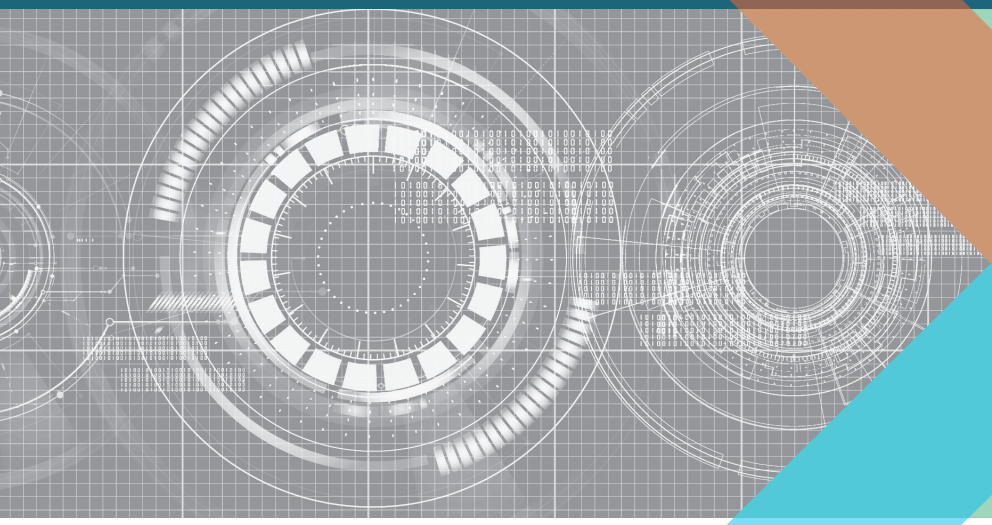
BETTER IDENTITY COALITION



Better Identity at Five Years:
An Updated Blueprint for Policymakers

January 2024

INTRODUCTION

Five years ago, the Better Identity Coalition published *Better Identity in America: A Blueprint for Policymakers* in response to significant questions from both government and industry about the future of how the United States should address challenges in remote identity proofing and other key issues impacting identity and authentication.

The Blueprint outlined five key initiatives that, taken together, if implemented and funded, would solve the majority of our challenges in the digital identity space.

As this report details, America has made mixed progress on the Blueprint – in some cases embracing the recommendations and in doing so, making noteworthy progress. In other cases, we are stalled – and with it, rudderless in efforts to counter organized criminals and hostile nation-states looking to exploit compromised identities to steal money and data.

Since the Blueprint was published, however, much has changed:

- America lived through a global pandemic that made many in-person transactions impossible for more than a year – and adversaries swept in to exploit the chaos of our shift to all-digital transactions by using compromised digital identities to steal hundreds of billions of dollars from government and the private sector.
- We have also seen the rise of new, more sophisticated attacks on identity powered by generative AI that, if unaddressed, threaten to push losses from identity-related cybercrime to new levels and undermine confidence in our increasingly digital economy.
- Every peer country in the world has either created robust digital identity infrastructure or has launched a national initiative to do so; the U.S. stands alone among its peers in lacking a comprehensive initiative.

This report assesses our progress on each of the Blueprint's five key initiatives and also updates the Blueprint to focus on meeting future challenges.

TABLE OF CONTENTS

REPORT CARD

In 2018, the Better Identity Coalition outlined five key initiatives for policymakers to address digital identity challenges in America. Government has made great progress on some of these initiatives and struggled with others - below we assess progress on each.

Initiative	Grade	Progress/Comments
1. Prioritize the Development of Next-Generation Remote ID Proofing & Verification Systems	D	Two successive Administrations have effectively ignored this issue; 2023's National Cybersecurity Strategy included language on digital identity only to see it dropped in the Strategy's implementation plan. Current Federal efforts are focused on trying to solve remote ID proofing solely for government benefits programs or other "one off" sector-specific use cases, rather than focusing on addressing shortcomings in the overarching digital identity infrastructure and enabling cross-sector solutions. We lack any vision of what "good" looks like with digital identity proofing or a strategy on how to get America there. In total, more than $1 billion has been invested in addressing sector-specific ID proofing challenges that could have been better spent on multi-use infrastructure. On the bright side, efforts underway at the National Institute of Standards and Technology (NIST), the Department of Homeland Security Science & Technology Directorate (DHS S&T), and the Transportation Security Administration (TSA) are starting to put some foundational elements in place to support better identity solutions. Congress directed NIST to launch important work here as part of the 2022 CHIPS and Science Act.
2. Change the Way America Uses the Social Security Number (SSN)	B	Policymakers understand that the SSN is used as both an identifier and an authenticator – and that its use as an authenticator poses the biggest risk. It is critical that the SSN continue to be used as an identifier and not an authenticator. The value of government services that can validate SSN data to aid in identity proofing and prevent fraud is now widely embraced – though SSA is not yet providing these services to every sector – and SSA efforts to support the financial services sector are faltering.
3. Promote and Prioritize the Use of Strong Authentication	A	The White House and the Cybersecurity Infrastructure & Security Agency (CISA) have led robust efforts to promote multifactor authentication (MFA) adoption nationally and have leaned forward to drive the use of phishing-resistant MFA, like FIDO, which can stand up to attacks that compromise legacy MFA.
4. Pursue International Coordination and Harmonization	B-	Treasury led the effort to create robust Digital Identity Guidance in the Financial Action Task Force (FATF); NIST has led U.S. efforts in the Trade and Technology Council (TTC). The G7 highlighted the importance of digital identity in building trust and sharing best practices as well. But at a time when our peers are all advancing robust digital identity initiatives, the lack of a U.S. strategy means we are increasingly excluded from conversations.

Initiative	Grade	Progress/Comments
5. Educate Consumers and Businesses About Better Identity	B-	There have been significant education efforts from CISA and other agencies on the MFA front. However, the lack of any U.S. initiative on remote identity proofing means education on best practices for consumers and businesses on that front is almost non-existent. Likewise, identity theft victims continue to face a confusing landscape when it comes to knowing how and where to get help.

Identity by the Numbers: The Cost of Outdated Solutions

- 1,802 data compromises reported in 2022 – the second highest number ever of compromises reported in a single year, impacting roughly 422 million individuals primarily due to cyberattacks.[1]
- The Treasury Department's Financial Crimes Enforcement Network (FinCEN)[2] revealed that an estimated $212 billion in transactions reported in 2021 Suspicious Activity Reports were tied to failures in the identity verification process.[3]
- The Government Accountability Office estimates that the amount of fraud in unemployment insurance (UI) programs during the COVID-19 pandemic was between $100 billion and $135 billion.[4]
- Synthetic identity fraud, where fraudsters create an artificial identity out of multiple pieces of real and fabricated data, resulted in $20 billion in losses for U.S. banks and financial institutions in 2020.[5]
- 915,000 U.S. children were victims of identity fraud in the past year, costing an average of $1,128 for a single household—$752 for the fraud itself and $376 out-of-pocket to resolve the fraud—while spending 16 hours on resolution overall.[6]
- The Federal Trade Commission reported a 3,000% increase in identity theft complaints related to compromised credentials, such as stolen government benefits in 2020.[7]
- More than 80% of confirmed breaches are related to stolen, weak, or reused passwords.[8]
- In 2022 more than 24 billion passwords were exposed to hackers.[9]
- Spending on Know Your Customer (KYC) and Anti-Money Laundering (AML) technology and operations by financial institutions worldwide will reach $58.0 billion in 2023.

Is the Policy Blueprint Still Relevant?

One of the questions we asked our members when crafting this report was "Is our 2018 Policy Blueprint still relevant?" Five years is a long time in the security and technology space, and changes in both technology and threats mean that ideas from half a decade ago may no longer be relevant.

In the case of the Blueprint, however, the answer is "Absolutely." For the issues that have been ignored, the need for action is greater than ever. And for those issues where government has made progress, more work still needs to be done.

That does not mean that the Blueprint and its associated Action Plan should stay stagnant. We have updated the Action Plan that supports the Coalition's five key initiatives to reflect work done to date, as well as address new concerns, such as the rise of attacks on identity and authentication systems enabled by the increasing availability of AI-powered tools like deepfakes. Going forward, this Action Plan provides a comprehensive set of recommendations for the United States to get ahead of digital identity challenges.

Amidst Some Progress, More Must Be Done To Combat Existing and Evolving Threats

The Coalition's original Policy Blueprint was crafted in the wake of the 2017 Equifax breach, which highlighted the limitations of our current identity infrastructure. The theft of sensitive personal data from more than 147 million people – including supposedly "secret" data that had been used by consumers and businesses to verify identities online – made clear that some of our legacy systems that relied on knowledge-based solutions to verify identity were no longer good enough.

Launched in July 2018, the Coalition's Policy Blueprint won instant bipartisan support, and generated a number of Congressional hearings examining different aspects of America's digital identity challenges. Out of those hearings, new bipartisan legislation was introduced – the Improving Digital Identity Act[10] – that embraced core ideas from the Blueprint and would direct the White House to coordinate action among Federal, state, and local officials to drive a nationwide approach to addressing key deficiencies in digital identity infrastructure.

The Improving Digital Identity Act was passed by key House and Senate Committees in both 2022 and 2023, but passage of the bill has stalled, and the bill remains in political limbo.

One key accomplishment: as part of the 2022 CHIPS and Science Act, Congress incorporated the section of the Improving Digital Identity Act that directed NIST to create new guidance for Federal, state, and local agencies when creating new identity or attribute validation services. While not accompanied by funding, this new language embraced a core priority from our 2018 Blueprint and turned it into law.

Additionally, Congress in 2020 enacted the REAL ID Modernization Act, which modernized the definition of "REAL ID compliant" state driver's licenses and state identification cards to make clear that these credentials were no longer limited to a physical card form factor. The law made clear that a "REAL ID" could also include credentials *"stored or accessed via electronic means, such as mobile or digital driver's licenses, which have been issued in accordance with regulations prescribed by the Secretary,"* such as mobile Driver's Licenses (mDLs). Passage of the law was a step forward, but as we detail in this paper, we believe DHS has erred in prioritizing in-person use cases of mDLs, such as clearing a TSA checkpoint, over remote ID proofing use cases, such as proving identity to open a bank account.

In the Executive Branch, both the Trump and Biden Administrations have largely failed to address identity verification challenges strategically. Instead, the focus has been on "one-off" sector-specific use cases, rather than a holistic approach that addresses deficiencies across sectors. This is in spite of a 2019 declaration by the Department of Homeland Security that identity is one of 55 "National Critical Functions" - defined as "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[11]

The Biden Administration's 2023 National Cybersecurity Strategy included language calling for the government to take a more strategic approach to digital identity, only to skip over the issue in the Strategy's implementation plan. A long-rumored identity theft executive order is reportedly limited solely to addressing ID theft in government benefits programs, rather than taking a broader approach to protect Americans from identity theft in every sector.

While progress on digital identity from Congress and the Administration has stalled, identity-related cybercrime continues to soar, and the emergence of new attacks on digital identity leveraging AI-powered deepfakes and other advanced attacks suggests the problem is about to get much worse. A strategic plan is needed now to address core deficiencies in America's digital identity infrastructure – in a way that not only enhances security, but also focuses on privacy, security, civil liberties, equity, accessibility, and interoperability.

Investments Have Been Made – But Not the Right Ones

Our 2018 Policy Blueprint called for investing $1 billion over five years to jumpstart the creation of modern digital identity infrastructure, focusing on closing the "identity gap" between the nationally recognized, authoritative credentials governments issue at the federal, state, and local level – and the lack of any digital counterparts to those credentials that people can use to prove their identity online. While some policymakers cringed at the size of this number, the fact is that the Federal government has spent more than $1.1 billion on identity verification in recent years – most of it on siloed programs that are only for government services, and that cannot be used across other sectors. This includes:

- $500 million allocated for dozens of new identity verification contracts across the federal government.[12]
- $187 million to Login.gov, which is focused solely on identity for government services.
- $377 million to the U.S. Labor Department for state grants to improve unemployment insurance program integrity – including identity verification.
- $53 million for development and administration of the electronic Consent-based Social Security Verification (eCBSV) system. (note: eCBSV is the one industry-focused program; industry is reimbursing SSA for these costs)
- $45 million by the Internal Revenue System to stand up the Secure Access Digital Identity (SADI) program.

While some of these investments have helped to address sector-specific challenges – ID verification needs in public sector programs – they have ignored the bigger issue that presents challenges in nearly every sector: the "identity gap."

Rather than build siloed solutions, the government should be investing more broadly in robust, privacy-preserving digital identity infrastructure. The goal should be to close the gap between physical and digital credentials, so that anybody can ask a state or federal agency who issued them a credential to validate that information and "vouch" for them online.

Where digital credentials are emerging, government is getting the priorities wrong.

Several states have started issuing mobile driver licenses (mDLs) – digital versions of the ubiquitous plastic card 90% of U.S. residents carry. The primary use case for these mobile IDs now is enabling in-person use cases – such as letting someone use their phone instead of their driver's license when going through an airport security checkpoint or entering a bar. These are "nice to have" but viewed against the backdrop of the epidemic of massive identity fraud in online applications, they should be a second-tier priority.

By prioritizing mDL solutions that can help easily and securely identity proof consumers online, states can address the most critical shortcoming in America's digital identity infrastructure and stop billions of dollars in identity-related cybercrime and fraud each year.

This is not to diminish the importance of mDL standards like ISO 18013-5 which focuses on in-person use cases. The TSA and others have said they will not accept mDLs that do not adhere to this standard, and thus states should embrace it in any mDL offering. However, Federal and state agencies need to focus first on how mDLs can address online identity fraud and identity proofing challenges. Had government followed the Coalition's recommendations on this front five years ago – rather than defer to the International Standards Organization (ISO) to get around to the remote identity proofing use cases when it felt the time was right – America could be in a very different place with regard to digital identity infrastructure.

Progress is on the horizon with standards for how to use mDLs online expected in 2024. NIST and the National Cybersecurity Center of Excellence (NCCoE) are kicking off a project for online use cases for mDL with a variety of identity vendors and relying parties. The project plans to develop a reference implementation of the digital identity standard with outcomes of this project potentially resulting in contributions to the ISO standard. The outcomes of this project will be leveraged by organizations to align their digital identity goals towards a standardized, secured, and trustworthy digital identity.

These efforts that are underway are helpful, but in total, they are too small and too slow, relative to the scope of the problem. America lacks an overarching strategy to define what "good" looks like in digital ID or a plan to get us there. The longer we delay, the more problems tied to inadequate digital identity infrastructure will fester. And the greater the risk that solutions that do emerge will fall short when it comes to privacy, security, civil liberties, equity, accessibility, and interoperability.

Revised Action Plan: A Path to Better Identity

Our 2018 Policy Blueprint included not just five key initiatives, but a 17-point Action Plan for the Federal Government to deliver better digital identity solutions. This section updates that plan – both to reflect work that has already been achieved since 2018, as well as to address new challenges in digital identity that have emerged since the original Blueprint was published. Note that we include a complete review of the 2018 Action Plan in an Appendix to this report.

Initiative 1: Prioritize the development of next-generation remote identity proofing and verification systems. Adversaries have caught up with the systems America has used for remote identity proofing and verification. Next-generation solutions are needed that are not only more resilient, but also more convenient for consumers.

1. Establish a White House led task force charged with bringing Federal, state, and local agencies together to develop a coordinated plan to close the gap between physical and digital credentials in a way that promotes security, privacy, equity, and interoperability. The White House can do this on its own today; if they do not, Congress can direct them to do so by passing the Improving Digital Identity Act.
2. Direct NIST and DHS to jointly accelerate the development of standards and guidance to states to enable them to launch remote identity proofing applications for mDLs and other digital credentials. As part of this, direct both agencies to prioritize digital use cases over in-person use cases in its work on mDLs.
3. Create a new five year, $200 million per year grant program to support states in their migration to being digital identity providers. Dollars would be tied to adherence to forthcoming NIST guidance for Federal, state, and local agencies for creating new identity and attribute validation services and would be used to support the modernization of legacy identity infrastructure to support digital solutions. 10% of grant dollars should be used to support "identity inclusion" efforts in states, ensuring that as we advance digital identity efforts, we do not leave behind those who cannot easily get foundational physical IDs today.
4. Open up SSA's electronic Consent Based Social Security Number Verification (eCBSV) system to cover account opening use cases for government services, demand deposit accounts, background checks, and other use cases where an individual might have a need to ask SSA to "vouch" for them – by validating the information SSA has on them in SSA databases.
5. Address fundamental challenges tied to eCBSV's current pricing model by extending SSA's cost recovery period to recover dollars expended to create the eCBSV system.
6. Establish additional consent-based attribute validation services at other agencies that hold authoritative identity information on Americans, such as the IRS, State Department, and U.S. Postal Service.

7. Direct the State Department to offer Americans the option of getting a digital counterpart to the paper passport which, like mDLs, can be stored securely in their smartphone; ensure State prioritizes the use of digital passports for online use cases rather than in-person ones.
8. Pass the POST ID Act, which authorizes the United State Postal Service to offer in-person identity verification and related services for government agencies and the private sector.
9. Convene a Digital Identity Task Force led by Treasury and including regulators in the Federal Financial Institutions Examination Council (FFIEC). This task force will, focus on exploring how government policy can drive the adoption of more resilient digital identity solutions across the financial services market.
10. Create a new NIST publication in the next 12 months detailing which biometric algorithms have been proven through NIST testing to meet a high threshold for both accuracy and equity; direct agencies to use only those algorithms in identity solutions.
11. Accelerate work at NIST to develop more robust guidance and criteria for liveness detection in biometrics, with an eye toward helping defenders stay ahead of emerging attacks such as those powered by deepfakes.
12. Develop a new, forward-looking investment strategy for R&D and standards work in identity that 1) ensures alignment in priorities across agencies, with a focus on addressing security, privacy, interoperability, and equity, and 2) ensures that necessary work around identity is adequately funded.
13. Create a multi-agency task force to monitor and combat emerging, scalable threats to identity system from deep fakes and other artificial intelligence generated attacks.

Initiative 2: Change the way America uses the Social Security Number (SSN).

The SSN plays a unique role in America's identity infrastructure, serving as both an identifier and an authenticator. With every breach where SSNs are targeted or exploited; it has become clear that the way the SSN is used must change.

1. Government and industry alike need to move away from using the SSN as an authentication factor – and migrate to alternative solutions that can more securely authenticate consumers. To ensure the government can lead the way, the President should issue an Executive Order banning agencies from using the SSN as an authenticator.
2. Congress and/or the Administration should launch a task force charged with reviewing more than 20 existing laws and regulations that require the use of the SSN and identifying whether any can be changed.

Initiative 3: Promote and prioritize the use of strong authentication. Inherent in any policy change that prohibits use of the SSN as an authenticator is a way to replace it with something better. Here, the problem is not just with SSNs, but also with passwords and other "shared secrets" that are easily compromised by adversaries.

1. Within the Federal government, enforce M-22-09, which requires that all agencies use only phishing-resistant authentication in enterprise applications, and that all public-facing applications offer people the option of using phishing-resistant authentication.

2. With policies focused on the private sector, avoid creating new restrictions that might preclude use of promising technologies such as data analytics for risk-based authentication that can assure security and prevent fraud, such as by detecting AI-powered attacks powered by deepfakes. Continue to promote CISA's "More than a Password" campaign, which helps educate the private sector on best practices for MFA.

Initiative 4: International coordination and harmonization. Consumers and businesses operate in environments beyond American borders, and other countries are also contemplating new approaches to making identity better. The United States should look for ways to coordinate with other countries and harmonize requirements, standards, or frameworks where feasible and compatible with American values.

1. As the European Union moves forward with its eIDAS digital identity wallet initiative, NIST, DHS and Treasury should actively engage with European counterparts to identify opportunities for collaboration and interoperability, and share lessons learned, and best practices.

2. Engage in broader standards work – NIST and DHS are engaged in a number of international digital identity standards bodies, but presence is limited in part by budget and resource constraints. Properly funding these efforts would enable U.S. agencies to be better represented alongside peer countries on the global standards stage.

Initiative 5: Educate consumers and businesses about better identity. As part of improving the identity ecosystem, Americans must be aware of new identity solutions and how to best use them. Government should partner with industry to educate both consumers and businesses, with an eye toward promoting modern approaches and best practices.

1. CISA should build off its excellent education campaign around MFA to also educate consumers on best practices for remote identity proofing and identity protection and provide support to private sector organizations that help with this education.

2. Develop a public-private "one-stop shop" led by the Federal Trade Commission and the Consumer Financial Protection Bureau that supports identity crime victims. This would enable victims to access services more easily from local, state, and federal government agencies as well as access private sector and non-profit services from a single virtual contact center or series of regional centers.

Next Steps: A Call to Action

While some progress has been made since the publication of our 2018 Policy Blueprint, digital identity continues to be treated as a third-tier priority by the U.S. government.

The United States Faces a Clear Choice

We can sit back and fail to modernize our identity policies. Identity-related breaches will keep getting worse and legacy solutions will continue to fail – a step that will create additional barriers to the availability of services online and erode trust in digital commerce.

Or we can take a proactive approach and act to get ahead of the identity conundrum – a step that will position the U.S. to address security challenges and enable the digital economy to thrive.

This revised Blueprint for Policymakers lays out a clear set of policy initiatives that are both significant in impact and achievable – should government choose to act on them – in the next 2-3 years.

The Administration, Congress and state governments should each move to advance the initiatives outlined in this Blueprint, with an eye toward a market where identity is the great enabler – driving trusted digital service delivery in a way that enhances security, privacy, inclusion, convenience, and innovation.

Appendix: Review of Action Plan

Our 2018 Policy Blueprint outlined a 19-point action plan for policymakers to address digital identity challenges. Below we review each of the priorities and where we are five-years later.

Initiative	Grade	Progress/Comments
1. Prioritize the Development of Next-Generation Remote ID Proofing & Verification Systems		
1. Establish the White House led, interagency task force – as called for in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity – to *"find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market."*	F	Two successive Administrations have failed to act on this issue. The Biden Administration called for similar action in its March 2023 National Cybersecurity Strategy. However, when the implementation plan was released for the Strategy in July, it skipped the digital identity action as if it had never been in the strategy.
2. Advance the work of the task force by funding the "Modernizing Identity Proofing" PMO at the General Services Administration (GSA) called for in the FY19 budget – and also funding NIST to develop a framework of standards and operating rules that agencies at all levels of government can leverage to deliver attribute validation services in a way that is secure, designed around the needs of consumers and protects privacy.	B-	The project management office at GSA has been shuttered. However, the CHIPS and Science Act of 2022 directed NIST to develop guidance on best practices for identity and attribute validation services provided by Federal, state, and local governments, but did not allocate additional funding. NIST is updating its Digital Identity Guidelines for the first time since 2017. NIST also has launched a project on mDL and digital entitled Accelerate Adoption of Digital Identities on Mobile Devices. This project will evaluate the interoperability of different vendors implementation of the ISO standards and produce a reference implementation.

Initiative	Grade	Progress/Comments
3. Stand up the service at the SSA called for in Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act to establish an attribute validation service for consumer financial applications that fall under the Fair Credit Reporting Act (FCRA).	B	SSA launched the electronic Consent-Based Social Security Verification (eCBSV) program, providing financial institutions with a powerful new tool to root out synthetic identity fraud and also improve the quality of their identity proofing efforts. However, SSA's unwillingness to share details on its use of fuzzy matching has decreased the effectiveness of eCBSV by making it harder for financial institutions to know if a "no match" response is likely fraud or just someone who used a nickname on their application for credit. Likewise, the economics around eCBSV have created challenges, particularly as an SSA decision to accelerate the recovery of dollars expended to create the eCBSV system has led to sharp price increases that have led some institutions to either abandon use of the system or only use it in a limited subset of transactions.
4. Amend Section 215 to cover account opening use cases not covered by the FCRA where SSN must still be collected and verified.	F	Has not happened – and the limited pool of users of eCBSV continues to contribute to some of the economic challenges described in the item above.

Initiative	Grade	Progress/Comments
5. Create a new five year, $200 million per year grant program to support states in their migration to being digital identity providers: work with the states and AAMVA to accelerate development of the mDL standard and incentivize adoption of mDL solutions by accepting them in lieu of traditional driver's licenses across the Federal government.	F	A grant program was originally proposed in the bipartisan Improving Digital Identity Act, but then was cut from a subsequent version of the bill. Federal work with the states on mDLs has primarily focused on in-person use cases to support TSA requirements at airport checkpoints, rather than the more important online use cases for mDLs. AAMVA work to date is likewise focused primarily on in-person uses cases, though the new AAMVA Digital Trust Service for mDLs should be able to help support adoption for online use cases over time.
6. Develop a new, forward-looking investment strategy for R&D and standards work in identity that 1) ensures alignment in priorities across agencies, and 2) ensures that necessary work around identity is adequately funded.	C-	There is no coordinated R&D strategy across government, but NIST has created an Identity & Access Management roadmap that lays out a plan for research into digital identity standards and ensure that U.S. Agencies are aligned. This roadmap is robust but remains underfunded; additional resources are required to accelerate the Roadmap's work amidst a sharp rise in identity-related cybercrime.
7. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity – and create incentives that promote adoption of innovations.	N/A	A post-Blueprint review revealed that there were not significant policy or regulatory barriers, but concerns remain that regulators may not embrace innovations that can enable better identity solutions.

Initiative	Grade	Progress/Comments
8. Convene a Digital Identity Task Force led by Treasury and including regulators in the Federal Financial Institutions Examination Council (FFIEC), focused on exploring how government policy can drive the adoption of more resilient digital identity solutions across the financial services market	B-	No Task Force was launched, but Treasury and FinCEN have taken a leadership role in promoting better digital identity solutions; CFPB has called for Congressional action to address shortcomings in digital identity infrastructure.
2. Change the Way America Uses the Social Security Number (SSN)		
1. Government and industry alike need to move away from using the SSN as an authentication factor – and migrate to alternative solutions that can more securely authenticate consumers. To ensure the government can lead the way, the President should issue an Executive Order banning agencies from using the SSN as an authenticator.	B	There has not been an Executive Order, but the SSN's role as an authenticator has been reduced. Policymakers understand that the SSN is used as both an identifier and an authenticator – and that its use as an authenticator poses the biggest risk. It is critical that the SSN continue to be used as an identifier and not an authenticator.
2. Congress and/or the Administration should launch a task force charged with reviewing existing laws and regulations that require the use of the SSN and identifying whether any can be changed.	F	No action.

Initiative	Grade	Progress/Comments
3. Promote and Prioritize the Use of Strong Authentication		
1. The Administration should enforce Executive Order 13681, which requires *"all agencies making personal data accessible to citizens through digital applications (to) require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."*	A	Executive Order 14028, Improving the Nation's Cybersecurity, mandated that cabinet agencies move to zero trust, which mandated multi-factor authentication. In its zero trust guidelines, the Office of Management and Budget Memorandum 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, mandated the use of phishing-resistant multi-factor authentication for federal agencies.
2. The "Lock Down Your Login" initiative – jointly developed by industry and government to promote the importance of strong authentication to consumers and businesses – should be reinvigorated and expanded, with a focus on providing more practical implementation guidance to businesses on how to deliver stronger authentication to employees and customers.	A	The Cybersecurity Infrastructure & Security Agency (CISA) has prioritized promoting MFA with its "More than a Password" campaign, which is the successor to the Lock Down Your Login initiative, though with more of a '70s rock vibe. CISA has promoted FIDO as "the gold standard" for MFA, has advocated for the use of phishing-resistant MFA in tweets and other forums, and has produced solid guidance for the private sector on how to best implement MFA.

Initiative	Grade	Progress/Comments
3. Where government offers guidance to industry on use of strong authentication – including in regulated industries – the government should look to modernize rules that govern use of strong authentication. Government should embrace multi-stakeholder efforts like the Fast Identity Online (FIDO) Alliance, the World Wide Web Consortium (W3C), and the GSMA, who have developed standards for next-generation authentication.	A	The White House Office of Management and Budget Memorandum 22-09, detailing the zero trust strategy for federal agencies, explicitly calls out the need for phishing resistant MFA. The FIDO2/WebAuthN standard – jointly crafted by FIDO Alliance and the W3C – is cited as a phishing-resistant authenticator that agencies can use. The Federal Trade Commission has also advocated for phishing-resistant MFA in consent orders where consumer data has been at risk due to lax security controls. And the Department of Health and Human Services and the CFPB and CISA have also issued advisories calling for the use of phishing-resistant MFA.
4. States should avoid creating new restrictions that might preclude use of promising technologies for risk-based authentication that can assure security and prevent fraud.	C	Most state privacy laws create a clear carve-out to ensure that data can be used to support solutions such as risk-based authentication that can assure security and prevent fraud. Not all states have taken this approach, however: the California Consumer Privacy Act (CCPA) and the more recently passed California Delete Act contains language that some have interpreted as as potentially precluding or limiting the use of some data-driven security and fraud prevention tools. Additional language is necessary to clarify the intent of these bills and make clear to implementers that the use of data for security and fraud prevention purposes is permitted. Additionally, New York State is implementing different online identity verification requirements for remote notaries, which could lead to compromised identities.

Initiative	Grade	Progress/Comments
4. Pursue International Coordination and Harmonization		
1. The Administration should task the Department of the Treasury with developing and executing a plan to engage with the eIDAS office in the European Commission, with an explicit focus around ensuring harmonization of international account openings.	C	While Treasury has not engaged with the EC, NIST has led these efforts in the Trade and Technology Council (TTC). But at a time when our peers are all advancing robust digital identity initiatives, the lack of a U.S. strategy means we are increasingly excluded from conversations.
2. The Administration should task the Department of the Treasury with developing and executing a plan to engage the FATF, with an explicit focus around ensuring harmonization of international account openings.	A	Treasury led a global effort to create robust Digital Identity Guidance in the Financial Action Task Force (FATF).
5. Educate Consumers and Businesses About Better Identity		
1. The Administration should partner with the National Cyber Security Alliance (NCSA) to develop a new initiative focused on educating both consumers and businesses about identity.	B-	There have been significant education efforts from CISA and other agencies on the MFA front. However, the lack of any U.S. initiative on digital identity proofing means education and on best practices for consumers and businesses on that front is almost non-existent. Likewise, identity theft victims continue to face a confusing landscape when it comes to knowing how and where to get help.

ENDNOTES

[1] https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

[2]https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity

[3] https://www.centerforcybersecuritypolicy.org/insights-and-research/fincen-212-billion-in-likely-financial-crimes-linked-to-identity-verification-breakdowns

[4] https://www.gao.gov/blog/more-fraud-has-been-found-federal-covid-funding-how-much-was-lost-under-unemployment-insurance-programs

[5] https://www.bostonfed.org/news-and-events/news/2022/08/synthetic-identity-fraud-is-not-a-victimless-crime-costs-billions-damages-lives.aspx

[6] https://javelinstrategy.com/press-release/17-million-us-children-fell-victim-data-breaches-according-javelins-2022-child

[7] https://www.pandemicoversight.gov/spotlight/identity-theft-in-pandemic-benefits-programs

[8] https://us.norton.com/blog/privacy/password-statistics

[9] ibid

[10]https://www.congress.gov/bill/117th-congress/house-bill/4258

[11]https://www.cisa.gov/topics/risk-management/national-critical-functions

[12] https://www.bloomberglaw.com/product/blaw/bloomberglawnews/privacy-and-data-security/BNA%20 0000018b-878d-dce3-a3fb-dfafe1380000