This three-paper series was developed through three volunteer workshops at the Federal Identity Forum (FedID) in June 2024, each of which operated under "Chatham House Rules." These papers compile insights and recommendations from workshop participants, aiming to inform the 2024–2025 presidential transition teams on strategic actions to enhance identity security and public trust. Disclaimer: These papers reflect the perspectives of workshop participants and do not represent the formal views of FedID organizers, including federal agencies, MITRE, and the Armed Forces Communications & Electronics Association International (AFCEA).

Interoperable Digital Identities

SEPTEMBER 2024

FEDERAL IDENTITY

Implementing a robust national digital identity strategy will enhance security, build public trust, and drive economic growth, positioning the United States as a leader in digital identity infrastructure.

The Case for Action

The current state of digital identity in the United States is fragmented and underdeveloped, with cyber crime growing and undermining public trust. Phishing attacks and other scams outpace security measures in both public and private sectors. Accountability for digital identity is split across federal departments and state governments, with no national policy or strategy in place. Congress failed to pass the Digital Identity Act, and a promised policy was never released by the White House.

The desired state is a cohesive, secure, and efficient digital identity infrastructure that enhances public trust, improves access to services, and drives economic growth. Countries like Australia, Estonia, and Canada have demonstrated significant economic benefits from strong digital identity programs, with potential gross domestic product (GDP) growth ranging from 2% to 6%. The United States is falling behind and remains a prime target for cyber crime.

Key Challenges and Opportunities

Cyber crime is growing and undermining public trust.
Phishing attacks and other scams are commonplace, with innovation by fraudsters outpacing security in our public infrastructure and private sector services. Quantifying the problem is difficult due to a lack of transparency about fraud attack data, which undermines public trust in both government and private sector services.

Accountability for digital identity is distributed between the public and private sectors.
Responsibility is split across federal departments and state governments for issuing identity documents, validating government attributes, and providing digital access to services. Many states have started issuing mobile driver's licenses as digital identity credentials. Private sector service providers offer varied security and digital identity products, some leveraging government attribute validation.

Government cannot fully outsource digital identity infrastructure to the private sector.
If digital identity is critical infrastructure, the government must offer an option. For access to government services like the Internal Revenue Service (IRS), there should be both public (Login.gov) and private sector options (ID.me).

Artificial intelligence (AI) and generative AI pose new risks.
Fraudsters are exploiting generative AI to create deep fakes, adding a new category of scams.
While bias in AI algorithms has improved, consistent policies and ongoing monitoring are essential.

There is not a clear demand from the public for digital identity.
Identity credentials are "public goods," but their transformative potential is not widely understood.
Public education on the benefits of digital identity is essential to mitigate misinformation and disinformation.

There is still no national policy or national strategy regarding digital identity.
Congress failed to pass the Digital Identity Act, and a promised policy has yet to be released by the White House. Other countries have developed policies and launched digital identity programs, leaving the United States behind and vulnerable to cyber crime.

There are equity issues related to digital identity access.
Digital identity can improve secure access to services and national security but may not benefit individuals without foundational identity documents, digital devices, internet access, or computer literacy.

A strong digital identity program is strategically and economically important.
The United States needs a comprehensive analysis to forecast GDP growth and cost savings across the government and the broader economy. Studies have shown that a robust digital identity program could add 2% to Estonia's GDP, 4% to U.S. GDP, and 6% to Canada's GDP.

Data-Driven Recommendations

Pass the National ID Act.
Require the use of shared government-wide identity solutions and ensure adequate funding at federal and state levels. Elevate digital identity to its own area of focus to ensure cross-agency accountability and alignment with state and local policies.

Fund citizen-facing agencies that own digital identity infrastructure delivery and a senior lead at each such agency, and form a public and private task force.
The public and private sectors will continue to be interconnected in the issuance, acceptance, regulation, standards, and governance of digital identity. By funding citizen-facing agencies and appointing a senior-level "chief digital identity advisor" at each agency, we can ensure these agencies effectively implement digital identity initiatives. Coordination among agencies is crucial to avoid inefficiencies and ensure a cohesive approach. Public-private collaboration will inform ongoing governance and ensure the ecosystem remains robust and secure.

Empower the Social Security Administration to issue digital identity credentials.
Enhance the Social Security Number by incorporating digital information, encryption, and biometrics over time. This will strengthen each individual's profile and enable secure interagency sharing. Provide multiple registration options to make it easy for all residents to obtain a digital ID. For example, leverage local resources like post offices and schools to reach people in remote areas. This approach ensures inclusivity and broad access to digital identity credentials.

Fund public incentives such as higher tax refunds and the ability to file directly with the government more easily, without paying for a tax service.
McKinsey reported the United States could save 4% of GDP ($1 trillion a year) with digital identity, justifying investment and incentives.

Fund public education on scams and phishing and on the benefits of digital identity.
Educate the public to inform and alert them about scams and communicate the benefits and safeguards of digital identity. Offer multiple mechanisms to access government services. Provide both private sector and public options, ensuring neither is the sole option.

Enable access to attribute validation services at federal and state levels.
For agencies like the IRS and Social Security at the federal level, and DMVs and birth and death registries at the state and local levels, enable qualified third parties to access attribute validation services. Where appropriate, allow these government entities to issue digital identity credentials to qualified third parties or government-enabled wallet services.

Allow capabilities to be shared across all of government.
Utilize open-source infrastructure to reduce costs, avert vendor lock-in, and ensure conformance to laws.
Enable acceptance of government-issued digital identity credentials across all levels of government.

Allow credentials to be digitally linked.
Link residency cards with Social Security cards, link digital birth certificates with digital driver's licenses or state identity cards, and link foreign identity credentials with temporary work authorization visas, all of which will help remove friction, costs and boost productively. Empower people with the ability to create Death Directives for their digital estate (including handling of digital assets and data), similar to Health Directives that empower named individuals to follow your healthcare wishes.

Learn from other countries' approaches.
Leverage the experience of other nations to work toward cross-border interoperability of digital identity solutions.

Implementation Considerations

- Expand the Executive Order on Artificial Intelligence to include digital identity as a critical tool to mitigate threats.
- Stand up an entity responsible for citizen services with centralized authority on technology and policy more generally including digital identity. This entity should be the administration's point for digital identity. If not a separate agency, direct the Social Security Administration to drive digital identity strategy nationally. Other key stakeholders would include the White House and the Departments of Treasury, Commerce, and Health and Human Services.
- Expand the Veterans Affairs VSAFE program to other agencies to protect veterans and the wider population from scams and fraud attacks.
- Build systems based on globally interoperable standards. Require entities receiving funding to implement solutions using global open and interoperable standards. Encourage the use of open-source code to accelerate deployment, lower costs, and facilitate interoperability.
- Communicate benefits of digital identity to the public. Educate residents on why they should get a digital identity credential, its benefits, and the safeguards in place to prevent misuse.