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).

Overcoming Identity Threats

SEPTEMBER 2024

FEDERAL IDENTITY

In an era where artificial intelligence (AI), deepfakes, synthetic biology, and social engineering are rapidly evolving, identity attacks are increasing at an alarming rate while public confidence in protections lags. Urgent action is needed to reverse these trends. The incoming presidential administration should implement a whole-of-government strategy, allocate resources, and launch a nationwide public education campaign on preventing and recovering from identity theft. These actions will significantly reduce identity theft risks, bolster public trust, and provide timely aid to victims.

The Case for Action

Identity attacks are becoming increasingly sophisticated and widespread, driven by advancements in AI technologies such as deepfakes and generative AI. The Federal Trade Commission (FTC) received 1.4 million identity theft reports in the past year alone, nearly triple the number of 10 years ago, with cybercrime losses surging to an estimated $10.2 billion. Technologies like biometrically enabled multi-factor authentication offer potential protections, but public acceptance and adoption remain low due to a lack of understanding and confidence in the handling of personal information.

Immediate action is needed to ensure citizens have access to effective, user-friendly solutions that build trust with both industry and government. It’s crucial to provide victims with readily available resources and assistance without shame or stigma. Implementing and enhancing digital identity certifications can help combat evolving identity threats by ensuring compliance and accountability. These steps will help create a secure and trustworthy digital environment for all citizens.

Key Challenges and Opportunities

Identity theft affects U.S. citizens across all demographic groups and generations.
Victims face significant emotional trauma and financial costs while trying to reverse the damage to credit scores and compromised accounts and devices. The incoming administration has a unique opportunity to establish a nationwide training and messaging campaign that emphasizes the importance of securing one’s identity, outlines practical steps for protection, and provides clear guidance on where to seek help. This must be backed by public access to resources and assistance.

The rapid advancement of AI capabilities, particularly deepfakes and generative AI, poses a major challenge.
These technologies enable bad actors to impersonate individuals using synthetically generated documents, voices, and fingerprints. They facilitate identity theft through socially engineered phishing, unauthorized access to private accounts, and fraudulent activities. Addressing these threats requires immediate and coordinated action.

A whole-of-government strategy is essential to provide effective privacy and sensitive information protection.
This strategy should include comprehensive policies and guidelines, adequate budget allocations for coordinated executive branch actions, and industry certifications that ensure accountability and enforcement.

Data-Driven Recommendations

Launch a comprehensive public education campaign in partnership with industry.
This initiative should present a unified voice to highlight the severity of identity theft and its impact on everyday lives, raising awareness about the financial losses to both individuals and government. The campaign should educate all demographic groups about the sophisticated threats posed by deepfakes and generative AI, emphasize personal responsibilities in prevention and recovery, and provide a centralized resource hub for victims. Additionally, it should offer training on using mitigation tools and address misconceptions about biometrics to build public confidence in multi-factor authentication.

Enhance certification, accountability, and enforcement for federal suppliers of digital identity products and services.
Digital security certification standards, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, must be regularly updated to keep pace with technological advancements and their misuse by bad actors. Credentialing service providers should be independently certified according to these enhanced standards, ensuring greater accountability and proper handling of identity information. This will enable the government to acquire and use compliant technologies with greater assurance they can withstand new threats.

Implement a whole-of-government, living strategy to protect the public and support identity theft victims.
This strategy should include issuing and frequently revising policies, guidance, and directives across all levels of government. It should guide the public to necessary resources and assistance, ensuring both prevention of identity theft and effective recovery for victims. By implementing these recommendations, the government can create a more secure environment for all citizens.

Implementation Considerations

- Establish a federal interagency group led by the FTC, including the Departments of Health and Human Services, Veterans Affairs, Treasury, and Justice, to develop a whole-of-government, living strategy to protect citizens and assist victims of identity theft.[1]
- Create a multi-agency/multi-stakeholder task force led by the FTC, with representation from the interagency group above, state government, industry, and academia.[2] This task force should launch a nationwide public education campaign on social media and through advertisements to inform the public on preventing and recovering from identity theft.
- Enhance certification, accountability, and enforcement for federal suppliers of digital identity products by requiring NIST to regularly update digital security standards like SP 800-63. Issue an executive order stipulating the federal use of products and services certified to the latest standards.
- Instruct the Office of Management and Budget to prioritize a whole-of-government strategy and nationwide public education on identity theft prevention and recovery in its budget directives to all departments and agencies.

Endnotes

[1] This interagency group could be modeled after the Identity Fraud Reduction & Redress Working Group formed during the pandemic to protect the public from identity fraud and help victims recover—in this case expanding beyond dealing with identity fraud in pandemic relief programs.
See https://www.pandemicoversight.gov/news/articles/new-prac-working-group-combat-identity-fraud-pandemic-response-programs-and-improve

[2] State government representation could involve organizations such as the National Governors Association. Industry representation could involve organizations such as the International Biometrics and Identity Association.