GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

DECEMBER 2022

Digital Identity + the Federal Government: Recent Actions + Interest

In recent years, the federal government has taken notice of cybersecurity, identity management, authentication, and identity proofing issues. This short resource guide highlights some key actions at the federal level around digital identity topics. As new developments occur, the Digital Benefits Network (DBN) will continue updating and publishing on them.

Executive Branch Priorities

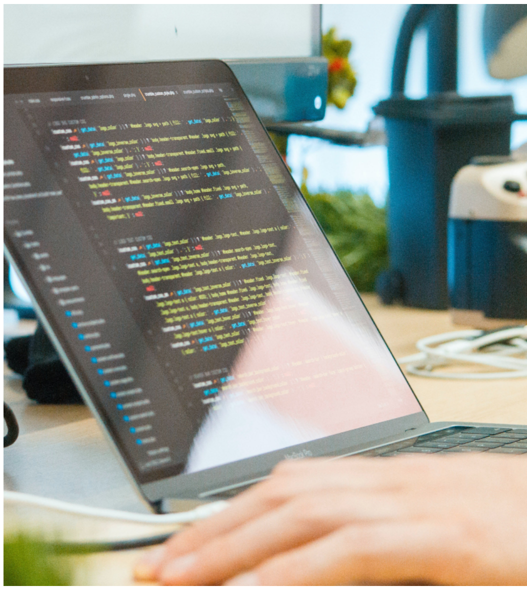
President Biden's Executive Order on Advancing Racial Equity and Support for Underserved Communities through the Federal Government, issued on his first day in office, made addressing inequity a whole-of-government priority. It also highlighted equitable delivery of government benefits as a priority area. Since then, the Office of Management and Budget (OMB) released a study on methods to assess equity in government programs. The agency included identity proofing requirements as a known driver of burden that agencies can address. In response to the Executive Order, federal agencies have also released their own equity action plans, including the Food and Nutrition Service and the Department of Labor (DOL). The DOL's plan acknowledges that fraud detection and identity verification methods may "deter or disproportionately flag as ineligible underserved workers."

In response to fraud and identity theft in pandemic relief programs, President Biden also announced plans in early 2022 to issue an executive order on Preventing Identity Theft in Public Benefits, that would focus on efforts to "prevent and detect identity theft involving public benefits, while protecting privacy and civil liberties and preventing bias that results in disparate outcomes."

Contributing Author

Elizabeth Bynum Sorrell
Researcher,
Digital Benefits Network,
Beeck Center for Social
Impact + Innovation

The recently released *Blueprint for an AI Bill of Rights*, issued by the White House Office of Science and Technology Policy, is not an enforceable set of standards. However, it shows the executive branch is more broadly thinking about privacy, data security, and individual rights in relation to developing technologies. In the future, this guidance may have implications for identity proofing technologies and automated fraud detection strategies. Other activity at the federal level includes President Biden's 2021 Executive Order on Improving the Nation's Cybersecurity, which outlines key benchmarks towards modernizing federal cybersecurity in partnership with the private sector. The Office of Management and Budget (OMB) followed up on this executive order with standards for moving federal agency systems to Zero Trust Architecture practices by the end of FY 2024.



Agency Activities

Federal agencies are also tackling authentication, identity proofing, and identification questions. For example, the General Services Administration (GSA) began expanding access to the Login.gov sign-on and identity proofing platform beyond federal agencies in 2021. GSA has set ambitious performance goals for increasing the number of customer agencies using at least one GSA identity management solution, increasing the number of annual active users on the Login.gov platform to 100 million, and expanding the number of identity vendors and government data source providers on the platform.

The National Institute of Standards and Technology (NIST) released digital identity guidelines in 2017, and is in the process of revising and updating them. NIST also released a study of facial recognition vendor technologies in 2019, and GSA is currently scoping its own study of equity in remote identity proofing, specifically techniques using facial recognition.

The Government Accountability Office (GAO) issued an assessment of federal agencies' online identity verification practices in 2019. Following NIST's 2017 guidance cautioning against knowledge-based verification for identity proofing, GAO advised multiple agencies to discontinue the practice and strengthen their identity proofing protocols. More recently, the Joint Financial Management Improvement Program, a project between GAO, OMB, the Office of Personnel Management, and the Department of the Treasury, published a report offering guidance to federal agencies. It includes best practices for implementing identity verification to prevent fraud while mitigating disparate impacts and bias. Additionally, the Transportation Security Administration (TSA), the Department of Homeland Security's Science and Technology (S&T) Biometric and Identity Technology Center (BI-TC), and NIST have been working with states, technology experts, and standards organizations to explore the use and implementation of mobile driver's licenses. In early 2022, TSA began testing mobile driver's licenses from participating states as identification forms at some TSA Precheck checkpoints.

Federal agencies have also issued benefits-program specific guidance and rules on authentication and identity verification practices. These include:

- The Department of Labor's April 2021 guidance on identity verification in unemployment programs which outlined requirements for identity verification adjudication standards, and encouraged state workforce agencies to participate in the Integrity Data Hub.
- The Food and Nutrition Service's (FNS) October 2022 Interim Final Rule for SNAP on Interstate Data Matching to Prevent Duplicate Issuances, as well as FNS' 2019 guidance allowing states to implement new identity authentication processes without FNS approval.

Legislative Action

Much of the recent federal-level activity on digital identity issues has come in the form of guidance. However, proposed legislation like the Improving Digital Identity Act, which was introduced in 2020 and has bipartisan support, would increase federal involvement in identity verification in the private and public sectors. If passed, the bill would create a Digital Identity Task Force to "establish a government-wide effort to develop secure methods for governmental agencies to validate identity attributes to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors."

The bill also highlights NIST's role in developing and updating standards for federal, state, and local governments to use in digital identity verification. The legislation tasks GAO with submitting a report to Congress analyzing the legal and regulatory requirements around collection and retention of Social Security Numbers by nongovernmental organizations.

The American Data Privacy and Protection Act, introduced in June 2022, focuses on consumer data privacy rights and oversight mechanisms. The bill has bipartisan sponsorship, but it is unclear whether it will move forward and if it does, in what form. If passed, the bill could have significant impacts on privacy regulations and protections across the country. It could also shape digital identity practices by updating data security requirements for a range of entities, and requiring large data holders to conduct algorithmic impact assessments, among other actions.

Looking Forward

Although there is no national set of identification credentials – offline or online – the federal government has an important role to play in the digital identity space through policy, regulations, and guidance. As part of our continued work on digital identity, the DBN will closely monitor executive and legislative efforts to create additional standards for identity verification, management, and authentication, which could have major implications for online access to government services including public benefits.

You can read more about digital identity on the Digital Benefits Hub, and find our other introductory resources including:

- A glossary of digital identity terms,
- An overview of digital identity broadly,
- A primer on digital identity in public benefits.

Agencies or individuals interested in our research on digital identity, can subscribe to the DBN and follow updates. If you would like to discuss our research further, or are interested in sharing your own experiences administering identification and authentication processes in a benefits program, we encourage you to reach out to us at digitalbenefits@georgetown.edu.

Get in Touch

Our Digital Benefits Network team is here to help!

Visit us at the Digital Benefits Hub

Please contact us with any thoughts, questions, or potential collaborations via email at digitalbenefits@georgetown.edu