PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

# POTENTIAL STUDY TOPIC | ENSURING TRUSTED IDENTITY ACROSS NETWORKS

## IMPACT

The President's National Security Telecommunications Advisory Committee (NSTAC) provides industry-based analyses and policy recommendations to the President regarding information and communications technologies, information assurance, infrastructure protection, and other national security and emergency preparedness (NS/EP) telecommunications issues. Improving identity (ID) management (IdM) is fundamental to ensuring the safety of Americans in cyberspace. As such, the NSTAC is well-poised to offer policy guidance to the President on this topic to strengthen the Nation's NS/EP posture.

## OVERVIEW

The inability to authenticate a person's identity online, as described in the *National Strategy for Trusted Identities in Cyberspace*, has been a subject of thoughtful discussion. The problem relates to how a person establishes their ID in cyberspace. Mastercard's report, *Restoring Trust in a Digital World*, observes that "[t]he absence of a simple, safe, and reliable way of authenticating [ID] digitally creates friction, increases fraud, degrades privacy, and restricts access to services."[1]

Attribute-based systems, like Social Security Numbers (SSN) or enhanced numeric identifiers, are no longer sufficient. This is particularly true of SSNs, which are tied to extremely sensitive transactions, such as filing tax returns, claiming federal benefits, and seeking credit. Unfortunately, frequent disclosures of personal ID data, whether authorized or not, mean that this information is easy to discover and misuse.

As a result, the United States needs to implement a new digital ID paradigm and an improved personal ID system given: (1) the increasing vulnerability of attribute-based systems; (2) growing fraud and ID theft; (3) the proliferation of devices and new applications; and (4) a multiplicity of new business and service delivery models requiring a high-level of trust. To achieve this vision, the Federal Government should help shape the strategy, tactics, and operational environment impacting the design and governance of such a system.

The proposed NSTAC study would assess the current state of digital ID systems, analyze key success elements, determine stakeholder requirements, and recommend a roadmap to the President on how to implement a more secure IdM system in the United States. The resulting approach would describe how the Government can work with industry to develop an interoperable system that would: identify, authenticate, and authorize individual IDs; generate broad end user acceptance; address privacy; and enable secure governmental, financial, and NS/EP transactions.

## POTENTIAL KEY FOCUS AREAS

Potential focus areas for this topic include:

- **Current state of digital ID systems:** Assess the benefits and challenges associated with current frameworks, technologies, and business models (e.g. centralized, federated, hybrid).
- **International deployments**: Review lessons learned from large-scale digital ID deployments (e.g., Norway, Canada) to ascertain what obstacles exist in implementing a national digital ID card.
- **Personal ID verification:** Identify weaknesses in existing U.S. mechanisms for trusted identification, authorization, and authentication.
- **Digital ID needs:** Determine key stakeholder requirements, including those from the Federal Government, financial institutions, intermediaries, and enterprise end users.
- **The root of trust:** Examine how the root of trust would be obtained for digital IDs (e.g., in person verification, other methods).
- **Secure transactions:** Identify which Government IDs (e.g., SSNs) are being leveraged by the private sector to determine how they can be transmitted and linked to existing records.
- **Risk capture and mitigation solutions:** Investigate improved solutions to: (1) address ID theft; and (2) mitigate cross-device and cross-network assurance risks through known methods, including secure remediation.

[1] MasterCard, "Restoring Trust in a Digital World," (March 2019).

- **Privacy issues:** Describe the: (1) safeguards needed to ensure appropriate privacy protection (e.g., anonymization); and (2) technical solutions that can limit the production of personally identifiable information.
- **Public-private ID standards:** Measure the value of establishing standards-based, privacy-enhanced data validation for public and private sector ID proofing services.
- **Required federal identity authorities:** Determine the authorities and activities required to establish a modern digital ID infrastructure.
- **NS/EP implications:** Research the impact that digitally-secure IDs will have on NS/EP systems to determine an efficient way of authenticating individual access to facilities and communications systems during a crisis.

## EXPECTED OUTCOMES

- Produce a report to the President describing the needs, benefits, and enhancements required for the U.S. Government to effectively implement a trusted digital ID system.
- Provide strategic perspectives on the requirements for a new digital ID system to enable and protect digital economies now and into the future.
- Determine the authority or authorities under which an updated ID system could be implemented.
- Address key gaps to effectively implementing a truly secure digital and financial ecosystem.