NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

"The internet has transformed how we do business, opening up markets and connecting our economy as never before. It has revolutionized the ways in which we communicate with one another, whether with a friend down the street or a colleague across the globe. And as we have seen in recent weeks, it has empowered people all over the world with tools to share information and speak their minds. In short, the growth of the internet has been one of the greatest forces for innovation and progress in history."

—President Barack Obama

A PLATFORM FOR SECURITY, PRIVACY AND INNOVATION

The NSTIC's vision statement is: "Individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

For our nation to continue to drive economic growth over the Internet, we must provide individuals and organizations the ability and the option to more securely identify each other. When individuals and organizations have greater trust in online identities, they can offer and use online services for more sophisticated and sensitive transactions than have been available to date. They will also be better protected against online fraud and identity theft.

The Strategy emphasizes choice for individuals, who can

- Choose whether or not to participate at all: participation is optional.
- Choose one or more different identity providers: the Strategy envisions a vibrant marketplace that provides individuals with choices among multiple identity providers—both private and public.
- Choose between different types of credentials: individuals will be able to choose credentials that meet their needs, including smart cards, cell phones, keychain "fobs," one-time password generators, and, undoubtedly, secure solutions that have yet to be invented.
- Choose when to use a credential: if people want to use cyberspace without a credential in ways that don't require authentication, like browsing or blogging anonymously, they can do so at any time.
- Choice drives competition and innovation—and will result in a thriving market of diverse solutions to fit different individuals' needs.

EXAMPLES

Faster Online Errands—Mary is tired of memorizing dozens of password and username combinations to conduct her personal online errands. She opts instead to get a smart card from her Internet service provider. She inserts the card into her computer and in a matter of seconds, with just clicks of her mouse, she is able to securely move between her online account with her

bank, her mortgage company, and her doctor; next she sends an authenticated email to her friend and remotely checks her office calendar on her employer's intranet.

Age Appropriate Access—Antonio, age 13, visits online chat rooms to talk to other students his age. His parents give him permission to get an identity credential, stored on a keychain fob, from his school. The credential verifies his age so that he can visit chat rooms for adolescents, but it does not reveal his birth date, name, or other information. Nor does it inform the school about his online activities. Antonio can speak anonymously but with confidence that the other participants are his age.

Smart Phone Transactions—Parvati does most of her online transactions using her smart phone. She downloads a "digital certificate" from an ID provider that resides as an application on her phone. Used in conjunction with a single, short PIN or password, the phone's application is used to prove her identity. She can do all her sensitive transactions, even pay her taxes, through her smart phone whenever and wherever it is convenient for her—and without remembering complex passwords.

Efficient and Secure Business Operations—Juan owns a small business and is setting up a new online storefront. Without making large investments in information technology, he wants customers to know that his small firm can provide the same safety and privacy for their transactions as sites for larger companies. He installs standard software and agrees to follow the Identity Ecosystem privacy and security requirements, earning a "trustmark" logo for his Web site. To reduce his risk of fraud, he needs to know that his customers' credit cards or other payment mechanisms are valid and where to ship his merchandise. There are a number of different ID providers that can issue credentials that validate this information. Millions of individuals can now use his Web site without having to share extra personal information or even set up accounts with Juan's company. This saves his customers time, increases their privacy and confidence, and saves Juan money.

Enhanced Public Safety—Joel is a doctor. A devastating hurricane occurs close to his home. Using his interoperable credential located on a USB thumb drive and issued by his employer, he logs in to a Web portal maintained by a federal agency. The site tells him that his medical specialty is urgently needed at a triage center nearby.

PRINCIPLES

PRIVACY ENHANCING AND VOLUNTARY

- Participation in the Identity Ecosystem will be voluntary: there is no requirement that any individual obtain a credential.
- The envisioned Identity Ecosystem will be grounded in the implementation of the full set of the Fair Information Practice Principles (FIPPs) in order to provide multi-faceted privacy protections. The privacy rules must address not only the circumstances under which participants in the Identity Ecosystem may share information but also the kinds of information that they may collect and how that information is managed and used.
- Although individuals will retain the right to exchange their personal information in return for services they value, these protections will provide a default level of privacy

and will enable individuals to form consistent expectations about the treatment of their information within the ecosystem.
- A FIPPs-based approach will also promote the adoption of privacy-enhancing technical standards. As envisioned by NSTIC, such standards will minimize the ability to link credential use among service providers, thereby preventing them from developing a complete picture of an individual's activities online.

SECURE AND RESILIENT

- Identity solutions will provide secure and reliable methods of electronic authentication. Authentication credentials are secure when they are issued based on sound criteria for verifying the identity of individuals and devices; resistant to theft, tampering, counterfeiting, and exploitation; and issued only by providers who fulfill the necessary requirements.
- Credentials are resilient when they can recover from loss, compromise, theft—and can be effectively revoked or suspended in instances of misuse. Another contributor to resilience is the existence of a diverse environment of providers and methods of authentication.

INTEROPERABLE

- Interoperability encourages service providers to accept a variety of credentials and identity media, similar to the way ATMs accept credit and debit cards from different banks.
- Interoperability also supports identity portability: it enables individuals to use a variety of credentials in asserting their digital identities to service providers. Finally, the interoperability of identity solutions envisioned in the Strategy will enable individuals to easily switch providers, thus aligning market incentives to meet individuals' expectations.

COST-EFFECTIVE AND EASY TO USE

- Individuals, businesses, organizations, and all levels of government will benefit from the reduced cost of online transactions: fewer redundant account procedures, a reduction in fraud, decreased help-desk costs, and a transition away from expensive paper-based processes.

BENEFITS

INDIVIDUALS

- **Convenience.** Individuals will be able to conduct their personal business online with less time and effort.
- **Privacy.** Individuals' privacy will be enhanced.
- **Security.** Individuals can work and play online with fewer concerns about identity theft.

PRIVATE SECTOR

- **Innovation.** The Identity Ecosystem will provide a platform on which new and more efficient business models will be developed—just as the Internet itself has been a platform for innovation. It will also enable organizations to put new services online, especially for sectors such as healthcare and banking.

- **Efficiency.** Online transactions will be practical in more situations. The private sector will have lower barriers to customer enrollment, increased productivity, and decreased costs. Cross-organizational trust will provide businesses with exposure to a large population of potential customers they might not otherwise reach. Not only is there potential access to new customers, the traditional barriers associated with customer enrollment can be eliminated, reducing a friction that prevents potential customers from using a service.
- **Trust.** Trusted digital identities will allow organizations to better display and protect their brands online. Participants in the Identity Ecosystem will also be more trusted, because they will have agreed to the Identity Ecosystem's minimum standards for privacy and security.

GOVERNMENT

- **Constituent Satisfaction.** The Identity Ecosystem will enable government to expand its online services in order to serve its constituents more efficiently and transparently.
- **Economic Growth.** Government support of the Identity Ecosystem will generate innovation in the marketplace that will create new business opportunities.
- **Public Safety.** Increasing online security will reduce cyber crime, improve the integrity of networks and systems, and raise overall consumer safety levels. Enhanced online trust will also provide a platform to support more effective and adaptable response to national emergencies.