# National Strategy for Trusted Identities in Cyberspace

## Creating Options for Enhanced Online Security and Privacy

June 25, 2010

Draft

# Table of Contents

# Executive Summary

Cyberspace – the interdependent network of information technology components that underpins many of our communications – is a crucial component of the Nation's critical infrastructure. We use cyberspace to exchange information, buy and sell products and services, and enable many online transactions across a wide range of sectors, both nationally and internationally. As a result, a secure cyberspace is critical to the health of our economy and to the security of our Nation. In particular, the Federal Government must address the recent and alarming rise in online fraud, identity theft, and misuse of information online.

One key step in reducing online fraud and identity theft is to increase the level of trust associated with identities in cyberspace. While this Strategy recognizes the value of anonymity for many online transactions (e.g., blog postings), for other types of transactions (e.g., online banking or accessing electronic health records) it is important that the parties to that transaction have a high degree of trust that they are interacting with known entities. Spoofed websites, stolen passwords, and compromised login accounts are all symptoms of an untrustworthy computing environment. This Strategy seeks to identify ways to raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions. The Strategy's vision 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.***

More specifically, the Strategy defines and promotes an Identity Ecosystem that supports trusted online environments. The Identity Ecosystem is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities. The Identity Ecosystem enables:

- **Security,** by making it more difficult for adversaries to compromise online transactions;
- **Efficiency** based on convenience for individuals who may choose to manage fewer passwords or accounts than they do today, and for the private sector, which stands to benefit from a reduction in paper-based and account management processes;
- **Ease-of-use** by automating identity solutions whenever possible and basing them on technology that is easy to operate with minimal training;
- **Confidence** that digital identities are adequately protected, thereby increasing the use of the Internet for various types of online transactions;
- **Increased privacy** for individuals, who rely on their data being handled responsibly and who are routinely informed about those who are collecting their data and the purposes for which it is being used;
- **Greater choice,** as identity credentials and devices are offered by providers using **interoperable** platforms; and
- Opportunities for **innovation,** as service providers develop or expand the services offered online, particularly those services that are inherently higher in risk;

Privacy protection and voluntary participation are pillars of the Identity Ecosystem. The Identity Ecosystem protects anonymous parties by keeping their identity a secret and sharing only the information necessary to complete the transaction. For example, the Identity Ecosystem allows an individual to provide age without releasing birth date, name, address, or other identifying data. At the other end of the spectrum, the Identity Ecosystem supports transactions that require high assurance of a participant's identity. The Identity Ecosystem reduces the risk of exploitation of information by unauthorized access through more robust access control techniques. Finally, participation in the Identity Ecosystem is voluntary for both organizations and individuals.

Another pillar of the Identity Ecosystem is interoperability. The Identity Ecosystem leverages strong and interoperable technologies and processes to enable the appropriate level of trust across participants. Interoperability supports identity portability and enables service providers within the Identity Ecosystem to accept a variety of credential and identification media types. The Identity Ecosystem does not rely on the government to be the sole identity provider. Instead, interoperability enables a variety of public and private sector identity providers to participate in the Identity Ecosystem.

Interoperability and privacy protection combine to create a user-centric Identity Ecosystem. User-centricity will allow individuals to select the interoperable credential appropriate for the transaction. Through the creation and adoption of privacy-enhancing policies and standards, individuals will have the ability to transmit no more than the amount of information necessary for the transaction, unless they choose otherwise. In addition, such standards will inhibit the linking of an individual's transactions and credential use by service providers. Individuals will have more confidence that they exchange information with the appropriate parties, securely transmit that information, and have the information protected in accordance with privacy best practices.

With the vision of the Identity Ecosystem in mind, the National Strategy for Trusted Identities in Cyberspace (NSTIC) identifies the following goals:

| | |
|---|---|
| **Goal 1:** | Develop a comprehensive Identity Ecosystem Framework |
| **Goal 2:** | Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework |
| **Goal 3:** | Enhance confidence and willingness to participate in the Identity Ecosystem |
| **Goal 4:** | Ensure the long-term success of the Identity Ecosystem |

The first two goals focus on designing and building the necessary governance, policy, standards, and infrastructure to enable secure delivery of online services. The third goal targets the necessary privacy protections and the education and awareness required to encourage adoption by individuals and businesses. The fourth establishes the mechanisms to promote continued development and improvement of the Identity Ecosystem over time.

Nine high-priority actions align to these goals and the vision. These actions provide the foundation for the Identity Ecosystem implementation. The actions are:

| | |
|---|---|
| **Action 1:** | Designate a Federal Agency to Lead the Public/Private Sector Efforts Associated with Achieving the Goals of the Strategy |
| **Action 2:** | Develop a Shared, Comprehensive Public/Private Sector Implementation Plan |
| **Action 3:** | Accelerate the Expansion of Federal Services, Pilots, and Policies that Align with the Identity Ecosystem |
| **Action 4:** | Work Among the Public/Private Sectors to Implement Enhanced Privacy Protections |
| **Action 5:** | Coordinate the Development and Refinement of Risk Models and Interoperability Standards |

| | |
|---|---|
| **Action 6:** | Address the Liability Concerns of Service Providers and Individuals |
| **Action 7:** | Perform Outreach and Awareness Across all Stakeholders |
| **Action 8:** | Continue Collaborating in International Efforts |
| **Action 9:** | Identify Other Means to Drive Adoption of the Identity Ecosystem across the Nation |

The execution of the actions above requires the Federal Government to continue to provide leadership, coordination, and collaboration in order to enhance the security of digital identities. To lead the day-to-day coordination of these actions, the Executive Office of the President (EOP) will designate a lead agency within the Federal Government. The Office of the Cybersecurity Coordinator within EOP will continue to lead interagency policy development specified in this action plan. The lead agency will work closely with The Office of the Cybersecurity Coordinator.

This Strategy is a call to action that begins with the Federal Government continuing its role as a primary enabler, first adopter and key supporter of the envisioned Identity Ecosystem. The Federal Government must continually collaborate with the private sector, state, local, tribal, and international governments and provide the leadership and incentives necessary to make the Identity Ecosystem a reality. The private sector in turn is crucial to the execution of this Strategy. Individuals will realize the benefits associated with the Identity Ecosystem through the conduct of their daily online transactions in cyberspace. National success will require a concerted effort from all parties, as well as joint ownership and accountability for the activities identified.

# Introduction

Imagine a world where individuals can seamlessly access information and services online from a variety of sources – the government, the private sector, other individuals, and even across national borders – with reduced fear of identity theft or fraud, lower probability of losing access to critical services and data, and without the need to manage many accounts and passwords. Individuals can conduct a wide variety of transactions online and trust the identities of the entities with which they interact. Individuals know what information service providers are collecting about them and how they are using it. They have choice in the number and types of user-friendly identity credentials they manage and use to assert their identity online. They have access to a wider array of online services to save time and effort.

In this user centric world, organizations efficiently conduct business online by trusting the identity proofing and credentials provided by other entities as well as the computing environment in which the transactions occur. They are able to eliminate redundant processes associated with collecting, managing, authenticating, authorizing, and validating identity data. They reduce loss due to fraud or data theft through identity assurance efforts appropriate to the types of transactions they conduct, and they are able to offer additional services and higher risk transactions online.

**Envision It!**

An individual voluntarily requests a smart identity card from her home state. The individual chooses to use the card to authenticate herself for a variety of online services, including:

- Credit card purchases,
- Online banking,
- Accessing electronic health care records,
- Securely accessing her personal laptop computer,
- Anonymously posting blog entries, and
- Logging onto Internet email services using a pseudonym.

This ideal online world is within reach; however, we must first overcome barriers in the current environment. This Strategy and its associated implementation actions aim to transform the current identity landscape to the desired target state – the Identity Ecosystem. The Identity Ecosystem comprises a combination of transaction participants and interoperable infrastructure to foster trusted digital identities. The Identity Ecosystem is an online environment where individuals, organizations, services, and devices can trust one another through proper identification and authentication.

## Current Landscape

The United States has grown increasingly reliant on the interconnectivity of the Internet to provide instant access to information and services. However, the benefits that these online services provide have not come without a price. The Nation faces a host of increasingly sophisticated threats against the personal, sensitive, financial, and confidential information of organizations and individuals. Fraudulent transactions within the banking, retail, and other sectors along with intrusions against the Nation's critical infrastructure assets that are essential to the functioning of our society and economy (utilities, transportation, financial, etc.) are all too common. As more commercial and government services become available online, the amount of sensitive and financial data transmitted over the Internet is ever increasing. Consequently, the probability of loss associated with data theft and corruption, fraud, and privacy breaches increases as well.

Although the total amount of losses due to online fraud and cybercrime are difficult to quantify, a few studies illustrate the magnitude of the problem:

- The 2009 Internet Crime Report states, “From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions. This was a 22.3% increase as compared to 2008…the total dollar loss from all referred cases was $559.7 million…up from $264.6 million in 2008.”[1]
- In 2004, the Congressional Research Service estimated that economic losses totaled $46 billion due to cyber theft.[2]
- The Cyberspace Policy Review stated that, “Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion.”[3]

Over 10 million Americans[4] are also victims of identity theft each year. The costs of these crimes extend beyond financial loss to include other costs associated with restoring an identity. A survey by the Federal Trade Commission states that victims of identity theft can spend up to 130 hours reconstructing their identities (e.g., credit rating, bank accounts, reputation, etc.) following an identity crime.[5]

There are various causes of the online fraud and identity theft identified in the statistics above. Out-of-date software, unsafe web browsing habits, or lack of appropriate anti-virus systems can all lead to the compromise of computer systems. Criminals and other adversaries often exploit weak identity solutions for individuals, websites, email, and the infrastructure that the Internet utilizes. The poor identification, authentication, and authorization practices associated with these identity solutions are the focus of this Strategy.

Further, the online environment today is not user-centric; individuals tend to have little control over their own personal information. They have limited ability to utilize a single digital identity across multiple applications. Individuals also face the increasing complexity and inconvenience associated with managing the large number of user accounts, passwords, and other identity credentials required to conduct services online with disparate organizations. The collection of identity-related information across multiple providers and accounts, coupled with the sharing of personal information through the growth of social media, increases opportunities for data compromise. For example, personal data used to recover lost passwords (e.g., mother’s maiden name, the name of your first pet, etc.) is often publicly available.

In some cases, services providers have met consumer demand for online services, but they have provided inadequate identity assurances. Service providers have also deemed some highly desirable services that could provide further efficiencies and cost savings too risky to conduct online. In order to meet the demand for online services without compromising security, the United States must improve the standards associated with trusted identities in cyberspace.

[1] “2009 Internet Crime Report.” Internet Crime Complaint Center. IC3. 12 Mar. 2010. Web. 2 Jun. 2010. <http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf/>.

[2] Congressional Research Service, Report to House Committee on Homeland Security, 2004. < http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf>

[3] “Cyberspace Policy Review.” The White House. The White House. May 2009. Web. 2 Jun. 2010. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf/>.

[4] United States. Department of Justice. Office of the Inspector General. The Department of Justice’s Efforts to Combat Identity Theft. Mar. 2010. Web. 2 Jun. 2010. <http://www.justice.gov/oig/reports/plus/a1021.pdf/>

[5] Federal Trade Commission. Federal Trade Commission – 2006 Identity Theft Survey Report. Nov. 2007. Web. 2 Jun. 2010. <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>

## Scope

The Strategy focuses on ways to establish and maintain trusted digital identities, a key aspect for improving the security of online transactions. Online transactions are electronic communications among two or more parties, connected over the Internet via networks, systems and computers. Identification, authentication, and authorization of these parties within a given transaction enable trust. Individuals, organizations, hardware, and software are all participants in an online transaction; therefore, attention to the identification, authentication, and authorization of each is paramount.

**Envision It!**

A power utility remotely manages Smart Grid software deployed on an electricity meter. Trusted hardware modules and secure authentication between the power company and the meter prevent deploying fraudulent meters as a way to steal electricity; ensure that the hardware and software configurations are correct; and restrict meter software to only run on authorized meters. Likewise, the meter trusts that instructions and periodic software upgrades come from the power company. These trusted interactions reduce the threat of fraudulent activity and deployment of malware within the Smart Grid.

This Strategy focuses on transactions involving the private sector, individuals, and governments. It addresses the international nature of many transactions. It also recognizes ongoing public and private sector efforts relative to trusted identities and builds upon them for application in the larger national and global forum for online services.

Numerous other cybersecurity efforts affect the security of online transactions; trusted identity is just one part. These other cybersecurity efforts (which are not within the scope of this Strategy) include securing the cyber supply chain, malware detection and analysis, software assurance, and configuration management. The Strategy recognizes that trusted digital identities are one part of layered security. By themselves, trusted digital identities cannot solve all security issues associated with online transactions, but trusted digital identities do play a critical role in the overall enhancement of security in online transactions.

The identity aspects of securing online transactions are a subset of the overall identity management sphere. The Strategy does not explicitly address identity and trust issues in the offline world. However, online and offline identity solutions can and should complement each other.

Lastly, the Strategy does not advocate for the establishment of a national identification card. Instead, the Strategy seeks to establish an ecosystem of interoperable identity service providers and relying parties where individuals have the choice of different credentials or a single credential for different types of online transactions. Individuals should have the choice of obtaining identity credentials from either public or private sector identity providers, and they should be able to use these credentials for transactions requiring different levels of assurance across different sectors (e.g., health care, financial, and social transactions).

## National Strategy Development

In recognition of the far-reaching impacts of cyber threats to our Nation's economy, society, government, and critical infrastructure, the EOP has called for a unified effort across public and private sectors to improve online security. Most recently, the President's *Cyberspace Policy Review* stated that:

> *The Federal government - in collaboration with industry and the civil liberties and privacy communities - should build a cyber security-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies. The Federal government must interact with citizens through a myriad of information, services, and benefit programs and thus has an interest in the protection of the public's private information as well.* [3]

This recommendation targets not just the activities of the Federal Government, but also the activities of the Nation as a whole – including both public and private interests. The role of government is to address the safety and economic needs of its people. As a result, the White House determined that the Federal Government would take a leadership role in developing a strategy to combat these threats. The Federal Government has already done much in addressing trusted digital identities. For example, the Federal Government's ongoing efforts to execute the Federal Identity, Credential, and Access Management (FICAM) Roadmap[6] are representative of the progress made. This Strategy seeks to accelerate those activities and extend trusted digital identities beyond the Federal boundaries and into the national domain.

Working in close collaboration with the private sector through eighteen critical infrastructure and key resource sectors and encompassing nearly seventy different stakeholder groups, an interagency writing team developed the National Strategy for Trusted Identities in Cyberspace. This writing team developed the Strategy over approximately 12 months from October 2009 to October 2010.

## National Strategy Organization

The organization of the remaining sections of the Strategy is as follows:

- Guiding Principles – Establishes the tenets that this Strategy must uphold in order to be successful. The Guiding Principles are necessary characteristics of the Identity Ecosystem.
- Vision and Benefits – Presents the overarching vision the Strategy seeks to achieve along with the details of the Identity Ecosystem and the benefits for individuals, private sector, and Government.
- Goals and Objectives – Defines what this Strategy intends to accomplish.
- High Priority Action Plan – Introduces critical tasks that form the basis for realization of the Strategy Goals and Objectives.
- Conclusion – Provides a high-level summary of the Strategy and a call to action for the public and private sectors.

[6] www.idmanagement.gov

# Guiding Principles

The Guiding Principles form the foundation for all of the goals, objectives, and actions in the Strategy. The Guiding Principles answer the question: What are the essential characteristics of solutions that support Trusted Identities in Cyberspace?

## Identity Solutions will be Secure and Resilient

Securing identity solutions against attack or misuse is paramount. Security ensures the confidentiality, integrity, and availability of identity solutions. Strong cryptography, the use of open and well-vetted security standards, and the presence of auditable security processes are critical to the trustworthiness of an identity solution. Identity solutions should have security built into them such that they detect and prevent intrusions, corruption, and disruption to the maximum extent possible.

Identity solutions should be resilient, able to recover and adapt to drastic or abrupt change. They should be capable of timely restoration after disruption occurs and should adapt to the dynamic nature of technology. Tolerance to loss, compromise, or theft is crucial for maintaining services during and after disruption. Security infrastructure should prevent unauthorized transactions by authorized individuals/entities. The ability to support robust forensic capabilities maximizes recovery efforts and provides a valuable opportunity to apply lessons learned to future enhancements.

## Identity Solutions will be Interoperable

Interoperability encourages service providers to accept a variety of credential and identity media, similar to the way ATMs accept credit and debit cards from different banks. Interoperability supports identity portability by allowing individuals to use a variety of credentials in asserting their digital identities to various service providers.

**Envision It!**

An online auction website sets a policy that it will accept trustmark-approved credentials. The auction incentivizes private sector organizations and individuals to participate by offering a one-time discount on the service charge associated with an auction purchase and by accommodating a large variety of credentials and identity media.

This principle recognizes two interoperability ideals within the Identity Ecosystem:

1. There will be standardized, reliable credentials and identity media in widespread use; and
2. If an individual, device, or software presents a valid and appropriate credential, any qualified relying party could accept the credential as proof of identity and attributes.

To achieve these ideals, identity solutions should be scalable across multiple federations, spanning traditional geographic borders. An identity federation allows an organization to accept and trust external users authenticated by a third party. Within the Identity Ecosystem, individuals will have the capability to conduct online transactions seamlessly across numerous service providers and identity federations. Identity solutions achieve scalability when all participants in the various federations agree upon a common set of standards, requirements, and enforcement mechanisms for securely exchanging digital identity information, resulting in authentication across federations.

There are three types of interoperability requirements for identity solutions:

- **Technical Interoperability** – The ability for different technologies to communicate and exchange data based upon well defined and widely adopted interface standards.

- **Semantic Interoperability** – The ability of each end-point to communicate data and have the receiving party understand the message in the sense intended by the sending party.
- **Policy Interoperability** – Common business policies and processes (e.g., identity proofing and vetting) related to the transmission, receipt, and acceptance of data between systems, which a legal framework supports.

Lastly, the Identity Ecosystem will encourage identity solutions to utilize non-proprietary standards to help ensure interoperability. In addition, identity solutions will be modular, allowing service providers to build sophisticated identity systems using smaller and simpler sub-systems. This improves the flexibility, reliability, and reuse of these systems, and allows for simplicity and efficiency in change management as service providers can add and remove components without requiring wholesale updates.

## Identity Solutions will be Privacy Enhancing and Voluntary for the Public

There are practical barriers in place that preserve individual privacy in the offline world. For example, an individual can utilize a driver's license to open a bank account, get onto an airplane, or get into an age-restricted movie. The Department of Motor Vehicles does not know all the places that service providers accept driver's licenses as identification. It is also difficult for the bank, the airport, and the movie theater to get together and link the transactions together. At the same time, there are aspects of these offline transactions that are not privacy-protective. The movie theater attendant that checks the driver's license only needs to know that the individual is over age 18. However, the driver's license reveals unnecessary information, such as address and actual date of birth, when the individual provides it for age verification.

Ideally, identity solutions should preserve the positive privacy benefits of offline transactions, while mitigating some of the negative privacy aspects. The eight Fair Information Practice Principles (FIPPs)[7] — Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing — are the widely accepted framework for evaluating and mitigating privacy impacts. Universal and integrated adoption of the FIPPs in the Identity Ecosystem should enable individuals to understand and make meaningful choices about the use of their personal information in cyberspace. Adoption of the FIPPs should also ensure that organizations limit data collection, only use and distribute information that is relevant and necessary, maintain appropriate safeguards on that information, and are responsive and accountable to individuals' privacy expectations.

**Envision It!**

An individual authenticates himself to an online pharmacy using a credential bound to his personal computer. The individual makes an online request for the pharmacy to fill his prescription. Through privacy-enhancing technology, the individual's attribute provider provides authoritative proof that he is over 18 and that his prescription is valid. The technology ensures that no unnecessary information is exchanged in this transaction (e.g., his birth date, reason for the prescription). The technology also filters information so that the attribute providers –the authoritative sources of the age and prescription information – do not know which pharmacy the individual is using.

Fully integrating all of the FIPPs into the Identity Ecosystem will be the key to achieving trusted identities in cyberspace that are truly privacy enhancing. For example, many privacy approaches focus on the principles of Transparency and Individual Participation, which include the provision of privacy notices and individual privacy choices. However, if such approaches fail to incorporate the

[7] See appendix C at the end of this document for further detail on the Fair Information Practice Principles.

other FIPPs, the entire burden of implementing privacy protections is on the individual. Alternatively, an Identity Ecosystem grounded in a more holistic adoption of the FIPPs provides multi-faceted privacy protections. It includes, for example, the creation and adoption of privacy-enhancing technical standards that allow individuals to transmit the minimum amount of information necessary to the transaction. Such policies and standards would also minimize the linkage of credential use among and between service providers.

In circumstances where individuals make choices regarding the use of their data (such as to restrict particular uses), those choices are communicated to and implemented by all subsequent data holders. In addition, the Identity Ecosystem includes limits on the length of time organizations can retain personal information and requires such organizations to provide individuals with appropriate opportunities to access, correct, and delete it. The Identity Ecosystem also requires organizations to maintain auditable records regarding the use and protection of personal information and compliance with applicable standards, law, and policies.

Voluntary participation is another critical element of this Strategy. Engaging in online transactions should be voluntary to both organizations and individuals. The Federal Government will not require organizations to adopt specific identity solutions or to provide online services, nor require individuals to obtain high-assurance digital credentials if they do not want to engage in high-risk online transactions with the government or otherwise. The Identity Ecosystem should encompass a range of transactions from anonymous to high assurance. Thus, the Identity Ecosystem should allow an individual to select the credential he or she deems most appropriate for the transaction, provided the credential meets the risk requirements of the relying party.

## Identity Solutions will be Cost-Effective and Easy To Use

**Envision It!**

An individual uses a strong credential issued by a third party and bound to his existing cell phone to access government tax services online. He views tax history, changes demographic information, monitors refund status, and files his taxes electronically. Both the online service provider and the individual are able to leverage existing infrastructure (e.g., cell phone and online services) in support of the transaction.

From the individual's perspective, the increasing complexity and risk of managing multiple credentials threaten the convenience associated with online transactions. The number and diversity of service providers requires individuals to have multiple usernames and passwords, generally one for each provider. Many require complex and frequent password changes, a burden for both the service provider and the individual. This also imparts an increased risk of account compromise through insecure user management of account credentials and an increased likelihood of account abandonment.

The Identity Ecosystem must address this complexity as well as the underlying security vulnerabilities created by it. The Identity Ecosystem will promote federated identity solutions and foster the reduction and elimination of silos that require individuals to maintain multiple identity credentials. Individuals will benefit from the federated identity solution by establishing a small number of identity credentials that they can leverage across a wide variety of service providers. Organizational entities will benefit from the federated identity solution through the elimination of locally administered or application-specific credential issuance and maintenance.

Identity solutions can result in efficiencies for all parties due in part to reduction in fraud, help desk costs, and expensive paper-based processes. Further, identity solutions that leverage reusable infrastructure promote operational efficiency and further reduce the cost of implementation, thereby increasing the potential return on investment.

Identity solutions should be simple to understand, intuitive, easy to use, and enabled by technology that requires minimal user training. Service providers should perform usability studies to quantify ease-of-use. Many existing infrastructure components in use today (e.g., cell phones, smart cards, personal computers) should be leveraged to facilitate ease-of-use through their wide adoption, accessibility, and availability. Whenever possible, identity solutions should be "built-in" to the infrastructure to enable usability.

# Vision and Benefits

## Vision Statement

***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.***

The vision applies to individuals, businesses, non-profits, advocacy groups, associations, and governments at all levels. The broad applicability of the vision necessitates close collaboration across the private and public sectors. The vision also reflects the user-centric nature of the Identity Ecosystem, which provides greater transparency, privacy protection, flexibility, and choice to the individual. Lastly, the vision incorporates all of the guiding principles.

The identity solutions identified in the vision are primarily associated with **identification** (establishing unique digital identities) and **authentication** (associating an individual with a unique identity) technologies and processes. Trusted and validated attributes provide a basis for organizations that offer online services to make **authorization** decisions.

## Identity Ecosystem

The Identity Ecosystem is the embodiment of the vision. It is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities. Similar to ecosystems that we find in nature, it will require disparate organizations and individuals to function together and fulfill unique roles and responsibilities, governed by an overarching set of standards and rules. The Identity Ecosystem also enables anonymity for individuals interacting with services that do not require strong identification and authentication.

The Identity Ecosystem is composed of three layers:

- **Execution Layer** – Conducts transactions in accordance with the rules of the Identity Ecosystem.
- **Management Layer** – Applies and enforces the rules for participants in the Identity Ecosystem.
- **Governance Layer** – Establishes the rules required to function within the Identity Ecosystem.

### Ecosystem Components

The layers of the Identity Ecosystem identify the participants, policies, processes, and technologies required to provide trusted ***identification, authentication,*** and ***authorization*** across diverse transaction types. Listed below are the various participants in the Identity Ecosystem. It is important to note that a single organization need not fill each discrete role; rather, it is possible that an organization provides services that cross multiple roles.

- An **Individual** is the person engaged in an online transaction. A **digital identity**, which is a set of attributes, represents an individual in a transaction.
- A **non-person entity (NPE)** may require authentication in the Identity Ecosystem. NPEs can be an organizations, hardware, software, or services and are treated much like

individuals within the Identity Ecosystem. NPEs may engage in a transaction or simply support it.

- Individuals and NPEs are collectively referred to as the **subjects** of a transaction.
- An **Identity Provider (IDP)** is responsible for the processes associated with enrolling a subject, and establishing and maintaining the digital identity associated with an individual or NPE. These processes include identity vetting and proofing, as well as revocation, suspension, and recovery of the digital identity. The IDP is responsible for issuing a **credential**, the information object or device used during a transaction to provide evidence of the subject's identity; it may also provide linkage to authority, roles, rights, privileges, and other attributes.
- The credential can be stored on an **identity medium**, which is a device or object (physical or virtual) used for storing one or more credentials, claims, or attributes related to a subject. Identity media are widely available in many formats, such as smart cards, security chips embedded in PCs, cell phones, software based certificates, and USB devices. Selection of the appropriate credential is implementation specific and dependent on the risk tolerance of the participating entities.
- An **Attribute Provider (AP)** is responsible for the processes associated with establishing and maintaining identity attributes. Attribute maintenance includes validation, updates, and revocation. **Attributes** are a named quality or characteristic inherent or ascribed to someone or something (e.g., "Jane's age is at least 21 years"). An attribute provider asserts trusted and validated attribute claims in response to attribute requests from relying parties. In certain instances, a subject may self-assert attribute claims to relying parties; however, relying parties often depend upon attribute assertions from trusted third parties capable of validating the accuracy of claims. Trusted, validated attributes form the basis by which relying parties will authorize subjects.
- A **Relying Party (RP)** makes transaction decisions based upon its receipt, validation, and acceptance of a subject's authenticated credentials and attributes. Within the Identity Ecosystem, a relying party selects and trusts identity, credential, and attribute providers of their choice based on risk and functional requirements. Relying parties are not required to integrate with all permutations of identity media. Rather, they will trust an identity provider's assertion of a valid subject credential as appropriate. Relying parties also typically need to identify and authenticate themselves to the subject as part of transactions in the Identity Ecosystem.
- **Participants** refer to the collective subjects, relying parties, identity media, service providers, and NPEs within a given transaction.
- A **Trustmark** is a badge, seal, image or logo that indicates a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority. To maintain trustmark integrity, the trustmark itself must be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity. The trustmark provides a visible symbol to serve as an aid for individuals and organizations to make informed choices about the providers and identity media they use.
- The **Identity Ecosystem Framework** is the overarching set of interoperability standards, risk models, privacy and liability policies, trustmark requirements, and enforcement mechanisms that govern the Identity Ecosystem.
- A **Governance Authority** oversees and maintains the Identity Ecosystem Framework and defines the rules by which a product or service provider in the Identity Ecosystem attains trustmarks. In addition, the Governance Authority is accountable for certifying organizations that wish to become **Accreditation Authorities.**

- An **Accreditation Authority** assesses and validates that identity providers, attribute providers, relying parties, and identity media adhere to an agreed upon **Trust Framework**.
- A **Trust Framework** defines the rights and responsibilities of a particular set of participants in the Identity Ecosystem; specifies the rules that govern their participation; and outlines the processes and procedures that provide assurance. A Trust Framework considers the level of risk associated with a given transaction and its participants. Many different Trust Frameworks can exist within the Identity Ecosystem, as sets of participants can tailor them to their particular needs. However, the participants must align the Trust Frameworks with the overall Identity Ecosystem Framework.

The combination of these participants, and the standards and agreements among them, form the trust fabric that makes the Identity Ecosystem possible. The following sections provide a functional example of online transactions that take advantage of the Identity Ecosystem. The example addresses each layer of the Identity Ecosystem and demonstrates the benefits associated with adoption, such as:

- Availability of new and innovative services,
- Credential acceptance and trust among diverse industries and governments,
- Privacy enhancement,
- Process efficiency, and
- International applicability.

This example is not an endorsement of specific technologies or processes; rather, it is intended to articulate one of the many possibilities.

## Part 1: Execution Layer

The Execution Layer is the place where individuals, organizations and NPEs come together to interact in online transactions following established rules.

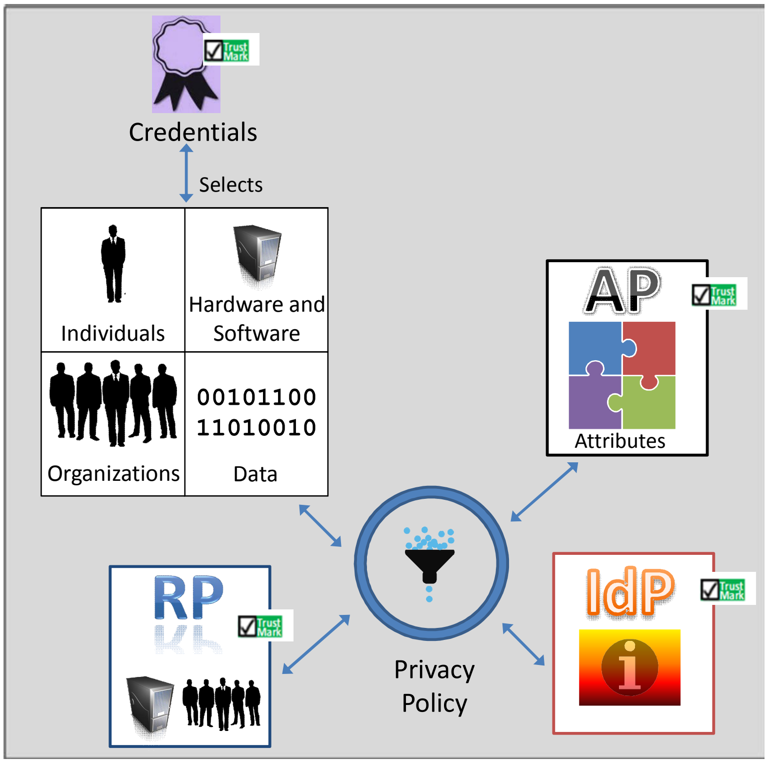

Figure 1: Execution Layer

As shown in Figure 1, an individual can make informed choices about which relying parties to trust aided by the trustmark they hold. When the individual accesses the online services of the relying party, the relying party may ask her to present a credential and attributes to support authorization of the individual's requested action. The relying party can request verification of the credential's validity and the associated digital identity of the individual from a certified identity provider; and validated attribute assertions from certified attribute providers. The user can also provide all validations directly to the relying party through the mediation of privacy-enhancing technology. Attribute providers may supply attribute values (for example, birth date is March 31, 1974) or attribute claims (for example, individual is older than 21).

NPEs, which include both the hardware and software involved in a transaction, also require rigorous identification, authentication, and authorization within this layer. Similar to individuals, NPEs must have a digital identity managed by an identity provider, and they can have attributes managed by an attribute provider. In Figure 1, individuals, organizations, hardware, software, and data authenticate to a relying party. The relying party must also authenticate to these subjects.

Consider the situation in which a woman requests medical information from the hospital that her husband has recently visited. She would like to know the results of his last blood test using a hospital website. The hospital requires that any such requests be authenticated using a strong credential. In addition, the hospital requires patient approval prior to releasing personal medical information to individuals. The woman has the confidence to perform this transaction online using her cell phone because all parties involved are using a trustmark, which signifies that they adhere to the Identity Ecosystem Framework. She is able to conduct her transaction with minimal personal information exchange, since the hospital (RP) only requires her to reveal the necessary information to complete the transaction, and the authoritative sources of her credential (IDP) and patient approval (AP) only know the identity of the RP as appropriate.

The woman navigates to the hospital website to view her husband's test results. The website authenticates itself to her, so that she knows she is on the correct website and not sending information to an imposter. For a transaction of this level of risk, the hospital requires the individual to authenticate using a strong credential. The woman has a Public Key Infrastructure (PKI) certificate issued by her cell phone carrier (also her IDP). The certificate is stored on her cell phone and associated to her verified identity. The cell phone contains a Trusted Platform Module (TPM) that is used to authenticate the cell phone. The woman plugs her cell phone into her computer via USB cable to conduct the authentication. The hospital validates the authenticity of the credential, the digital identity and the cell phone. Next, the hospital obtains validation sourced from the husband's primary care clinic (AP) that he has approved that his wife can have access to his records. Using the clinic's assertion as proof of approval, the hospital then allows the wife to view the test results.

NPEs within the Identity Ecosystem have embedded identification and authentication processes that support online transactions. In the example, the participant's Internet Service Providers (ISPs) and hospital networks use Border Gateway Protocol Security (BGPSEC), Internet Protocol Security (IPSEC), and Domain Name System Security Extension (DNSSEC) to authenticate network traffic and transaction data. The developer of the software that the hospital uses to display the health information has digitally signed the software. Infrastructure owners and operators deploy these technologies without requiring the woman to be aware of their existence or how they are used, yet she benefits from the increased authenticity of the communications and data flow that occurs across the Internet infrastructure supporting this transaction.

This entire process executes rapidly; all automated processes, from first click to receiving the test results, are completed at the speed of the Internet.

### Part 2: Management Layer

The Management Layer is where individuals and NPEs acquire at least one credential to work in the Identity Ecosystem, and they affiliate with at least one identity provider. An individual acting within the Identity Ecosystem obtains a credential from an identity provider before he or she conducts transactions online. Identity providers validate the subject's physical identity and make sure that their digital identity accurately reflects the real world person or NPE. Next, identity providers associate a subject's credential to their digital identity. Finally, they provide identity validation to relying parties who accept the credential. Similarly, attribute providers will confirm, bind and assert attribute information about a subject.

In the case of the hospital transaction discussed above, the woman had to have already established and maintained a certified credential accepted by the hospital before accessing online services. In addition, her husband's primary care provider validated and maintained the appropriate attributes in the form of her husband's approval to release medical information. She had established her digital identity when she subscribed to a mobile service plan offered by a cell phone carrier. The cell phone carrier verified her identity based on defined identity proofing standards and issued her a credential on her cell phone that she could use within the ecosystem. When her husband signed the medical release authorization form, he provided her name and cell phone number. The hospital obtained an Extended Validation Certificate for its website to enable individuals to indicate that the website has not been spoofed. In addition, the hospital digitally signed their website software to prevent unauthorized modifications to their services. Software developers, ISPs, and hospital data center administrators obtained credentials enabling code signing and the use of BGPSEC, DNSSEC, and IPSEC.

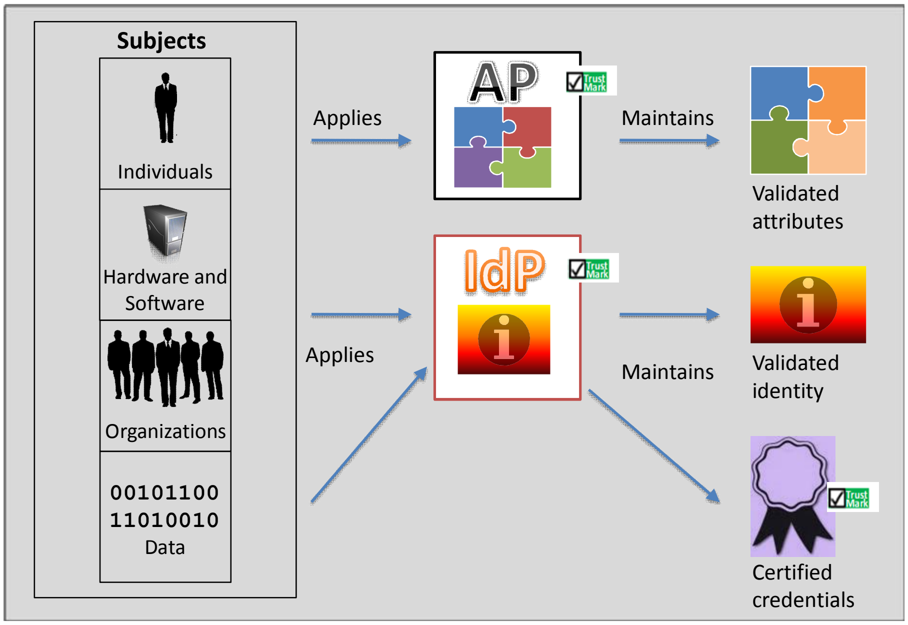

**Figure 2: Management Layer**

## Part 3: Governance Layer

The Governance Layer enables unaffiliated entities to trust each other's digital identities. A Governance Authority will establish the criteria for assessing and certifying Accrediting Authorities, who in turn assess and certify service providers. In addition, the Governance Authority will control the rules for trustmarks that indicate the service provider's standing as a participant within the Identity Ecosystem. The Identity Ecosystem Framework provides the overarching standards and laws that govern specific Trust Frameworks. Trust Frameworks identify the specific requirements associated with a particular set of participants and transactions within the Identity Ecosystem.

Assessment and validation services performed by the Accreditation Authority make sure that Identity Ecosystem providers apply the rules agreed upon under the Trust Framework. Upon successful validation, an Accreditation Authority will issue a trustmark to the provider, indicating that the appropriate mechanisms are in place. Before any participant, with the exception of individuals, can join the Identity Ecosystem, an Accreditation Authority must certify them. These assessments and the application of trustmarks foster trust among all Identity Ecosystem participants.

In the case of the hospital transaction discussed above, a Trust Framework was in place governing the relationships between the hospital, cell phone carrier, primary care clinic, and individual. This Trust Framework was based on the overarching standards in the Identity Ecosystem Framework. Using the Trust Framework as a guide, an Accreditation Authority had to certify each provider. The hospital first had to request certification to allow them to request and accept credentials issued by certified entities like the cell phone company. Likewise, the Accreditation Authority assessed and certified the woman's cell phone carrier as an identity provider. The physician's clinic also underwent assessment as an attribute provider. Each of these providers received a trustmark because of this certification. As a result, the participants in the Trust Framework were able to provide a valued online service to the individual in a secure and convenient manner.

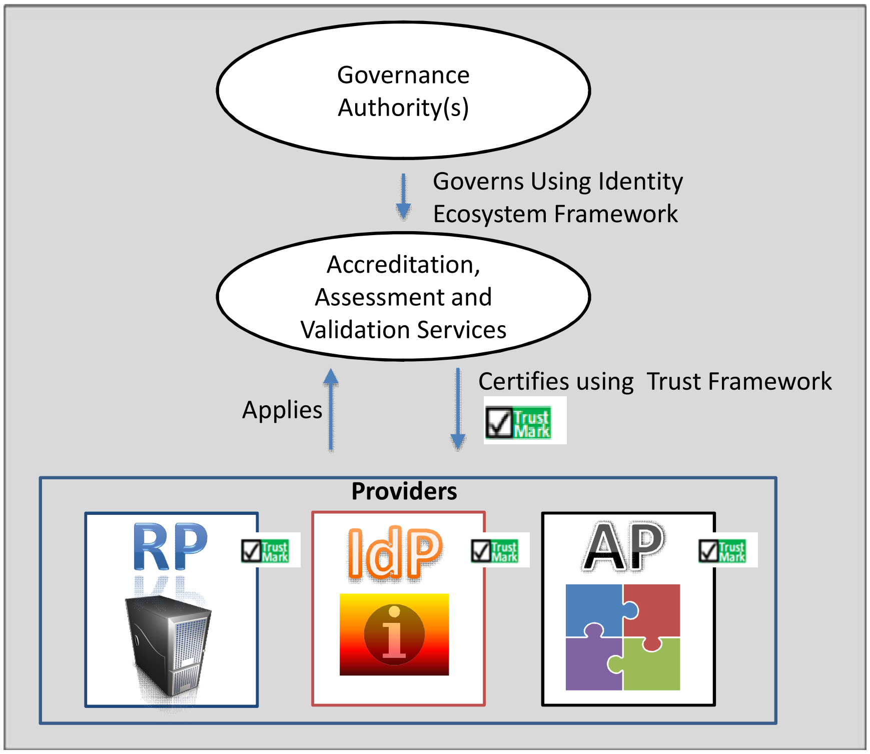
Governance Authority(s)
Governs Using Identity Ecosystem Framework
Accreditation, Assessment and Validation Services
Applies
Certifies using Trust Framework
Trust Mark
Providers
RP
IdP
AP
Trust Mark
Trust Mark
Trust Mark

**Figure 3: Governance Layer**

## Summary of Identity Ecosystem Characteristics

Looking across all three layers, the Identity Ecosystem will have the following characteristics:

- **Individuals and organizations choose the providers they use and the way they conduct transactions securely.** Relying parties determine authentication requirements, including credential types and attributes, based upon an evaluation of acceptable risk for a particular transaction or transaction type. The individual chooses his or her preferred identity, credential, and attribute providers, and the types and number of credentials he or she possesses based on desired privacy characteristics. Further, an organization or entity may choose to provide multiple services within the Identity Ecosystem.
- **Participants can trust one another and have confidence that their transactions are secure.** When necessary, identity providers authenticate participants involved in the transaction, providing secure identities to support the creation of various online communities in ways not possible today. Consistent risk assessment models allow flexibility for relying parties to set authentication criteria based upon a balance among security, risk, convenience, privacy, and ease of use. This approach allows the participants to tailor the requirements of a transaction (e.g., confidentiality, data and system integrity, content and site integrity, availability, and performance). The identity providers also appropriately identify and authenticate underlying infrastructure associated with the transaction, further promoting confidence.
- **Individuals can conduct transactions online with multiple organizations without sacrificing privacy.** Individuals can conduct transactions with multiple organizations at

their desired level of privacy. An individual has the choice to use a strong credential to authenticate to a transaction anonymously or a pseudonym without uniquely identifying himself. Organizations protect individual privacy by applying rules and ethics about the sharing of information, while protecting identity data provided to service providers. In addition, individuals will have the capability to request, obtain, modify and redact personal information.

- **Identity solutions are simple for individuals to use and efficient for providers.** The Identity Ecosystem achieves user convenience and simplicity by an authentication experience that reduces the need to log in using different credentials for different relying parties. The Identity Ecosystem reduces redundant processes for identity vetting, credentialing, and account management through new trust relationships and shared services.
- **Identity solutions are scalable and evolve over time.** Identity solutions are interoperable by using modular components and well-defined and widely accepted interface specifications. Such an environment allows service providers to upgrade or replace components without impact to the rest of the Identity Ecosystem. Best practices and guidelines are flexible and evolve to adapt to the changing technological, security, and privacy landscape.

## Benefits of the Identity Ecosystem

The value propositions for the participation of individuals, the private sector, and government in the Identity Ecosystem are closely intertwined. In other words, widespread adoption across these groups will increase the value derived by all parties participating in the Identity Ecosystem. At a national level, the value proposition is clear. Our economy and substantial components of our Nation's critical infrastructure rely heavily on the Internet. Any actions that increase the security of cyberspace also positively influence our national security posture and the stability of our economy.

### Benefits for Individuals

Individuals of all ages use the Internet for a wide variety of reasons and with varying degrees of technical familiarity. This Strategy acknowledges that individuals expect a safe and easy-to-use online environment that includes privacy protections and does not create undue burden for individuals. As a result, a focus on user control and experience is paramount for successful execution of this Strategy. Benefits of Identity Ecosystem for individuals include:

**Envision It!**

An individual learns of a new and more secure way to access online services using a strong credential provided by a trustworthy service provider. He learns that his cell phone carrier, bank, and local governments will all be offering credentials that will work with his personal computer. Upon further research, he also discovers that his email provider, social networking site, health care provider, and local utility companies accept the strong credential. He reflects upon his choices and selects the credential provider that provides him with the most personal convenience.

- **Security.** Providers secure data, specifically data tied to an individual's digital identity, using built-in technologies and processes that are common, well understood, and that evolve to protect the individual's interests. Security is further improved by the robust identification and authentication of the parties, both person and non-person entities, for a given transaction.
- **Efficiency.** Individuals have more online services increasing their transaction options, saving time and increasing productivity.
- **Ease-of-Use.** Enabling solutions are intuitive, easily understood, accessible, and widely available. Individuals are not required to manage different passwords for every online service.

- **Confidence.** Improved identity solutions reduce fear of fraud due to identity theft or misrepresentation. Individuals are comfortable conducting business online and voluntarily participate in online transactions.
- **Privacy.** Providers do not collect, use, or share personal information when not required, and providers protect data from inadvertent or unauthorized disclosure at all times. In addition, personal information is not linked or linkable across transactions or service providers except as necessary.
- **Choice.** Individuals choose from a variety of service providers and digital credentials. Individuals may also choose to take part in transactions of all kinds, including those that are anonymous and those that require a verified identity, using the same or different credentials.

**Envision It!**

An energy company partners with a new and innovative identity provider to extend its energy management services. Both companies are trustmark-approved. Using a smart card issued by the identity provider (and also used to access other online services at the discretion of the individual), an individual accesses the energy company's website to view the status of his home's energy consumption. The website allows individuals to view the energy intake of high-consuming devices such as refrigerators, microwaves, and stoves. The individual notices that the power attributed to a particular device is higher than normal, indicating that the device may need to be fixed or replaced.

## Benefits for the Private Sector

The private sector includes businesses, non-profits, non-government organizations, advocacy groups, and associations. This Strategy enhances the private sector's ability to be agile, innovative, and responsive to market dynamics. The Strategy supports the private sector's efforts to enrich the user experience associated with online transactions. The Strategy also provides the private sector with the flexibility to determine the type of credential and attributes required for its customers. It recognizes that the benefits for the private sector will vary based on the organization's role in the Identity Ecosystem (e.g., as a service provider or relying party).

The private sector has much to gain through the adoption of the Identity Ecosystem. Benefits include:

- **Security.** Improved identity solutions reduce losses associated with fraud and better protect intellectual property and confidential information transmitted between parties. Alignment with the Identity Ecosystem can help provide brand protection.
- **Efficiency.** The consistency and accuracy of trusting digital identities improves productivity by, for example, reducing paper-based processes and help desk costs associated with account management and password maintenance. This increase in productivity could enhance shareholder value and increase competitiveness.
- **Confidence.** Achievement of the vision reduces fear of security breaches, thereby increasing the confidence of both the private sector and its partners in online transactions. Entities share a common understanding of risk and can make and communicate decisions accordingly.
- **Privacy.** The Identity Ecosystem reduces the complexity of managing and maintaining employee or customer personal data, thereby reducing risk relative to privacy breaches.
- **Innovation.** Introduction of the Identity Ecosystem creates new market opportunities in the form of new and innovative services, particularly those associated with higher risk and user-centric transactions. Early adopters can leverage innovative solutions within the Identity Ecosystem to differentiate their brands in the marketplace.

## Benefits for Government

All levels of government (i.e., Federal, state, local, and tribal) have the opportunity to serve as a leader in the implementation of the Identity Ecosystem. The Strategy recognizes that the security of online transactions is a public safety concern, and government must become involved to help improve the security posture of those participating in online transactions. Government benefits include:

- **Security.** Security is improved by increased trust in the appropriate identification and authentication of the parties, both person and non-person entities, for a given transaction. Online trust reduces cyber crime, improves the sustainability and integrity of networks and systems, and raises overall consumer safety levels. The Identity Ecosystem may assist law enforcement in investigating fraudulent activity that arises out of misuse of the system.
- **Efficiency.** The Identity Ecosystem allows government to serve its citizens and perform its functions more efficiently and transparently through consistent and accurate services and reduction in redundant processes.
- **Innovation.** A clear commitment from the government to promote trusted identities through early adoption and research and development leads to innovation in the marketplace that assists in securing cyberspace over time. Further, many existing technology initiatives, such as the Smart Grid and Health Information Technology, will benefit from the Identity Ecosystem implementation, encouraging further innovation.

**Envision It!**

A large national emergency erupts on the coastline and a call for support results in a flood of first responders at the emergency site. A federal agency is able to share information with and provide direction to state and local officials, utility providers, and emergency first responders from all over the country about the local event. Each participant in the information exchange uses a credential issued by his employer to log into the information-sharing portal to see the status of events in each respective area. Resources are deployed more quickly and with greater focus based on the information shared.

# Goals and Objectives

This section outlines goals and objectives to achieve the vision. Each goal addresses specific barriers in the current environment and defines the desired outcome. The related objectives for each goal provide additional supporting details.

There are four goals for the National Strategy for Trusted Identities in Cyberspace:

- **Goal 1:** Develop a comprehensive Identity Ecosystem Framework.
- **Goal 2:** Build and implement interoperable identity infrastructure aligned with the Identity Ecosystem Framework.
- **Goal 3:** Enhance confidence and willingness to participate in the Identity Ecosystem.
- **Goal 4:** Ensure the long-term success of the Identity Ecosystem.

The first two goals focus on designing and building the necessary governance and infrastructure to deliver online services securely. The third goal targets the necessary privacy and security protections and the education and awareness required to encourage adoption. The fourth goal establishes the structure and priorities to promote continued development and improvement of online identity security over time.

## Goal 1: Develop a comprehensive Identity Ecosystem Framework.

The Identity Ecosystem Framework guides the development of individual Trust Frameworks within the Identity Ecosystem. The Identity Ecosystem Framework will enable policy development and creation of robust practices for identity assurance across the Nation. The Identity Ecosystem Framework will also be flexible enough to accommodate the differing needs of the various participants in the Identity Ecosystem.

The Identity Ecosystem Framework should address the following barriers in the current environment:

- Service providers base their current authentication processes and requirements on individual business uses rather than a commonly understood notion of the risk associated with a transaction.
- There is an absence of a common framework to help establish trusted identities among participants in a broad, diverse landscape of online transactions.
- Existing standards do not drive sufficient interoperability across service providers.
- Concerns regarding liability for providing identity, credential, and attribute-related services have prevented development of the Identity Ecosystem.

### Objective 1.1: Establish comprehensive identification and authentication standards based on defined risk models.

The development and adoption of national standards of practice for online identification and authentication processes is critical in promoting consistency and trust in a distributed online environment with radically diverse transaction types and diverse identity management solutions. A risk model provides the capability to assess and tailor the level of security to the risk of the transaction; it also provides a common understanding of the level of assurance required based upon the types of threats and the potential severity of impacts when conducting a particular type of transaction. These standards, which may be based on existing efforts within international standards organizations, will define how to remotely authenticate and govern, manage and execute the digital identity of users, devices, and services over open networks to provide the desired level of interoperability and security commensurate with the risk of the transaction. The standards must also enable consistency, while maintaining agility to adapt as security threats evolve and the market innovates.

### Objective 1.2: Define participant responsibilities in the Identity Ecosystem and establish mechanisms to provide accountability.

Key elements of the Identity Ecosystem Framework are defining the rights and responsibilities of the various participants in the Identity Ecosystem and establishing an enforcement mechanism, if participants do not carry out these responsibilities. To define these responsibilities, the Federal Government must address liability issues within the Identity Ecosystem (e.g., should there be liability caps or floors on identity providers if credentials are fraudulently used?). These liability concerns have historically prevented organizations from providing and using identity and attribute provider services. The Federal Government needs to establish new or amend existing policies and laws to address these liability concerns and to establish the enforcement mechanisms that provide accountability.

Multiple entities currently enforce online security and privacy standards in a distributed fashion across both government and the private sector. Any new laws and policies must maintain the flexibility of this approach, while harmonizing a diverse and sometimes conflicting set of requirements that currently prevents interoperability and trust across communities.

## Goal 2: Build and implement interoperable identity infrastructure aligned with the common Identity Ecosystem Framework.

Creating trusted identities among participants in the Identity Ecosystem requires an infrastructure to support the interactions between transaction participants. This goal seeks to address the following barriers in the current environment:

- Slow implementation pace of identity solutions to provide secure, streamlined access to online services.
- Lack of diverse identity solutions capable of operating successfully together.
- Lack of secure, convenient, user-friendly options for user authentication and identification.
- The high relative implementation and management costs that have prevented a rapid growth in the market for identity and attribute provider services.

### Objective 2.1: Continue government leadership and adoption of the Identity Ecosystem Framework.

Government is both a significant provider and customer of a large number of valuable online services. Through this role, Federal, state, local, and tribal governments must continue to lead by example and be early adopters of identity solutions that align to the Identity Ecosystem Framework. Over time, this will help drive consumer expectations and demand for improved identity solutions across all online services. Government must also continue to leverage its buying power as a significant customer of private sector to enhance the business case and marketplace for these solutions.

### Objective 2.2: Promote swift deployment of solutions to implement the Identity Ecosystem Framework.

In order to realize the benefits of the Identity Ecosystem Framework, the Federal Government must promote and incentivize swift implementation of private sector solutions and business models that support trusted identities for online transactions. Efforts in this area will drive innovation in the marketplace and will quicken the pace of adoption of existing identity solutions and promote the development of new ones. The Federal Government should work with industry to organize, coordinate and fund pilot programs, which could transform the landscape by expanding into a broad web of multiple interoperable offerings across numerous communities and transaction types.

### Objective 2.3: Promote broad availability of solutions to strengthen user value.

A limitation of the current environment is that most identity solutions apply to a specific business process or service, which results in a lack of identity portability and interoperability across services. This stove-piped approach offers little value or convenience to users. The Federal Government must take steps to incentivize all levels of interoperability among participants in the Identity Ecosystem, encourage the creation of a diverse set of identity providers both inside and outside of government, and promote the widespread use of Identity Ecosystem solutions by all citizens.

## Goal 3: Enhance confidence and willingness to participate in the Identity Ecosystem.

Individuals and organizations must have confidence in the Identity Ecosystem and be willing to participate in it. This Strategy will promote confidence via mechanisms that address privacy protection, data integrity, and data confidentiality associated with identity solutions. The Strategy will also address awareness and education of both the risks associated with poor identification and authentication approaches and the ways in which identity solutions mitigate those risks.

The Federal Government is already doing much work in this area, and the intention is to leverage existing activities to the greatest extent possible. The Federal Government will couple messaging on general awareness with the information necessary to drive long-term changes in behavior. The knowledge and awareness activities should be mindful of the different perspectives of individuals, government, and the private sector.

This goal seeks to address the following barriers in the current environment:

- Concerns regarding personal privacy and the potential for unauthorized collection, aggregation, use, or release of identity information.
- Concerns regarding the protection of intellectual property.
- General lack of awareness regarding trusted digital identities.

### Objective 3.1: Improve privacy and transaction security through fair and responsible management of information and solutions.

Implementation of the Identity Ecosystem Framework must provide strong privacy and security protections to individuals in addition to creating clear rules and guidelines concerning the circumstances under which a service provider or relying party may share information and the kinds of information that they may share. These protections support the general obligation to protect users from online threats and assure individuals of the protections to facilitate willing participation in online transactions. Efforts in this area will address inconsistencies in the way that service providers manage information across transactions in the current environment. New privacy protections will shift the current model of application-specific collection of identity information to a distributed, user-centric model that supports an individual’s capability to assert personal attributes without being required to provide all identifying data. Service providers should use, collect, share, and retain information only as required to accomplish the purposes of the transaction. In addition, the Federal Government should work with state governments and the private sector to establish redress mechanisms to adjust inaccurate personal data and provide consumers with a streamlined ability to change incorrect data in one place and have it propagated to the providers of their choice.

### Objective 3.2: Provide awareness and education to enable informed decisions.

Education and awareness efforts will raise the understanding of the importance of trusted identities and will teach users how to create trusted identities. The Federal Government, working with the private sector, will customize these education and awareness efforts to the relevant demographics. Meaningful consumer choice among multiple identity media and service providers and awareness of the available choices are a crucial aspect in promoting participation on the part of individual users. Programs associated with this Strategy must provide awareness of the available market choices, their benefits and protections for the user, and the information necessary to make an informed choice.

There is also a growing need for awareness and education across the service provider community, particularly as it relates to the service provider's responsibilities associated with the overall security and privacy protections established by the Identity Ecosystem Framework. The Federal Government, in conjunction with service providers, will develop educational resources for use by both large and small businesses in order to promote consistency and alignment within the Identity Ecosystem. As with the American public, service providers must understand not only their role in the solution, but also the role of other parties and the ways that these respective roles foster trust. Awareness and education activities must leverage existing programs and engagement efforts and begin as soon as possible to address known security risks and best practices. They must also evolve as the identity infrastructure matures to ensure that materials and messaging are in alignment with the current environment.

## Goal 4: Ensure the long-term success of the Identity Ecosystem.

Due to the global nature of the economy and the Internet, the scope of the Strategy extends beyond national boundaries. Governance and leadership is required at the national and international levels to create the Identity Ecosystem, including standards development, research and development, and program coordination among public and private efforts. The Federal Government must undertake leadership, coordination, and collaboration roles in order to strengthen digital identities both nationally and internationally, to promote the next generation of identity solutions, and to establish the Federal programs to execute this Strategy.

This goal seeks to address the following barriers in the current environment:

- Insufficient resources focused on U.S. participation in national and international standards efforts.
- The need for additional resources for research and development efforts to create innovative identity technologies.
- The need for improved coordination across multiple programs and efforts within the Federal Government related to trusted digital identities.

### Objective 4.1: Coordinate Federal Government efforts associated with digital identities (both domestically and internationally).

The United States has mobilized and established momentum in building a resilient and secure cyber infrastructure across government and private sector. In place are effective public/private collaboration mechanisms, as well as operational programs to provide solutions that mitigate the effects of cyber malfeasance. The Federal Government should build on these efforts and identity the appropriate coordination mechanisms for digital identity issues. Further, as cybersecurity policy is becoming a matter of diplomacy, activities under the Strategy intend to address the increased importance of international policy efforts. The Federal Government, by leading and coordinating national efforts, as well as collaborating on international policy efforts, can drive a unified approach to trusted digital identities.

### Objective 4.2: Increase participation in technical standards development nationally and internationally.

Continued progress and innovation in digital identities and the creation of a global, trusted infrastructure is reliant upon significant U.S. participation in national and international standards development. Today's environment is driven by a global economy, with transactions occurring without regard to physical or political boundaries; the infrastructure developed under this Strategy will, to the extent feasible, be interoperable among these environments, while also respecting the laws and policies of different nations. Efforts under this Strategy must facilitate the development of technical standards for the identification and authentication of organizations, devices, software, data, and users.

### Objective 4.3: Drive innovation through aggressive, focused Research and Development (R&D) efforts.

The Federal Government should align existing and future Federal R&D efforts with the requirements of the Identity Ecosystem. To be successful, the U.S. must focus on technologies and R&D that have the potential to shift the security, reliability, resilience, and trustworthiness paradigm to benefit those who conduct themselves responsibly online. Additionally, the Federal Government must continue to promote the transfer of the government's sponsored R&D results related to the Identity Ecosystem to the commercial sector. Lastly, R&D must be inclusive and highly collaborative among partners from varying communities and disciplines across the public and the private sector in order to develop innovative solutions rapidly.

# Commitment to Action

Implementation of the Identity Ecosystem requires a complex set of actions across policy, process, technology, and education disciplines that affect a wide range of autonomous stakeholders. This Strategy represents tasks that Government and the private sector can do together to improve identities in cyberspace. Successful implementation requires joint ownership, collaboration, and accountability across all participants in both the public and private sectors and across national borders. This section identifies High Priority Actions that are critical items for implementation. The Federal Government is committed to the actions herein and will move forward as a leader, first adopter, and enabler of the Identity Ecosystem.

## High Priority Actions

The High Priority Actions that are listed here are not all encompassing of the actions needed to meet goals and objectives. Rather, they represent a summary of many work streams that the Federal Government will later detail in a Trusted Identity in Cyberspace Implementation Plan (see Action 2).

### A1 Designate a Federal Agency to Lead the Public/Private Sector Efforts Associated with Advancing the Vision

The Federal Government must organize to provide leadership, accountability, and guidance in the implementation of the Identity Ecosystem. The White House will select an agency and hold it accountable for coordinating the process and organizations that will implement the Strategy. Many other Federal agencies will have implementation responsibilities associated with their respective mission areas, and some of these are outlined in this document. However, the Lead Agency will:

- Assess progress against the goals, objectives and actions stated herein;
- Ensure the government leads by example in developing and supporting the Identity Ecosystem;
- Coordinate collaboration and joint-owned actions across private and public entities, as they work to develop the Identity Ecosystem;
- Support interagency collaboration and coordinate interagency efforts associated with achieving the vision; and
- Establish private sector advisory mechanisms and engagement strategies.

The Lead Agency must actively seek interagency collaboration, harness multi-disciplinary and multi-sector contributions and provide collective thought leadership across Government in order to harmonize and integrate various public and private sector policies and efforts. The Office of the Cybersecurity Coordinator within the EOP will continue to lead inter-agency policy development specified in this action plan. The Lead Agency will work closely with the Office of the Cybersecurity Coordinator. In addition, the Lead Agency will participate in the Federal CIO Council and ensure coordination across existing and future relevant initiatives.

### A2 Develop a Shared, Comprehensive Public/Private Sector Implementation Plan

The actions in this section set the foundation and tone for future activities that public and private sector partners will execute together; yet these are not enough. The Federal Government will develop a detailed Implementation Plan that stresses swift deployment of the Identity Ecosystem, while identifying and planning for near and long-term actions. Development and socialization of the Implementation Plan with public and private sector stakeholders will leverage interagency processes and forums in place today to maintain momentum.

The planning of action tasks, timelines, dependencies, and owners will center on reuse of existing investments, standards, innovation, and best practices from all stakeholder communities. Public and private sector collaboration will be required to identify integration points with existing efforts, enable advisory and communication channels, assign individual and joint task owners, determine timelines, task inputs and outputs, and define critical success factors to ensure completeness and traceability to the Goals and Objectives. Both public and private sector actions will be coordinated through the Implementation Plan.

## A3 Accelerate the Expansion of Government Services, Pilots, and Policies that Align with the Identity Ecosystem

The Federal Government must be a role model and early adopter of the Identity Ecosystem. All levels of Government will play a part in the adoption of the Identity Ecosystem for government services. As a major provider of services spanning individuals, private sector, and other governments, the Federal Government is positioned to enable high impact, high penetration Identity Ecosystem services. The sheer scale and diversity of service offerings and stakeholders provide an excellent proving ground for the Identity Ecosystem. Additionally, knowledge transfer of lessons learned from Federal initiatives and other pilot projects to the private sector will increase the number of attempted adoptions and their overall success rate.

Government-led and funded programs, including pilots that implement ecosystem-aligned Federal services, are a crucial part of this action. The Federal Government will pay special attention to the potential for pilots in the health care, communications, information technology, Defense Industrial Base, energy, and financial sectors and with state government. To promote alignment, the Lead Agency in coordination with the White House should review internal Federal investments in identity solutions to maximize alignment to the Identity Ecosystem. In addition, Federal pilots should be extended wherever feasible to include transactions that support both the private sector and individuals. The Federal Government will also consider participation in international pilots to promote global alignment of Identity Ecosystem functions.

The Federal Government should expedite the adoption and implementation of existing policies and mandates that support the Identity Ecosystem. Many Federal policies and directives support the deployment of authentication infrastructures for both NPEs and individuals. These can immediately help reduce cyber threats against Government, businesses, and individuals. In addition, the Federal Government has many existing identity programs, pilots and roadmaps that align with the Identity Ecosystem, such as the implementation of Homeland Security Presidential Directive 12, the Federal Public Key Infrastructure, DNSSEC, IPSEC, and the Federal Identity, Credential, and Access Management Roadmap activities. These should be heavily leveraged and accelerated where possible to support the Identity Ecosystem.

## A4 Work to Implement Enhanced Privacy Protections

The Federal Government will work with the private sector to determine approaches to implement the FIPPs. Early focus on privacy policy, process, and technology implementation will enable Identity Ecosystem participants to develop best practices, guidance and standards that will enhance the way entities collect, use, protect, transmit, retain, and destroy personally identifiable information. The Federal Government will create detailed action plans to strengthen privacy policy and implementation such that Identity Ecosystem providers will:

- Provide concise, meaningful, timely, and easy-to-understand notice to end-users regarding collection, use, dissemination, and maintenance of PII in identity assurance solutions.
- Limit collection and transmission of information by Identity Ecosystem participants to the minimum information necessary to fulfill the purpose of the transaction.
- Limit secondary uses of individual data collected and transmitted in the Identity Ecosystem.
- Limit retention of data to the period necessary for the provision of the services to the individual end-user for which the data were collected, except as otherwise required by law.
- Minimize data aggregation and linkages across transactions in the Identity Ecosystem.
- Provide mechanisms to allow individuals to access, correct, and delete information, as well as minimize barriers to individuals' termination of their relationships with Identity Ecosystem participants.
- Establish accuracy standards for data used in identity assurance solutions.
- Protect and securely destroy information when terminating business or overall participation in the Identity Ecosystem.
- Provide provision(s) of redress mechanisms to individuals who believe their data may have been misused.

The user-centric nature of the Identity Ecosystem presents opportunities for individuals to control and release their private data in truly innovative ways. The Strategy calls for actions that will shape the way users provide data to organizations, as well as ways in which users can enjoy simple and effective mechanisms to update, publish, and redact their private information.

## A5 Coordinate the Development and Refinement of Risk Models and Interoperability Standards

A set of risk-based models and assessment tools will support the decisions that organizations make to determine how they will operate within the Identity Ecosystem. The risk model will minimize ambiguity associated with the ways in which risk-based controls are determined and established nationwide. Standards that cover interoperability requirements, trustmark criteria, and accreditation will pave a path that supports choice across solutions, ultimately accelerating Identity Ecosystem adoption. All detailed actions associated with Identity Ecosystem standards will build on existing efforts undertaken by the Federal Government, trust framework providers, private sector, standards bodies, and international organizations.

Standards established within the Identity Ecosystem will require incorporation of privacy guidelines. They should also require, to the extent feasible, adoption of protocols that minimize the ability to link or aggregate transactions and transaction data across Identity Ecosystem participants and relying parties, while maintaining individual transaction history, integrity, and auditability. Standards development, adoption, or enhancement will support autonomy and choice among Identity Ecosystem providers and flexibility within industry sectors, while facilitating cross-sector and international interoperability.

## A6 Address the Liability Concerns of Service Providers and Individuals

This Strategy defines an Identity Ecosystem where one entity vets and establishes identities and another entity accepts them. To date, the appropriate apportionment of liability has prevented the cross-sector issuance and acceptance of identity credentials. The Federal Government must address this barrier through liability reform in order to establish the multi-directional trust required by transaction participants. The Identity Ecosystem promotes models that mitigate liability to an acceptable level relative to the benefits associated with participation in the ecosystem. In addition, the Strategy will further sustain existing liability models and strengthen legislation to protect individuals and deter organizations from holding lawful individuals responsible for losses caused by unauthorized transactions.

## A7 Perform Outreach and Awareness across all Stakeholders

Individuals and the private sector play critical roles in the success of the Identity Ecosystem. They must understand the risks, benefits, and how to participate in the Identity Ecosystem. As a result, educational information should be easy to obtain and understand. Public and private sector outreach and awareness activities will include efforts to educate individuals and organizations on poor identification and authentication techniques and how to improve on them. The Federal Government will develop these efforts in conjunction with the National Initiative for Cybersecurity Education (NICE). Federal agencies will incorporate digital identity trust and protection into existing and future outreach and awareness programs. Private sector and other government entities have a distinct role to play in communicating with their specific stakeholders, both individuals and other organizations.

The Federal Government in collaboration with the private sector will tailor awareness campaign activities based on audience type, and focused across varied media outlets to make individuals aware of appropriate security behavior now and in the future. The long-term campaign should promote awareness of the activities, offerings, and providers in place to support the Identity Ecosystem and ultimately promote participation. Any mechanisms developed to support this high priority action will measure effectiveness of the messaging and the Identity Ecosystem to inform further enhancements.

## A8 Continue Collaborating in International Efforts

The Federal Government will increase commitment to the global activities associated with privacy and trusted digital identities. The Federal Government will prioritize and appropriately staff existing international efforts associated with trusted digital identities.

As discussed previously, standards development and adoption at the international level is a cornerstone of global commerce and information exchange. To avoid localized standards development and adoption, domestic efforts should endeavor to adopt international standards whenever they are consistent with domestic goals. Furthermore, information sharing and international forum and pilot participation will provide ongoing enhancement to the development of the Identity Ecosystem. Collaboration in international efforts is not only a Federal Government responsibility. The private sector shares responsibility for the Strategy’s implementation and adoption. Success of the Identity Ecosystem depends on participation from multi-national corporations and global providers in the use of federated identities that are interoperable and scalable to Internet levels.

The Federal Government will increase prioritization, coordination, and participation of government representatives, and encourage greater private sector prioritization, coordination, and participation of their representatives in international standards development activities related to the Identity Ecosystem. These activities will include international policy and technical working groups, forums, and councils performing relevant work. In order for the U.S. to collaborate internationally and benefit from the lessons learned, best practices, and interoperability of international integration, U.S. presence in these forums must increase and support standards that align with the Identity Ecosystem.

## A9 Identify Other Means to Drive Adoption of the Identity Ecosystem across the Nation

Widespread adoption of more robust identity solutions will likely not occur without comprehensive incentives. The Federal Government will take steps to evaluate the efficacy of economic incentives to private sector or individuals to spur adoption of strong, interoperable identity solutions. The Federal Government will consider incentive programs such as tax credits/breaks, cybersecurity insurance, grant programs, or loans for first adopters. The Federal Government should also analyze how it can better align identity solution requirements in existing grant programs against the Identity Ecosystem.

The Federal Government will also conduct economic analyses to evaluate needed regulatory changes within critical infrastructure sectors. In particular, the Federal Government will evaluate risks, costs, and benefits before recommending changes to certain transaction types within regulated sectors, such as requiring higher levels of authentication for credit card transactions.

# Conclusion

This Strategy provides a vision for how users, service providers, and other stakeholders can improve their use of digital identities in online transactions.  High-level actions are proposed that support the development and maintenance of governance, management, and execution-level activities needed to achieve the Identity Ecosystem.

Our reliance on cyberspace as a means to conduct business and exchange information will continue to grow in the years ahead, and with it our need to trust the identities of those with whom we interact online.  The protection of the identities of individuals and organizations while conducting online transactions is pivotal to protecting open commerce, promoting innovation, and securing our Nation's critical assets.  The Identity Ecosystem demonstrates the ability to protect individual rights, provide enhanced privacy, and prevent fraud to mitigate the risk of identity theft and malfeasant behavior online.

The Federal Government, in collaboration with individuals, businesses, non-profits, advocacy groups, associations, and other governments, must lead the way to improve how identities are trusted and used in cyberspace.  Ongoing collaboration between private and public sectors has already resulted in significant gains towards establishing Identity Ecosystem components.  However, much more remains to be done.

There is a compelling need to address these problems as soon as is practical, making progress in the short-term and planning for the long-term.  For the Nation to realize the vision of this Strategy and associated benefits, all stakeholders must come together in a collaborative partnership. The scope of this effort requires coordination across many boundaries and will require involvement and leadership from all sectors.

# Appendix A – Glossary

| Term | Definition |
|---|---|
| **Accreditation** | The authorization action; granting an authority to perform a defined service. |
| **Accreditation Authority** | Assesses and validates that identity providers, attribute providers, relying parties, and identity media adhere to an agreed upon Trust Framework. |
| **Anonymous** | Not named or identified. Anonymous transactions allow for information exchange between parties without the need to identify the parties involved. |
| **Attribute** | A named quality or characteristic inherent in or ascribed to someone or something. Attributes can include personal qualities (e.g. age), ambient information such as location, or certifications that serve as proof of a given capability. |
| **Attribute Provider** | Responsible for all the processes associated with establishing and maintaining a subject's identity attributes; they provide assertions of the attributes to the individuals, other providers, and relying parties. |
| **Authentication** | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. |
| **Authorization** | The official management decision to authorize operation of an information system and explicitly accept the risk operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed-upon set of security controls.<br>The act of approving or giving consent. |
| **Availability** | Ensuring timely and reliable access to and use of information. |
| **Confidentiality** | Preserving authorized restrictions on information access and disclosure to prevent disclosure to unauthorized individuals, entities or processes, including means for protecting personal privacy and proprietary information. |
| **Credential** | An information object created by a credential provider that provides evidence of the subject's authority, roles, rights, privileges, and other attributes. The credential is normally bound to an acceptable identity medium. |
| **Cybersecurity** | Measures taken to protect computers, computer systems and networks, and data against unauthorized access or attack. |
| **Cyberspace** | The interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, mobile devices, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people. |
| **Device** | A physical construct, generally electronic, that is capable of storing and processing information, e.g., a Personal Computer, web server, mobile phone, or smart card. |
| **Digital Identity** | The electronic representation of an entity (e.g., a device, software, service, organization or individual) in cyberspace that is comprised of an information artifact or correlated information sets. |
| **Identity Ecosystem** | It is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities. Similar to ecosystems that we find in nature, it requires disparate organizations and individuals to function together and fulfill unique roles and responsibilities, governed by an overarching set of standards and rules. |

| Term | Definition |
|---|---|
| **Identity Ecosystem Framework** | Overarching set of interoperability standards, risk models, privacy and liability policies, trustmark requirements, and enforcement mechanisms that govern the Identity Ecosystem. |
| **Identity** | A unique physical being that identifies somebody or something. Identities can apply to persons or non-persons. |
| **Identity Assurance** | Means to ensure the integrity and authenticity of identity information. |
| **Identity Provider** | Responsible for the processes associated with enrolling a subject, and establishing and maintaining the digital identity associated with an individual or NPE. These processes include identity vetting and proofing, as well as revocation, suspension, and recovery of the digital identity. The IDP is responsible for issuing a credential, the information object or device used during a transaction to provide evidence of the subject's identity; it may also provide linkage to authority, roles, rights, privileges, and other attributes. |
| **Identity Medium** | A device or object storing one or more credentials, claims, or attributes related to a single subject, and in the case of a device, capable of transforming these information objects for specific uses.<br>Any credential, card, badge, USB, smart phone or other media, regardless of form factor, issued or authorized for identification purposes within online transactions. |
| **Identity Proofing** | The process of providing sufficient information (e.g., identity history, credentials, documents) to a service provider for the purpose of proving that a person or object is the same person or object it claims to be. |
| **Infrastructure** | Consists of the integrated technical components (e.g., hardware, software, networks, applications and protocols) required to deliver online services in accordance with the trust framework and the programs necessary to support them. |
| **Integrity** | Assurance that data has not been modified or deleted in an unauthorized or undetected manner. |
| **Interoperability** | The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user.<br>The ability of independent implementations of systems, devices, applications, or components to be used interchangeably. |
| **Level of Assurance** | The degree of confidence in the vetting process used to establish the identity of the individual(s) or device(s) participating in the transaction.<br>The degree of confidence that the individual who uses the credential is, in fact, the individual to whom the credential was issued. |
| **Non-Person Entity (NPE)** | An entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts. |
| **Online** | The state associated with the ability to connect and communicate with other networks, systems, computers, subjects or components in real time through the Internet. |
| **Privacy** | The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use, and disclosure of personal information. |
| **Relying Party** | A relying party is a provider of online services to a subject. Within the ecosystem, a relying party is responsible for interacting with credential, identity, and attribute providers as needed to verify parties with whom they exchange information. |

| Term | Definition |
|---|---|
| **Resilient** | Capable of withstanding change (e.g., attacks) without suffering permanent damage. The ability of a solution or service to return to its original state after a disruption occurs. |
| **Secure** | Online transactions are secure if the implementation mechanisms meet their predefined security objectives of correctly authenticating the parties to the transaction, prevent unauthorized access and release of data, assure availability, faithfully conduct and record any negotiation, and preserve confidentiality and integrity of information. Pre-defined security objectives vary widely depending on the need. |
| **Service Provider** | Service providers may provide an access gateway to the Internet, security services, storage or processing services, or access to information and applications or a combination of these services. |
| **Standard** | A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard. |
| **Transaction** | An electronic communication among two or more parties (e.g., business, negotiations, activities, etc.) of a discrete unit of work brought to the mutually agreed conclusion or settlement. The parties have an obligation to play their parts during the transactions and honor their commitments after the transaction. |
| **Trust Framework** | The underlying structure of standards and policies that defines the rights and responsibilities of the various participants in the Identity Ecosystem, specifies the rules that govern their participation, outlines the processes and procedures to provide assurance, and provides the enforcement mechanisms to ensure compliance. |
| **Trustmark** | A badge, seal, image or logo that indicates a product, device, or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority. To maintain trustmark integrity, the trustmark itself must be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity. The trustmark provides a visible symbol to serve as an aid for individuals and organizations to make informed choices about the providers and identity media they use. |
| **Voluntary** | Acting without compulsion or obligation. |

# Appendix B – Participants

Under development.

# Appendix C – FIPPs

## The Fair Information Practice Principles

In order to truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy.[8]

Articulated briefly, the Fair Information Practice Principles are:

- **Transparency:** Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

[8] Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.