THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Identity Management Strategy

May 21, 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the direction of the Executive Office of the President and following a comprehensive scoping effort, the President's National Security Telecommunications Advisory Committee (NSTAC) established the Identity Issues Task Force in November 2008 to explore the role of the Federal Government in Identity Management (IdM) and how it could serve as a catalyst for broad implementation. As such, the NSTAC proposes a broad approach to assist the United States in achieving a national, comprehensive IdM strategy through a broad and enduring partnership between Government and industry. Internally, the Federal Government can implement IdM policies and technologies to improve privacy, security, and confidence in its own networks and services. Beyond that, a need has emerged for a national, comprehensive IdM strategy that would recognize and protect the roles and interests of private citizens and commercial participants while enabling collaboration among key stakeholders.

A comprehensive national vision and strategy will help create an IdM infrastructure capable of managing digital identities in the evolving electronic environment facilitating confidence and trust. This new IdM environment could have profound political and social implications, significantly improving how citizens interact while simultaneously meeting their basic expectations of privacy and anonymity. In addition, a comprehensive national vision and strategy for IdM will substantially enhance the overall security and integrity of the national communications infrastructure.

During emergencies, Federal, State, and local Governments rely on the availability of trusted Internet and other communications systems. National security/emergency preparedness (NS/EP) users have the same characteristics as most Internet Protocol (IP) network users—they are nomadic and demand access to all services at any time. However, they also differ from ordinary users in that they demand priority access to these services so they can respond to events where lives and property are in imminent danger. Consequently, network operators and service providers must be able to verify the identity of NS/EP emergency responders. These providers need a mechanism to establish trust in an NS/EP environment, and IdM provides that mechanism. A lack of IdM capabilities could result in a situation where unauthorized users have access to NS/EP priority services, perhaps interfering with an emergency responder's ability to use those services to fulfill the mission. Consequently, it is in the Government's best interest to pursue the development of a federation of interoperable IdM processes. Such a federation of interoperable IdM processes would enhance identity trust, awareness and education among end users, providers and devices. This federation would strengthen trust relationships and enhance the Nation's security. Such a federation would involve three operational characteristics: (1) interoperability; (2) Trust Anchors; and (3) Choice-based participation. A strong IdM system, based on robust trust in the Internet infrastructure and design, increases consumer confidence and ensures the Government's ability to rely on the Internet and other communications systems for commercial activities and security operations.

The evolving threat environment, coupled with the increasing reliance on communications networks, requires the development of a national, comprehensive Identity Management vision, strategy, policy and implementation procedures.

Both Government and the private sector are engaged in this area and are working toward individual solutions to IdM challenges to achieve the goals and overarching objectives for an IdM strategy addressed here. Although these efforts may be individually beneficial, they do not achieve the level of coordination, efficiency, and scope needed to create a holistic, integrated national IdM strategy for the mutual benefit of Government, industry, and society.

Commercial IdM service providers exist today and will likely increase in number, expand their roles and offerings, and develop business opportunities to meet the growing national IdM need. The national IdM strategy must embrace commercial IdM service providers willing to collaborate with the Government to develop standards-based interoperability between Federal and commercial IdM processes.

Privacy and civil liberties are vitally important components of any successful national IdM strategy that includes a federation of interoperable IdM processes. The NSTAC does not define a specific solution regarding how privacy should be integrated into a national IdM framework, but a fully-formed, Choice-based approach is fundamental to meet the citizens' expectations regarding privacy, civil liberties, and the protection of sensitive information, and will warrant further study. Importantly, the details of implementation of how to identify and authenticate users will not be answered in this report, but aspects are discussed to establish the contextual basis for this work and extend support for the NS/EP process. End users must have the ability to make fully-informed choices about the protection and use of their sensitive information. The relationship of these important civil liberties and the benefits of an interoperable IdM process warrant further study.

The recommendations to the President address possible first steps for an approach to identify issues and solutions related to IdM. This report builds upon IdM recommendations of previous task forces, working groups, researchers, and international bodies as referenced within the text herein. In addition, the IdITF considered the extensive IdM research and development (R&D), policy development, and technical research conducted by numerous national and international standards bodies and organizations.

This study is consistent with, and extends the work of, the President's NSTAC on the 60-day review of the Nation's cybersecurity efforts. Based on these efforts, the NSTAC believes a comprehensive national identity strategy would provide the crucial foundation for achieving success in many wide-ranging cybersecurity initiatives. The NSTAC also believes that the current political and policy landscape is ripe for promoting a comprehensive national strategy to improve trusted identification. Implementing such a strategy will impede malicious actors from posing as legitimate users and exploiting these networks, thereby placing NS/EP capabilities and everyday commerce at risk.

In light of these circumstances, the NSTAC concludes that the Government, working collaboratively with the private sector, the public, and interested nations, should develop a comprehensive national IdM vision and strategy that meets the security, business, and personal needs of American society and addresses the organizational, programmatic, legislative, and cultural components of IdM.

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

1) ***Demonstrate personal national leadership in IdM to positively influence the national culture, attitude, and opinion toward IdM.*** Successful development and implementation of a national IdM vision and strategy requires national commitment across Government, industry, and individuals dependent on cyber applications.

2) ***Charter a national IdM office under specifically appointed and dedicated leadership, in the Executive Office of the President.*** This office must have powers to integrate and harmonize national IdM policies and processes, including those related to law enforcement and security, as well as physical and logical access controls. This office should seek active private sector participation in developing such policies and processes in order to succeed and to ensure that successful solutions are shared with the private sector, as appropriate.

3) ***Direct the newly created office to develop a coordinated programmatic agenda to implement a comprehensive IdM vision and strategy to address, at a minimum, four component areas, specifically: Government organization and coordination; public-private IdM programs; policy and legislative coordination; and national privacy and civil liberties culture.*** Because no existing Government office or organization is engaged in all areas and issues across the total scope of IdM, new approaches are required to harness the expertise and interests across all areas.

   With respect to Governmental organization and coordination, establish a single, authoritative and comprehensive IdM governance process with a dedicated mission and office under an accountable official reporting directly to the President, embracing all Federal policy, technology, and IdM application activities related to both screening and access controls. The established lead official should have control over defined IdM programs and resources across Government, including budget, as needed to advance Federal IdM under a single coherent strategy.

   With respect to public-private programs, direct the appropriate Federal Government departments and agencies to work with the private sector to develop and advance a comprehensive and progressive IdM Research and Development agenda, focusing on Government-civil IdM interoperability. This effort should seek to establish interface standards to enable IdM applications to access and securely operate on global communications networks. In addition, this effort should partner with industry to embed IdM solutions in identity-sensitive applications of all kinds, promoting standards-based public-private programmatic collaboration.

   With respect to policy and legislative coordination, determine what changes to policy and regulation should be made, and what legislative initiatives should be advocated to move quickly toward national IdM goals. Further, establish policy and a legal framework to support internal Federal activities and streamline Government-civil collaboration and partnership in support of those goals. In particular, the IdM office

should pursue legislative efforts to support National IdM governance, organization and authority needs, as appropriate.

With respect to national privacy and civil liberties culture, develop a comprehensive and sustained communications plan to promote IdM reflecting key national and social values and embracing the strong National conviction to protect privacy and civil rights of both initiating and receiving parties as the national IdM strategy is developed and implemented.

All four of these components must be acted upon to achieve needed IdM alignment within Government, and between Government and industry. Collectively, these efforts will provide the Presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM throughout the Nation.

1.0 SCOPE AND PURPOSE

The National Security Telecommunications Advisory Committee (NSTAC) proposes a broad approach to enable our Nation to achieve a holistic, comprehensive Identity Management (IdM) strategy through an enduring partnership between Government and industry. The increasing dependence on communications networks for conducting Governmental, commercial, and social transactions requires participants to establish their identities through digital data and potentially physical means. Identity Management (IdM) provides unique characteristics and attributes to any Entity (e.g., people, object, device, or organization). Trusted, strong identification of users, devices, and communications service providers has not been universally adopted in cyberspace. This lack of trusted identification enables harmful and/or malicious activity[1] and diminishes national security/emergency preparedness (NS/EP) capabilities,[2] endangering national and homeland security as well as individual privacy and security. Private sector owners and operators of the Nation's information technology (IT) and communications infrastructure, along with Government, have a vested interest in identifying and deploying solutions to help the Nation reduce the occurrence and impact of harmful activity on communications systems.

The increasing dependence on communications networks for conducting Governmental, commercial, and social transactions requires participants to establish their identity through digital means. Trusted, strong identification of users, devices, and communications service providers has not been universally adopted in cyberspace. This lack of trusted identification diminishes NS/EP capabilities, endangering national and homeland security as well as individual security and privacy.

IdM covers a broad scope, including both digital and physical identification of individuals, applications, devices, objects, and information.

The purpose of this report is to identify Federal Identity Management (IdM)[3] policies and Government roles and responsibilities most likely to create a large-scale demand for strengthened IdM capabilities and practices by the private sector and individual users. In collaboration with Government and private sector

[1] "Banks Test 'Text Messaging' Security" Investor's Business Daily (08/10/07) P. A4 ; Howell, Donna
Banks and brokerages have been on the hunt for just the right balance between convenience and cost to boost log-on and transaction security for customers. Tokens have been one solution to reinforcing banking security, as users type an up-to-the-minute passcode that is displayed on a token. Thieves' efforts are thus thwarted from logging on as a user, even if they know the user's name and password. Financial firms are also considering sending users a one-time pass code via text messages to their mobile phones, or by an automated phone call that would eliminate the use for tokens. Passcode generators can also be built into cell phone handsets. Since most consumers have cell phones, sending mobile notifications could be a viable authentication measure. A built-in credit card authentication option is also being considered by financial institutions. The card would display a one-time passcode once a pressure-sensitive area of the card is touched. VeriSign's Fran Rosch says this technology will undergo pilot tests and reach a sizeable distribution by next year.

[2] "Information Technology Progress Impact Task Force Report on Convergence," *President's National Security Telecommunications Advisory Committee (NSTAC).* May 2000. http://www.ncs.gov/nstac/reports/2000/Convergence-Final.pdf.

[3] For the purposes of this report, Identity Management (IdM) is the structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use, and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices (*T SG17 Q6 Identity CG. International Telecommunication Union [ITU]*).

officials and technologists, the President's National Security Telecommunications Advisory Committee (NSTAC) Identity Issues Task Force (IdITF) explored the following topics:

- Functional identity requirements;
- Current Government IdM initiatives;
- Potential impact of IdM on Government priorities;
- Current domestic and international IdM standards adoption; and
- Creation of a process to develop, evaluate, and coordinate national comprehensive IdM strategies.

In the context of this IdM approach, Government and the private sector must commit to improve, to the extent possible, planning and execution in these areas. Sensitivity to public opinion in matters involving personal privacy and the proper roles—and limits—of Government must be taken into account. The recommendations are intended to present strategies and processes that improve privacy, relative to the status quo, while expanding the potential scope and scale of national IdM efforts, through establishing auditable and transparent privacy safeguards. Specifically, the recommendations herein promote a balanced public-private IdM strategic approach offering opportunity for business participation, standards development, and interoperability within and among Government and the private sector entities.

2.0 BACKGROUND

Federal, State, and local Governments, international bodies, private sector organizations, and individual end users depend on robust, reliable and functional communications networks for NS/EP and other business and personal needs. The Government and private sector rely upon these networks[4] increasingly for daily transactions (e.g., the provision of healthcare, emergency response services, commercial activities, and e-Government services). Numerous sources[5] show that these networks—and the Governments, people, devices, and the applications that rely on them—are under daily and sustained attacks. These attacks threaten core U.S. national communications objectives, including national security, law enforcement, public safety, and protection of intellectual property, and impair the availability and integrity of communications networks for NS/EP. In addition, they enable hostile disinformation capabilities, denial of service attacks, and malicious virus and spam attacks, all of which result in the general abuse and exploitation of communications networks by nation states and individual actors alike.

> The evolving threat environment, coupled with the increasing reliance on communications networks, requires a national, comprehensive Identity Management vision and strategy.

Both criminal and state-sponsored actors try to capture identity information. They subsequently use to gain unauthorized access to systems and information. The absence of strong identity controls makes it easy for them to get the information they need. The most common example of an inadequate identity control is a weak password (which is often 'password'). Captured identity information may be used to spoof communications networks' Authentication[6] processes to gain unauthorized access to networks and information. This increases the potential for theft, fraud, and the manipulation or disruption of finances, intellectual property, and other sensitive information. If information such as dates of birth and social security numbers are used as the basis of identity, and are compromised, recovery is difficult and sometimes impossible.

Recent studies by Government[7] and think tanks[8] have recognized the relationship between cybersecurity and IdM. Although this relationship has not yet been defined or described in detail, it clearly exists and current policy efforts related to broader issues of cybersecurity should be extended to IdM.

Inadequate identity control can negatively affect our communications infrastructure and all those who rely on it. A successful IdM strategy can help protect that infrastructure. As this strategy is adopted, there will be recognizable benefit in every identity-sensitive application. An effective

[4] For the purposes of this report, the term 'networks' includes Internet Protocol (IP)-based networks, digital communications, and all telecommunications network systems. Please see Appendix D for the definition of *Internet.*

[5] Various sources cite current cyber incident information and statistics, including us-cert.gov, sans.org, govtech.com, and cert.org.

[6] For the purposes of this report, *Authentication* is the provision of assurance of the claimed identity of an entity.

[7] *National Science and Technology Council*, Identity Management Task Force Report-2008, www.ostp.gov

[8] *Center for Strategic & International Studies*, Securing Cyberspace for the 44th Presidency, 2008, www.csis.org

IdM strategy can be a critical enabler for several Federal homeland security priority agenda items, including:[9]

- Protecting information networks;
- Improving intelligence capacity;
- Protecting civil liberties;
- Protecting Americans from terrorist attacks and natural disasters; and
- Protecting and modernizing critical infrastructure.

For example, IdM plays a key role in the healthcare reform agenda, promoting the adoption of online record-keeping and technology innovation initiatives, including widespread broadband access and an open Internet to improve access to healthcare while reducing healthcare costs.[10]

NS/EP, business, and even personal requirements drive the need for IdM and are linked to the evolution of the Internet as a critical infrastructure that supports vital processes in Government, business, and society. Transactions often occur over distances, where the sender and receiver do not share a common security framework or risk tolerance. Ubiquitous global networks have permitted the emergence of new functionality and efficiencies, but their full potential cannot be realized without a way to ensure their information is secure and their transactions are with trusted parties. Consequently, the ability of security organizations to differentiate between authorized users and intruders has become imperative.

Beyond network-based concerns, the ability to identify persons and objects for physical access control is part of the total need of IdM. The NSTAC addressed this issue in 2003.[11] The NSTAC's perspective on IdM should apply to both domains. Therefore, all references to interoperability of processes, applications, and systems in this report apply to both the physical and logical aspects of IdM.

The benefits of IdM extend beyond protecting the infrastructure and its users from malicious actors. Implementation of practical, large-scale IdM processes can also motivate users to take greater advantage of the functionality available, which in turn can stimulate further innovation. The ability to help all stakeholders appreciate these benefits will be essential to success and in some cases will require external advocacy and outreach programs. The benefits include:

- Expanded access to goods, services and information;
- Reduced process latency and error;
- Increased productivity and efficiency; and
- Cost savings.

[9] Going beyond securing communications networks and commerce, IdM could be used to help enforce immigration laws and improve border security, without adversely impacting lawful residents.
[10] The White House Agenda. http://www.whitehouse.gov/agenda/.
[11] The President's National Security Telecommunications Advisory Committee, "Vulnerabilities Task Force Report on Trusted Access," January 27, 2003.

The ubiquitous nature of the Internet and its application as a tool to meet Government and private sector mission needs underscores the increasing importance of IdM. The current environment requires collaboration among the Government and relevant stakeholders to ensure the development of a comprehensive, national IdM strategy.

The increasing emphasis on cybersecurity, healthcare technology innovation, and financial services initiatives has made key stakeholders interested in a broad IdM approach that addresses the full spectrum of issues and communities. This 'critical mass' has stimulated a greater awareness of IdM concerns, leading to opportunities for IdM policy development and implementation. With this awareness comes a need for Government to implement an outreach effort to ensure individuals have accurate and reliable information about how IdM can help them take full advantage of available technologies.

2.1 Privacy

A national IdM strategy must address personal privacy. Requiring identification for anonymous activity (for example, most Web browsing) could pose privacy risks by exposing Personally Identifiable Information (PII) to unauthorized third parties, who could then aggregate the information and link it to particular individuals. However, the implementation of an effective IdM strategy should enhance consumer privacy by increasing consumer control over personal information, strengthening information security, reducing unwanted intrusions such as spam, and improving transparency regarding how information will be used. Successfully strengthening identification processes while preserving privacy and civil liberties requires a delicate balance. To achieve this end, all participants in the design and implementation of a national IdM strategy should embrace the resolution of privacy concerns as a fundamental charge.

The NSTAC does not define a specific solution regarding how privacy should be integrated into a national IdM framework, but a fully-formed, Choice-based approach is fundamental to meet the citizens' expectations regarding privacy, civil liberties, and the protection of sensitive information. The NSTAC believes that all major participants should collaborate on an IdM strategy that establishes rigorous and auditable policy and technology frameworks while simultaneously ensuring identity privacy. This consideration of privacy applies broadly within Government, between the Government and commercially sensitive activities, and across society.

3.0 IDENTITY MANAGEMENT AND ITS USES

An identity is a representation of an Entity (such as an end user, a subject [as in law enforcement and security applications], an object, a device, or an organization) by which the entity is known in some context. The contexts considered in this report involve a broad array of infrastructures used for communications, transactions, or control of resources or facilities. Any entity may have one or more identity claims. A single identity may also be associated with multiple Entities. IdM includes discovery of and access to authoritative identity sources, and involves the life-cycle management and use of identity data elements to enable Attribution,[12] Authentication, and other identity-based services. IdM provides the means to authenticate the identity claims of Entities requiring identification on communications networks.[13] These claims include multiple roles (such as citizen, spouse, parent, customer, and patient) and range from commercial to social activities, and require participants to establish their identities through digital identity data and, in some cases, physical means.

The benefits that adoption of a comprehensive national IdM strategy would bring are far-reaching, as highlighted below.[14]

[12] For the purposes of this report, *Attribution* is the association of descriptive information bound to an entity that specifies a characteristic of an entity (such as condition, quality or other information associated with that entity) to that particular entity (NSTAC 2009).

[13] Rutkowski, Anthony, December 2008, "A Global Perspective on Identity Issues."

[14] Choice-based participation is crucial so that end user have a clear choice in whether or not to participate in the IdM federation and in determining the degree of Authentication commensurate with the level of sensitivity of their transactions. In some cases, end user choice will be linked to particular identity-sensitive applications. Applicants may be willing to voluntarily enroll in such applications, and provide certain, otherwise private, information as a condition of the enrollment process, if they expect to realize some benefit in doing so.

Identity Management Benefits

IdM processes and devices must be seen as valuable and useful by end-users. Those processes and devices must provide key positive incentives, such as passing through airports more quickly or gaining direct and secure access to Government systems online, so that voluntarily providing PII offers something of value. Advantages and cost savings will increase as IdM technology becomes more ubiquitous. The development of a comprehensive national IdM strategy would provide significant, tangible benefits to Government, industry, and the general public, such as:

- Reduced identity theft even with increased use of electronic commerce and e-Government;
- Reduced financial loss and improved recovery from identity fraud;
- Increased consumer confidence in Internet Protocol (IP)-based networks should result in the increased use of these networks for commercial transactions and thereby produce greater efficiencies at lower costs;
- Enhanced physical access controls and security screening processes;
- Cost savings through greater adoption of on-line applications for Government and commercial services requiring in-person identity verification;
- Recognizable, credible, and interoperable identities being made optionally available for all citizens, following essential industry and Government standards and applicable laws;
- Greater identity attribution without violation of citizens' privacy rights;
- More electronic value chains that can simultaneously promote U.S. innovation and international trade;
- Improved extensibility and interoperability of a smaller family of ID tokens and systems, benefiting both ID-dependent businesses and consumers;
- Streamlined and more secure access to the whole range of identity-sensitive applications, from law enforcement and security screening to e-commerce and access controls, including via Web-based processes never before possible. For example:
  - Secure Internet access to health services with improved privacy of personal medical records;
  - Enhanced secure e-pharmaceutical services (Web-based ordering, mail delivery), which could reduce total healthcare costs through greater efficiency; and
  - Consumer banking.
- Helping disabled home-bound users to live fuller lives by enabling them to participate in healthcare, commerce, and social services without the need for in-person identity verification; and
- Improved online safety for minors.

Increasing global complexity has yielded an evolving identity environment reaching across diverse domains. If IdM stakeholders do not address the fundamentals now, then more isolated IdM systems will emerge and it will become far more difficult to adopt viable, comprehensive, interoperable IdM solutions in the future.

3.1 IdM in the Context of National Security/Emergency Preparedness (NS/EP)

IdM has great potential to help fulfill national security, law enforcement, public safety, communications, security, and business and social needs. In addition, IdM advances are critical to NS/EP efforts because they help protect the networks, secure proprietary and Personally Identifiable Information (PII), and support Authentication assurance. Federal, State, and local Governments rely heavily on digital communications for NS/EP purposes. Improved trust through development of a robust federation of interoperable IdM processes would enhance the ability of public officials to provide key NS/EP services.

For example, the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) use simple Personal Identification Number (PIN) based and subscription based access mechanisms to authenticate authorized users but these methods do not preclude unauthorized use of the system. As GETS and WPS transition to an open Internet or Internet-like environment, a higher level of assurance (for example, confidence in the identity of NS/EP users) would provide for protection against unauthorized use.

A number of key technical and policy capabilities to improve IdM for NS/EP communications include the development of a holistic IdM infrastructure, improved interoperability under a federated identity system, and the development of scalable and extendible technical architectures.[15]

3.2 IdM in the Context of Cybersecurity

IdM is one of the most critical foundations of cybersecurity. Without robust IdM capabilities, achieving cybersecurity goals will prove difficult.

IdM is one of the most critical foundations of cybersecurity. IdM vulnerabilities allow malicious actors to exploit networks and information. The current administration's commitment to broadening transparency across the Government will likely have cybersecurity implications and intensify the need for a federation of interoperable IdM processes. Without robust IdM capabilities, achieving cybersecurity goals will prove difficult. As the Federal centralized management of cybersecurity matures, solutions will emerge for integrating IdM within the communications and IT infrastructure in a way that balances security and privacy.

[15] 2008 Research and Development Exchange Workshop Proceedings, September 2008, "Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment."

4.0 PROBLEMS AND IMPEDIMENTS IN THE CURRENT OPERATING ENVIRONMENT

Today's Internet originated in a closed environment in which a secure framework for managing identity was not required. As the Internet grew beyond its original closed environment, the need for a secure identity framework became more apparent. Existing identity credentials are weak and typically depend on both the context and application for which they were initially developed. In most cases, such identity credentials cannot be used in other situations or environments. For example, a patient may use a bank card to access funds at the bank or pay for a doctor visit, but the card cannot be used to verify the patient's insurance information. The lack of a uniform approach to establishing trust and confidence across different IdM federations impedes interoperability. The current dependence of identity assurance on the trust and confidence of a unique identity provider has played a large role in the maintenance of disparate IdM systems, effectively precluding interoperability.

Both the Government and the private sector have made significant progress in isolated areas of IdM. However, these positive efforts in Government and industry are not yet coordinated within an overarching strategic framework.

The successful development of a comprehensive interoperable IdM strategy requires overcoming cultural, technical, strategic, and economic problems. These problems extend to the Government, the private sector, and individuals. Both the Government and the private sector have made significant progress in isolated areas of IdM. However, these positive efforts in Government and industry are not yet coordinated within an overarching framework. There are four areas of concern that must be addressed in pursuit of a comprehensive IdM strategy, specifically:

- Social factors;
- Commercial factors;
- Technological factors; and
- Government factors.

The social factors include the following:

- The socially-acceptable limits of Government-sponsored IdM activity have not been rigorously established, nor effectively validated with the private sector or the public. Absent defined limits, the Government risks pursuing technologically-attractive initiatives that may be socially undesirable.
- Cultural sensitivity to the prospect of a national identity card complicates the adoption of IdM processes and needs to be accommodated.
- Historically, both the private sector and the public have considered IdM technology processes to be intrusive. Before this resistance can be overcome, a comprehensive cost-benefit analysis in support of IdM system development and implementation must be conducted. First and foremost, the Government must offer the private sector and the

public a trusted, easy-to-use, well-understood process that can protect privacy. Second, the Government must articulate the benefits that the IdM strategy can offer to the public, the private sector, and the Government, and make a convincing argument that a ubiquitous IdM infrastructure will be worthwhile.

The commercial factors include the following:

- Any broad federation of interoperable IdM processes must be sufficiently attractive to the general public (that is, these processes must be simple to use and understand). With these attributes, the private sector will be:
  - Encouraged to develop business applications that make deployment of the IdM capabilities economically feasible; and
  - Able to ensure public acceptance of processes involved and actions demanded of them.[16]
- Business cases must be developed that support emergence and sustainability of large-scale, commercial IdM processes; this has not yet been done.

Technical factors include the following:

- In today's environment, the lack of standards between independently-sponsored and managed IdM systems inhibits interoperability and extensibility.
- The various IdM federations do not share a uniform approach to establish trust and confidence across different IdM federations, including the vetting processes and identity validation.
- There are numerous Certificate Authorities[17]; in many cases, certificates do not interoperate with each other.

Government factors include the following:

- Government separates IdM programs designed to support security screening from those designed to facilitate the delivery of goods and services and access to information. This approach causes duplication of effort, inhibits efficient management, and artificially divides activities and applications across Government.
- The absence of a central IdM governance process across all Governmental IdM activities, including identity-sensitive[18] applications, inhibits Government's ability to holistically manage and advance IdM in support of the full range of security and efficiency drivers.

The Government can become the catalyst for addressing all of these factors and can ultimately implement a comprehensive, national IdM strategy.

[16] *Ibid.*
[17] "NSTAC Report to the President on Physical Assurance of the Core Network", FOUO, dated November 6, 2008. Certification Authority Services: Services infrastructure and facilities involved in providing identity management and chain of trust validation for critical Internet services and transactions."
[18] An application wherein accesses and privileges of an individual, organization or group are variable, depending on their identity attributes.

5.0 NEED FOR AN IDENTITY STRATEGY

Current Government and private sector IdM systems are numerous and stove-piped, causing redundancy and inefficient and uncoordinated IdM efforts. Private sector owners and operators of the Nation's information and communications technology (ICT) infrastructure, along with Government, have a vested interest in exploring potential solutions to reduce the frequency and impact of attacks on the Nation's network infrastructure and services, especially during emergency situations. The evolving and ubiquitous nature of the Internet demonstrates the criticality of ICT infrastructure to global security and stability.

A successful IdM strategy should promote a policy of interoperability and coordination of disparate systems to ensure both ease of use and security. If the private sector and Government develop a federation of interoperable IdM processes enhancing identity trust, awareness, and education among end users, providers and devices, then these strengthened network trust relationships will enhance the security posture of the United States. A comprehensive strategy and supporting federation of interoperable IdM processes would lead to more efficient use of Government and private sector resources, promote growth and innovation, and improve end user convenience when engaging in transactions across various domains.[19] Additionally, an effective, comprehensive IdM strategy will improve the management of PII and ensure the implementation of strict controls to protect unauthorized disclosure of privacy information across different domains.[20]

A successful IdM strategy should promote a policy of interoperability and coordination among disparate systems to ensure both ease of use and security. If the private sector and Government develop a federation of interoperable IdM processes enhancing identity trust, awareness, and education among end users, providers, and devices, then the these strengthened network trust relationships will enhance the security posture of the United States.

Currently, the international community is actively engaged in the debate on IdM. Specifically, digital identity is at the top of the Critical Information Infrastructure agenda of the European Union, with several member states pioneering projects and deployments in this area. The time is ripe for the United States to join the debate and leverage this opportunity to demonstrate leadership in the development of a unifying internationally interoperable solution.

[19] "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft," Organization for Economic Cooperation and Development (OECD). 27 January 2009.
[20] NSTC Subcommittee on Biometrics and Identity Management, September 2008, "Identity Management Task Force Report 2008."

6.0 COMPREHENSIVE IDM STRATEGY CHARACTERISTICS AND PRINCIPLES

Given the factors described above, a comprehensive IdM strategy developed jointly by Government and the private sector could be the first step toward developing a federation of interoperable IdM processes. Today, the IdM space is fragmented, affecting the availability, reliability, and accuracy of its processes.

A comprehensive IdM strategy must address the following categories of Entities:

- **People**. IdM includes a definable set of persons, who by their nature, will be everything from Federal employees, entitlement beneficiaries and individual citizens; to prospective foreign visitors to the United States and visa recipients; to criminals, fugitives from justice, and subjects of intelligence or counter-intelligence interest.
- **Digital IT Devices, Network Components, and Services**. IdM necessarily embraces the digital IT devices, network components, and services upon which identity attribution is predicated and through which it is communicated, such that each of these are strongly individually identifiable.
- **Software Components**. Authentication of trusted software components, such as operating systems and communication software, are critical to maintaining the chain of trust.
- **Objects**. Beyond the humans whose identities must be verified, and the hardware and software elements supporting the identification and verification processes, inanimate objects may also be verified and tracked, including: (a) material and goods entering the United States via air, land, or sea portal; (b) sensitive controllable objects used in commerce (such as pharmaceuticals or radioactive materials); and (c) digital rights or other objects of interest. This could extend to digital data and multimedia objects, including database records and documents.

Interoperability at the national and global level is critical to supporting multiple IdM solutions across communities and enables trust relationships within larger federations. The global information environment is the medium across which all identity-based transactions are conducted on network systems. Interoperability in physical access requires adoption of standardized credentials or other access protocols.

A verifiable Trust Anchor[21] methodology available to Government, the private sector, and social groups will create a mechanism all can use to issue authentic identities associated with a particular Trust Anchor. Essential Trust Anchor attributes include the abilities to trace:

- The asserted identity of some object or person back to the Trust Anchor; and
- The application to root sources and stores of digital identity data, both local and network-based.

[21] For the purposes of this report, a Trust Anchor is defined as an authoritative entity that has responsibility over verifying an identity.

Choice-based participation is crucial so that end users can decide whether or not to participate in the IdM federation and determine the degree of Authentication commensurate with the level of sensitivity of their transactions. In some cases, end user choice will be linked to specific identity-sensitive applications. If they anticipate some benefit to enrolling in such applications, individuals may be willing to provide certain, otherwise private, information as a condition of the enrollment process.

A successful federation of interoperable IdM processes would support an overarching, comprehensive IdM strategy with broad applications across a spectrum of communities and services and involve three key operational characteristics: (1) Interoperability; (2) Trust Anchors; and (3) Choice-based participation.

A comprehensive national IdM strategy must accommodate various levels of assurance to meet the diverse transaction needs. IdM must therefore provide a wide variety of enrollment options, identity data vetting/proofing capabilities, privacy protection capabilities, and Authentication mechanisms for nomadic users.

Additionally, a comprehensive national IdM strategy involves a key systemic characteristic—accountability—where all involved parties adhere to agreed-upon, standard procedures and processes, validated periodically with consistently applied rules (with appropriate consequences when users do not adhere to them). This ensures that all users respect the rules of the federation of interoperable IdM processes and diminishes the probability of exploitation of the system infrastructure.

Commercial IdM service providers exist today and will likely increase in number, expand their roles and offerings, and develop business opportunities to meet the growing national IdM need. The national IdM strategy must embrace commercial IdM service providers willing to collaborate with the Government to develop standards-based interoperability between Federal and commercial IdM processes.

A comprehensive IdM strategy should embody the following principles:

Privacy and Security

- Ensure security of process, data transmission, and storage;
- Ensure continuing emphasis on civil liberties and privacy;
- Provide secure management and use of PII and digital identities[22] where Government participation is non-intrusive, PII data storage is kept to a minimum, and disclosure of PII occurs only with the consent of the end user[23] (except where the Government, pursuant to appropriate legal process and other lawful circumstances, has the authority to access it);

[22] NSTC Subcommittee on Biometrics and Identity Management, September 2008, "Identity Management Task Force Report 2008."
[23] Microsoft-Scott Charney, 2008, "Establishing End to End Trust."

- Provide safeguards against unauthorized and unintended use, aggregation, dissemination and transfer of information;
- Maintain a network of vetted digital-identity repositories as Trust Anchors to assert identities within the federation of interoperable IdM processes;
- Provide oversight of standards processes required to support all IdM functions (to include aspects of digital identities and their repositories, standardized applications interfaces to permit 'plug and play' fielding of new applications, and processes of the supporting IT infrastructure);
- Ensure that IdM processes are auditable, enabling complete, automatic, and secure record keeping where appropriate;
- Ensure Choice-based participation among all stakeholders that accommodates different social customs regarding privacy and anonymity;[24] and
- Ensure that the security capabilities of IdM processes are auditable.[25]

Education & Outreach

- Conduct broadly-based and sustained outreach and education activities to encourage societal engagement and frame the case for defined, measurable benefits, recognizable by participating organizations and private citizens;
- Create an international liaison and outreach programs to seek synergies and opportunities for alignment with similar efforts abroad;
- Demonstrate a benefit for all targeted stakeholders, including Government, the private sector, society, and individual end users; and
- Encourage significant investment by industry and Government to ensure that the infrastructure required for implementation is in place.

Availability

- Implement easy-to-use technology[26] and create incentives for users to adapt the technology;
- Function in broad terms so that the strategy can be adapted for use in many communities throughout the private, civil, and public sectors, and globally while using interoperable applications to ensure consistency and efficiency;
- Provide extensibility that enables various communities to tailor identity profile attributes;
- Ensure ubiquitous availability, at global distances, of strong verification of stored digital identity upon demand;

[24] *Ibid*.
[25] *Ibid*.
[26] Excerpts adapted from the 2008 Research and Development Exchange Workshop Proceedings, September 2008, "*Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment.*"

- Provide standards-based connectivity, interoperability, and extensibility of the supporting information technology (IT) architecture; and
- Enable prospective application sponsors to develop, install, and operate applications in a way that permits the supporting IT grid to be seen as a freely available, ubiquitous service.

Policy and technology development in support of the above principles will help drive the realization of a comprehensive national IdM strategy.

Activities within the Federal Government

The size and complexity of the total Federal IdM enterprise is considerable. The enterprise will be highly diverse in both organization and relevance. Management structures and approaches would be broadly-based and much consideration should be given beforehand to ensure the efficient formulation and execution of the IdM strategy.

The Federal Government has expended substantial effort to consolidate and coordinate IdM technologies and approaches among the departments and agencies. However, to ensure the mission and to best achieve a comprehensive IdM strategy, the Federal Government would require a single office, independent of other departments and agencies, to oversee, coordinate, and direct IdM efforts across the entire Executive Branch. The interagency mission would be to develop, enable, and implement identity-sensitive applications with cross-organizational interoperability, coordinate configuration and change management, develop and adopt standards, and develop consistent legal and policy approaches to IdM across the Federal Government in the performance of all its missions. This process would provide a horizontal integration and coordination of many preexisting authorities, charters, responsibilities, and programs across the Federal Government. Through this process, the Government would also interact with commercial identity-sensitive activities that require interoperability with Federal IdM processes.

It is possible that the organizational model of a National Coordination Office (NCO) may be attractive as the home of Federal IdM governance. Current examples of this include the NCO for Networking and Information Technology Research*, the NCO for Space-Based Positioning, Navigation and Timing,** and the National Nanotechnology Initiative***. In all these cases, authorizing legislation has established a Federal charter and allocated funding. These organizations focus and direct the advancement of large-scale, broadly-impacting, and long-term technology issues of great national significance. This may be an effective way to achieve efficient and enduring management of IdM within Government, introduce the concept to the American public in optimal ways, and foster research into technologies. A successful IdM solution will operate on a global scale and support identity-sensitive applications to enhance the performance of Federal missions and citizen services.

* *http://www.nitrd.gov/*
***http://www.pnt.gov/*
*** *http://www.nano.gov/*

7.0 IDM STAKEHOLDER INCENTIVES

The development of a holistic, comprehensive IdM strategy could help coordinate efforts among the numerous private sector, Government, and individual stakeholders, while protecting and promoting their values and concerns, including:

- Secured communications for NS/EP needs;
- Increased security for online transactions and storage;
- Protection against fraud and identity theft; and
- Protection of privacy and civil liberties.

7.1 Private Sector and Individual User Incentives

Realistic potential exists for the private sector and individuals to benefit from participation in a federation of interoperable IdM processes. The current financial, political, and security environment provides a timely and unique opportunity to identify and prioritize critical IdM requirements. The shift towards digital communications, storage, and transactions in healthcare, banking, finance, commercial and retail activities, social networking, and print media has left individual end users increasingly at risk of identity theft, and private sector enterprises increasingly at risk of fraud in electronic commerce. Over the past 5 years, identity theft has emerged as the leading economic crime reported to the Federal Trade Commission Identity Theft Survey Report.[27] A robust federation of interoperable IdM processes would provide much-needed protection for consumers as digital communications supersede more traditional methods of commerce. In addition, in the modern business environment where corporate data may be stored on third-party premises and employees are increasingly nomadic and require access from any location, the ability to provide the appropriate level of access has become a business necessity.

To motivate the private sector and individual end users to participate in a Choice-based IdM federation, the scheme must offer something these users value when requiring them to provide identity information for the sake of secure Authentication. The private sector and the general public will not accept solutions that degrade or diminish privacy by failing to adequately protect stored data. A federation of interoperable IdM processes would enable end users to assert their identities with confidence.[28] It is ultimately desirable that end users retain control over their information, but some organizations may need to have access to particular data for certain operations, such as human resources. Solutions that degrade trust or diminish privacy by failing to adequately protect stored data will not be accepted by the private sector and the general public.

Although high levels of privacy are crucial in certain cases such as healthcare and insurance, even in these areas some services will constitute a higher risk and value than others and should have access control mechanisms appropriate to those risks and values. In addition, a federation

[27] Federal Trade Commission. "Identity Theft Survey Report," Prepared by Synovate. September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf.
[28] Microsoft-Scott Charney, 2008, "Establishing End to End Trust."

of interoperable IdM processes can include system maintenance of personal identity data that requires strong privacy protection; some users may expect to retain control over the use of at least some of this personal identity data, at least in some contexts.

Individual end users will not voluntarily participate in an IdM program if they perceive it to be inefficient, burdensome, intrusive, costly, unreliable, or of dubious or minimal value. To ensure effective participation by all stakeholders, the comprehensive IdM vision and strategy should offer a clear benefit to their missions or business processes. A successful comprehensive IdM vision and strategy balances the private sectors' and individual end users' desire for privacy protection with the universal need for improved security; it must also take into account that privacy and security needs may vary under different situations. To help build confidence in the federation of interoperable IdM processes, the private sector could develop an insurance model in the event of an identity breach to help build confidence among private sector and civil society stakeholders. The Government can help communicate the benefits of IdM by devoting resources to strengthen the sharing of threat information.

> Individual end users will not voluntarily participate in an IdM program if it is perceived to be inefficient, burdensome, risky, unreliable, or costly. A federation of interoperable IdM processes should offer a clear benefit to mission

In a Choice-based system, those who participate even minimally will be afforded a level of security they would not otherwise have, and their actions will also narrow the range of networks vulnerable to malicious actors. Private sector and individual end users will likely subscribe to an IdM solution if they feel the information they are providing online is protected. It is important for the Government to demonstrate the tangible security benefits of enhanced IdM capabilities while addressing privacy concerns and showing the other benefits IdM offers.[29] A federation of interoperable IdM processes that fails to provide significant security improvements and privacy protection will never gain the support of the private sector and individual end users.

> A robust federation of interoperable IdM processes would provide much-needed protections for consumers as digital communications supersede more traditional methods of commerce.

7.2 U.S. Government Incentives

Across the board, the U.S. Government stands to benefit from strengthened accountability and Attribution through robust IdM. The United States increasingly relies upon ICT for communications, military operations, commercial transactions, and banking and financial transactions. The Government and the private sector currently collaborate on several IdM

> The lack of coordinated United States leadership in international IdM efforts, coupled with the absence of a comprehensive national IdM strategy, places telecommunications-related national security and economic equities at risk.

[29] The ID Divide: Addressing the Challenges of Identification and Authentication in American Society. June 2008. (Swire and Butts).

efforts. Joint partnerships may help to broaden incentives for both sectors and improve efficiency.[30] Cost and liability risks must also be carefully examined in the context of a broad approach to an IdM strategy.

If the integrity of the infrastructure were compromised by intrusion and corruption, both economic and national security would be placed at risk. Specifically, exploitation of the Internet and other communications systems could lead to unauthorized disclosure of identity information and unauthorized access to Government systems with risks of disclosing sensitive, classified information.

During emergencies, Federal, State, and local Governments rely on the availability of trusted Internet and other communications systems. NS/EP users have the same characteristics as most IP network users—they are nomadic and demand access to all services at any time. However, they also differ from ordinary users as they need priority access to respond to events where lives and property are in imminent danger. Consequently, network operators and service providers must be able to verify the identity of NS/EP emergency responders. These providers need a mechanism to establish trust in an NS/EP environment, and IdM provides that mechanism. A lack of IdM capabilities could result in a situation where unauthorized users have access to NS/EP priority services, perhaps interfering with an emergency responder's ability to use those services to fulfill the mission. Consequently, it is in the Government's best interest to pursue the development of a federation of interoperable IdM processes. A strong IdM system, based on robust trust in the Internet infrastructure and design, increases consumer confidence and ensures the Government's ability to rely on the Internet and other communications systems for commercial activities and security operations.

> The Government and the private sector could benefit by collaborating to develop a federation of interoperable IdM processes.

[30] For lower levels of authentication, the Government currently partners with higher education entities and the Liberty Alliance, a group of private sector companies which works to develop open standard-based specifications for federated IdM and global identity theft prevention solutions, among other identity solutions, [www.projectliberty.org/liberty/about]. Management Board member organizations include: (1) America Online; (2) BT; (3) CA; (4) Fidelity Investments; (5) Intel; (6) Internet Society; (7) Novell; (8) NTT; (9) Oracle; and (10) Sun Microsystems. For lower levels of authentication, the Government current works within the Federal Bridge to collaborate with the private sector. [Spencer, Judith. "Identity, Credential and Access Management: The Government-wide Initiative," General Services Administration.]

8.0 FINDINGS AND CONCLUSIONS

The findings and conclusions in this section are derived from the above discussion and are presented here in direct support of the recommendations in Section 9.0 Recommendations below.

FINDINGS

Open and Secure Cyber Environment

- Based on the Identity Issues Task Force's examination of the IdM environment and previous reports, the Task Force believes that a robust identity strategy will provide a crucial underpinning for success in most wide-ranging cybersecurity initiatives. The Task Force also believes that the current political and policy landscape is ripe for promoting a comprehensive national strategy to ensure a trusted identification scheme for Entities (e.g., people, objects, devices, or organizations), coupled with Attribution[31] and Authentication assurance[32] requirements. Without such a strategy, malicious actors will continue to easily pose as legitimate users to exploit these networks and impact NS/EP capabilities and everyday business commerce.
- A comprehensive and sustained public outreach and education process will be necessary to support and nurture broad public acceptance of IdM. This process must emphasize the protection of the privacy rights of both the initiating and the receiving parties as a paramount objective.
- The administration's commitment to broadening transparency throughout Government will likely have cybersecurity implications and increase the need for an implementable federation of interoperable IdM processes.
- High levels of privacy are crucial in certain cases such as healthcare and insurance; however, even in these areas, some services will constitute a higher risk and value than others. Access control mechanisms should be available to accommodate the various levels of risks and values.

Global Interoperability

- The progress of national IdM in Government, business, and society will be commensurate with the extent to which it provides measurable and recognizable benefits to identity sponsors and end users. Therefore, identity-dependent applications should be encouraged to affiliate with an emergent national IdM process. At the same time, standards must be developed to support physical security applications within IdM processes.
- Global discovery and interoperability are essential to a successful federation of IdM processes and the need for U.S. engagement in various global forums is evident. The development of a national IdM strategy will help the Nation leverage its influence in international forums and promote the adoption of global, interoperable IdM standards in

[31] See Appendix C for definition.
[32] *Ibid*.

the best interests of the U.S. Government and private sector. Given the current international focus on IdM, the time is ripe for the United States to start influencing the debate.

- Despite laudable progress being made in many different areas across a broad organizational front, Government does not yet have a cohesive strategy to fulfill the potential of its considerable investment in all aspects of IdM, nor to meet the emergent need.
- The speed with which technology and media formats proliferate and expand contributes to evolving IdM challenges and the Government's stove-piped structural organization impedes internal interoperability.
- No uniformly-implemented approach exists to establish trust and confidence across different federations.
- There are inadequate drivers and incentives for uniform implementation to establish trust and confidence across different IdM federations.
- A federation of interoperable IdM processes, coupled with trust in the Internet infrastructure and design, would also increase consumer confidence and ensure the Government's ability to rely on digital communications systems for commercial activities and security operations.
- Individual end users will not voluntarily participate in an IdM program if it is perceived as inefficient, burdensome, intrusive, or costly.

Commerce

- Give the recent emphasis on efforts such as physical security screening, cybersecurity, healthcare technology innovation, and economic initiatives, consensus is emerging among key stakeholders in support of a broad IdM approach that covers a spectrum of issues, applications, and communities. This 'critical mass' is leading to greater awareness of IdM concerns and opportunities for IdM policy development and implementation.
- A comprehensive IdM strategy and supporting federation of interoperable IdM processes would enable more efficient use of Government and private sector resources, promote growth and innovation, and improve end user convenience when engaging in transactions across various domains.[33]
- Any broad interoperable IdM scheme must be sufficiently attractive to the general public (e.g., simple to use) to encourage development of interoperable IdM systems and business applications, thus making deployment of IdM capabilities economically attractive.[34] This will encourage the expanding role of commercial IdM service providers.
- It is important for a national IdM strategy to accommodate various levels of assurance to meet the diverse needs of the transactions being considered by both parties.

[33] "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft," Organization for Economic Cooperation and Development (OECD). 27 January 2009.
[34] Knode, Ron. "Identity Issues Report Precis: Digital Identity and Identity Management," 4 February 2009.

CONCLUSIONS

An Open and Secure Cyber Environment

- A strong degree of trust among all IdM stakeholders is crucial to the success of a federation of interoperable IdM processes.
- If IdM stakeholders do not address the fundamentals now, then more isolated IdM systems will emerge and it will become more difficult to adopt viable comprehensive and interoperable IdM solutions in the future.
- A federation of interoperable IdM processes should be voluntary and limit the amount of personal and proprietary information that is stored in a central location beyond the identity owner's control.
- Prior to implementation, the national IdM strategy security benefits—enhanced IdM security, personal convenience, expanded functionality, and improved organizational efficiency—must outweigh the costs, inconvenience, and privacy concerns.[35]
- The relationship between IdM efforts and cybersecurity will benefit from further exploration as the Federal centralized management of cybersecurity matures.
- Over time, as Federal organizational and programmatic approaches to cybersecurity mature, it will become increasingly important to identify the specific gaps and overlaps in policy and technology in the total relationship between cybersecurity and IdM.

Global Interoperability

- The United States must align domestic efforts with the ongoing work of the international community (e.g., standards bodies and foreign governments) and work with all stakeholders to ensure international interoperability.
- The national IdM need requires a network of interoperable, federated digital identity repositories. These will collectively support the establishment of Trust Anchors to confidently provide identity validation authority to support all needs.
- The Government should initiate a public-private partnership to help define the IdM space and work toward developing a federation of interoperable IdM processes that includes identity verification and validation, and Authentication of users, devices, objects and information under differing circumstances (e.g., general Web services, financial transactions, healthcare/insurance, and personal data access).
- A successful federation of interoperable IdM processes supports an overarching, comprehensive strategy with broad applications across a spectrum of communities and

[35] *The ID Divide: Addressing the Challenges of Identification and Authentication in American Society.* June 2008. (Swire and Butts).

involves three characteristics: (1) interoperability; (2) Trust Anchors; and (3) Choice-based participation.

- A national IdM strategy will require a comprehensive governance process, embracing the full scope and scale of IdM as described in this report.

Commerce

- A federation of interoperable IdM processes must demonstrate economic incentives/viability to ensure commercial participation and interoperability of identity service providers, private sector buy-in, privacy protections to ensure individual end user buy-in, and ease-of-use for general adoption.
- Industry and public acceptance are at the core of any progress in a federated IdM, as extended beyond the Government itself. This collaboration should involve a multi-faceted and sustained program of outreach, education, partnership, and incentives.
- Any emergent national IdM strategy must recognize and embrace the roles and participation of commercial IdM service providers of all types. Service providers should be invited to partner with Government to create an interoperable, standards-based IdM environment that can be extended to support all public and private IdM needs.
- A federation of interoperable IdM processes should leverage current and future Government and private sector investments, R&D, and Government agenda items to promote widespread adoption.
- A comprehensive IdM strategy should incorporate the key principles described in Section 7.0.

Government can help communicate the benefits of IdM by devoting resources and shoring up infrastructure and networks to protect NS/EP equities. In a recent letter[36] to the President in response to questions posed by his staff, the NSTAC offered prioritized recommendations regarding the greatest needs for cybersecurity at the national level. Those recommendations were based on historic reports and analyses conducted by the NSTAC in recent years. The first five of the eight stated priorities were:

- Adaptation of the current Federal Government organizational authorities for IdM to meet the desired need and optimize results;
- Information sharing;
- Identity Management;
- Standards; and
- Legal considerations.

The NSTAC finds that current IdM requirements encompass these priorities within a single, holistic vision. Both the Government and the private sector have performed great work

[36] Muller, Edward A. Letter dated 12 March 2009.

contributing to IdM goals and objectives. Service-specific systems and methods for retail, enterprise, communications, and other business applications proliferated with the growth of the Internet and IP-based technologies. However individually beneficial these are, these activities do not rise to the level of the coordination, efficiency, and scope of vision required for a holistic, integrated, national IdM strategy.

In light of these circumstances, the NSTAC concludes that the Government, working collaboratively with the private sector, the public, and interested nations, should develop a comprehensive national IdM vision and strategy that meets the security, business, and personal needs of American society and addresses the organizational, programmatic, legislative, and cultural components of IdM.

All four components of the total strategy listed below should be embraced and advanced collectively to achieve needed IdM alignment, effective collaboration between Government and industry, and broad social engagement. Taken together, these efforts will provide the presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM across the Nation.

National Integrated and Holistic IdM Vision and Strategy

9.0 RECOMMENDATIONS

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

1) ***Demonstrate personal national leadership in IdM to positively influence the national culture, attitude, and opinion toward IdM***. Successful development and implementation of a national IdM vision and strategy requires national commitment across Government, industry, and individuals dependent on cyber applications.

2) ***Charter a national IdM office under specifically appointed and dedicated leadership, in the Executive Office of the President***. This office must have powers to integrate and harmonize national IdM policies and processes, including those related to law enforcement and security, as well as physical and logical access controls. This office should seek active private sector participation in developing such policies and processes in order to succeed and to ensure that successful solutions are shared with the private sector, as appropriate.

3) ***Direct the newly created office to develop a coordinated programmatic agenda to implement a comprehensive IdM vision and strategy to address, at a minimum, four component areas, specifically: Government organization and coordination; public-private IdM programs; policy and legislative coordination; and national privacy and civil liberties culture***. Because no existing Government office or organization is engaged in all areas and issues across the total scope of IdM, new approaches are required to harness the expertise and interests across all areas.

   With respect to Governmental organization and coordination, establish a single, authoritative and comprehensive IdM governance process with a dedicated mission and office under an accountable official reporting directly to the President, embracing all Federal policy, technology, and IdM application activities related to both screening and access controls. The established lead official should have control over defined IdM programs and resources across Government, including budget, as needed to advance Federal IdM under a single coherent strategy.

   With respect to public-private programs, direct the appropriate Federal Government departments and agencies to work with the private sector to develop and advance a comprehensive and progressive IdM Research and Development agenda, focusing on Government-civil IdM interoperability. This effort should seek to establish interface standards to enable IdM applications to access and securely operate on global communications networks. In addition, this effort should partner with industry to embed IdM solutions in identity-sensitive applications of all kinds, promoting standards-based public-private programmatic collaboration.

   With respect to policy and legislative coordination, determine what changes to policy and regulation should be made, and what legislative initiatives should be advocated to

move quickly toward national IdM goals. Further, establish policy and a legal framework to support internal Federal activities and streamline Government-civil collaboration and partnership in support of those goals. In particular, the IdM office should pursue legislative efforts to support National IdM governance, organization and authority needs, as appropriate.

With respect to national privacy and civil liberties culture, develop a comprehensive and sustained communications plan to promote IdM reflecting key national and social values and embracing the strong National conviction to protect privacy and civil rights of both initiating and receiving parties as the national IdM strategy is developed and implemented.

All four of these components must be acted upon to achieve needed IdM alignment within Government, and between Government and industry. Collectively, these efforts will provide the Presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM throughout the Nation.

APPENDIX A:

TASK FORCE MEMBERS, OTHER PARTICIPANTS, AND U.S. GOVERNMENT PERSONNEL

APPENDIX A: TASK FORCE MEMBERS, OTHER PARTICIPANTS, AND U.S. GOVERNMENT PERSONNEL

TASK FORCE MEMBERS

CSC	Mr. Guy Copeland, Co-Chair
Nortel	Dr. Jack Edwards, Co-Chair
AT&T	Ms. Julie Thomas
	Ms. Rosemary Leffler
Bank of America	Mr. Larry Schaeffer
Boeing	Mr. Bob Steele
Juniper Networks, Inc.	Mr. Robert B. Dix, Jr.
Microsoft Corporation	Ms. Cheri McGuire
Qwest	Ms. Kathryn Condello
	Mr. Andrew White
Raytheon	Mr. Frank Newell
SAIC	Mr. Henry Kluepfel
Telcordia Technologies, Inc.	Ms. Louise Tucker
VeriSign, Inc.	Mr. William Gravell
Verizon	Mr. Marcus Sachs

OTHER PARTICIPANTS

ARTEL, Inc.	Mr. Julian Minard
AT&T	Mr. Brian Daly
	Mr. Martin Dolly
Bank of America	Mr. Manoj Govindan
	Mr. Todd Inskeep
CSC	Mr. Ron Knode
	Mr. Jim Zok
ID Analytics	Mr. Tom Oscherwitz
Industry Canada	Mr. Bob Leafloor
Information Assurance Advisory, LLC	Mr. Roger Callahan
Microsoft Corporation	Mr. Matt Broda
	Mr. Phil Reitinger
Netmagic Associates	Mr. Tony Rutkowski
Nortel	Mr. Abbie Barbir
	Mr. John Yoakum
Raytheon	Mr. Clifton H. Poole
Telcordia Technologies, Inc.	Mr. Robert Lesnewich
	Mr. Ray Singh
Unisys	Mr. Mark Cohn
Verizon	Ms. Deborah Blanchard
	Mr. Russel Weiser

U.S. GOVERNMENT PERSONNEL

Department of Commerce	Mr. William C. Barker
	Ms. Tanya Brewer
	Ms. Donna Dodson
	Dr. Elaine Newton
Department of Defense	Mr. Dick Brackney
	LTC Susan Camoroda, US Army
	Mr. David Milhelcic
Department of Homeland Security	Ms. Sue Daage
Department of State	Mr. James G. Ennis
Executive Office of the President	Ms. Carol Bales
	Mr. Duane Blackburn
	Mr. Thomas Donahue
Federal Communications Commission	Mr. Pat Amodio
General Services Administration	Ms. Judith Spencer
Office of the Director of National Intelligence	Mr. Thomas Seivert

APPENDIX B:

REFERENCES AND BIBLIOGRAPHY

APPENDIX B: REFERENCES AND BIBLIOGRAPHY

REFERENCES

Howell, Donna. "Banks Test 'Text Messaging' Security" Investor's Business Daily (08/10/07) P. A4.

President's National Security Telecommunications Advisory Committee (NSTAC). *Information Technology Progress Impact Task Force Report on Convergence*, May 2000. http://www.ncs.gov/nstac/reports/2000/Convergence-Final.pdf.

Center for Strategic & International Studies, *Securing Cyberspace for the 44th Presidency*, 2008, www.csis.org.

http://www.nano.gov/

http://www.nitrd.gov/

http://www.pnt.gov/

Muller, Edward A. Letter dated 12 March 2009 to Ms. Melissa Hathaway regarding the Nation's 60-day Cyber Review.

The ID Divide: Addressing the Challenges of Identification and Authentication in American Society. June 2008. (Swire and Butts).

The President's National Security Telecommunications Advisory Committee (NSTAC). *Vulnerabilities Task Force Report Trusted Access*, January 27, 2003.

BIBLIOGRAPHY

Ahamad, Mustaque, Dave Amster, et. al. *Emerging Cyber Threats Report for 2009: Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond*, October 15, 2008. Georgia Tech Information Security Center.

Albanesius, Chloe. *RIAA Confirms It Will Take Piracy Fight to ISPs*. December 19, 2008.

ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel (IDSP). *Final Report and Report Summary*. January 2008

Benson, Matthew. *Napolitano: Real ID a no-go in Arizona*. The Arizona Republic. June 18, 2008. http://www.azcentral.com/news/articles/2008/06/18/20080618real-id0618.html.

Carlton, Dennis, Peter Graham, and John Reiners. *Resolving the 'privacy paradox': Practical Strategies for Government Identity Management Programs*. November 2008. *IBM Institute for Business Value*.

Center for American Progress. *The ID Divide-Addressing the Challenges of Identification and Authentication in American Society*. June 2008.

Crosby, Sir James. *Challenges and Opportunities in Identity Assurance*. March 2008.

CSC Leading Edge Forum- Soren Thygesen Gjesse. *Architecture Blueprint for Leveraging Identity Federation*. Undated.

CSC Leading Edge Forum. *Digital Trust – Identity Management – Digitizing Your DNA*. Volume 2. 2007.

Document Security Alliance. *An Analysis of National Document Security Vulnerability*. March 2009.

ENISA Quarterly Review. Vol. 4, No. 4, October – December 2008.

Federal Trade Commission. *Identity Theft Survey Report*. Prepared by Synovate. September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf.

International Telecommunication Union (ITU) Standardization Sector – VeriSign. *A Trusted Provider Identity Framework for NGNs*. January 2009.

Kartz, Black and Ryan. *Identity Management Reference Architecture Practicum Report*. FEAC Winter 2008 session, March 2008.

Knode, Ron. *Identity Issues Report Precis: Digital Identity and Identity Management*. 4 February 2009.

Langevin, McCaul, Charney, Raduege, et. al. *Securing Cyberspace for the 44th Presidency*. 2008. Center for Strategic and International Studies.

McCallister, Erika, Tim Grance and Karen Scarfone. National Institute of Standards and Technology (NIST). Draft Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. January 2009.

Microsoft-Scott Charney. *Establishing End to End Trust*. 2008.

National Security Presidential Directive -59/Homeland Security Presidential Directive – 24. *Biometrics for Identification and Screening to Enhance National Security*. June 5, 2008. http://www.fas.org/irp/offdocs/nspd/nspd-59.html.

NSTC Subcommittee on Biometrics and Identity Management. Identity Management Task Force Report 2008. September 2008.

NSTAC Information Technology Progress Impact Task Force. *Information Technology Progress Impact Task Force Report on Convergence*. May 2000.

Presidents Identity Theft Task Force. *Combating Identity Theft-A Strategic Plan*. April 2007.

Rutkowski, Anthony. *A Global Perspective on Identity Issues*. December 2008.

Rutkowski, Anthony. *Identity Management and Network Cybersecurity Forensics*. January 10, 2009

Rutkowski, Anthony. *Identity Management: Exercise of FCC Authority*. January 2009.

Rutkowski, Anthony. *Survey of Network Forensics Exchange Initiatives*. January 2009.

Rutkowski, Anthony. *The Death of Paid Standards (and the Birth of New Identity Services).* February 2009.

Scholl, Matthew, Kevin Stine, et. al. National Institute for Standards and Technology (NIST). *Draft Security Architecture Design Process for Health Information Exchanges (HIEs)*. January 2009.

Organization for Economic Cooperation and Development (OECD). *The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft*. 27 January 2009.

Silver, Dave, et. al. (editors). General Services Administration. *Technical Approach for the Authentication Service Component*. May 4, 2007.

The UK Office of Public Sector Information. *Challenges and Opportunities in Identity Assurance*. March 2008. www.hm-treasury.gov.uk/d/identity_assurance060308.pdf.

The White House Agenda. http://www.whitehouse.gov/agenda/.

2008 Research and Development Exchange Workshop Proceedings. *Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment*. September 2008.

APPENDIX C

DEFINITIONS

APPENDIX C: DEFINITIONS

These terms and definitions are drawn from many sources. In some cases, a term may have several definitions because it is used by different entities to describe various types of activity. With modern technology, and ICT in particular, it is sometimes difficult to find a word or phrase that accurately describes the activity. Understanding is helped by providing additional information about the situation or context in which the term is being used; this will be found in the notes column. In some cases, it helps to state the situation or context that does not apply.

Where a suitable definition exists for a listed term, the construction of new descriptions should be avoided. Ideally, a single definition should be agreed for each term; some are more difficult than others, but those agreed so far are shown in ***bold italics***.

All of the information contained below has been obtained from publicly available sources, primarily web-sites, and is not thought to have breached any Intellectual Property Rights or copyright.

Term	Definition	Source
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	ITU-T X.800
Anonymity	a. ***Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behavior such as user location, frequency of a service usage, and so on.***	ITU-T X.1121 (04), 3.2.1
	b. Lack of any capability to ascertain identity.	ITU-T Y.IDMsec
	c. The quality or state of being anonymous which is the condition of having a name or identity that is unknown or concealed.	OASIS SAML 2.0, RFC2828
Asserting Identity	An entity making an identity representation or claim to a relying party within some request context.	ITU-T IdM Editors
Assurance	A measure of confidence that the security features and architecture of the Identity Management capabilities accurately mediate and enforce the security policies understood between the Relying Party and the identity provider.	ITU-T Y.IDMsec
Attribute	***NOTE:*** *The FG IdM Framework document will discuss attributes in context with the significant technical implications that arise.*	
	a. Descriptive information bound to an entity that specifies a characteristic of an entity such as condition, quality or other information associated with that entity	ETSI TS102 042 V1.2.4 and ITU-T Y.IDMsec
	b. Information of a particular type. In IdM, objects and object classes are composed of attributes	ITU-T X.501
	c. A distinct characteristic of an object. An object's attributes are said to describe the object. Objects' attributes are often specified in terms of their physical traits, such as size, shape, weight, and color, for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, and network address.	WSIA Glossary
Authenticated Identity	A distinguishing identifier of a principal that has been assured through authentication.	ITU-T Y.2702, X.811
Authentication	The provision of assurance of the claimed identity of an entity.	ITU-T Y.2702, X. 811
Authorization	The granting of rights, which includes the granting of access based on access rights.	ITU-T Y.IdMsec, X.800

Term	Definition	Source
Biometrics	The use of measurable biological characteristics, such as fingerprint recognition, voice recognition, retina and iris scans to provide authentication.	BT Report on Identity Theft
Choice-based	Case in which end users have a clear choice in whether to participate in an IdM federation and over the degree of Authentication reflecting the level of sensitivity of their transaction.	NSTAC Identity Issues Task Force, 2009
Claim	***NOTE:*** *A Claim could just convey an identifier Another Claim might assert that a Digital Subject knows a given key. A set of Claims might convey personally identifying information. A claim might simply propose that a Digital Subject is part of a certain group. A claim might state that a Digital Subject has a certain capability. Claims may or may not be directed to specific Parties. A Claim is an association between a Claimant, a Digital Subject, and an Identity Attribute.*	
	An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject, typically an assertion which is disputed or in doubt.	Identity Gang
Credential	a. ***An identifiable object that can be used to authenticate the claimant is what it claims to be and authorize the claimant's access rights.***	
	b. Data that is transferred to establish the claimed identity of any entity.	
	c. The private part of a paired Identity assertion (user-id is usually the public part). The thing(s) that an entity relies upon in an assertion at any particular time, usually to authenticate a claimed identity. Credentials can change over time and may be revoked. Examples include; a signature, a password, a drivers license number (not the card itself), an ATM card number (not the card itself), data stored on a smart-card (not the card itself), a digital certificate, a biometric template.	
Digital Identity	a. ***The digital representation of the information known about a specific individual, group, or organization.***	Based on CERIAS
	b. A digital representation of a set of claims made by one party about itself or another digital subject.	Identity Gang, et.al.
	c. A set of claims made by one digital subject about itself or another digital subject.	Cameron, CERIAS
Entity	***NOTE:*** *The choice was made to provisionally keep this definition open to any type of person (including legal persons, to facilitate e.g., eProcurement), but also to any other type of entity, such as objects (e.g., computers or other forms of machinery), digital resources or processes (e.g., programs), as this allows abstraction to the largest common element and thus offers the largest number of applications. In order for its existence to be acknowledged, an entity needs to have at least one unique identity. In an identity system implementation an Entity is abstract, conceptual, and non-modeled.*	
	a. Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.	ITU-T Y.IdMsec
	b. An entity is anyone (natural or legal person) or anything that shall be characterized through the measurement of its attributes.	Modinis
	c. A person, physical object, animal, or judicial entity.	Identity Gang
	d. A particular thing, such as a person, place, process, object, concept, association, or event.	IEC 61804-2, ed. 2.0
Federation	a. ***An act of establishing a relationship between two or more entities or an association compromising any number of service providers and identity providers.***	Based on ETSI TR 133 980 V7.5.0
	b. An established relationship among a domain of a single service provider or among next generation network providers.	ITU-T Y.IdMsec
	c. A federation is a collection of realms that have established a producer-consumer relationship whereby one realm can provide authorized access to a resource it manages based on an identity, and possibly associated attributes, that are asserted in another realm. A federation requires trust such that a Relying Party can make a well-informed access control decision based on the credibility of identity and attribute data that is vouched for by another realm.	FG IdM Use Case Working Group
Federated Identity	a. ***A collective term describing agreements standards and technologies that make identity and entitlements portable across autonomous domains.***	The Burton Group

Term	Definition	Source
	b. A single user identity that can be used to access a group of services or applications that are bounded by the ties and conditions of a federation.	ITU-T Y.IdMsec
	c. A shared identity and/or authentication, as the result of federation by either the Entity or by two or more organizations.	Identity Dictionary
Identifier	***NOTE:*** *In the context of IdM, identifiers are generally labels issued by some kind of authority or service provider, or established between peers. Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties.)*	
	a. An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).	ITU-T Y.2091
	b. A data object (for example, a string) mapped to a system entity that uniquely refers to the system entity. A system entity may have multiple distinct identifiers referring to it. An identifier is essentially a "distinguished attribute" of an entity.	OASIS SAML 2.0
	c. Either an "http" or "https" URI, (commonly referred to as a "URL" within this document), or an XRI (Reed, D. and D. McAlpin, "Extensible Resource Identifier (XRI) Syntax V2.0,".)	OpenID
Identity	***NOTE:*** *In the case of a person, the collection of attributes that make up their electronic/digital identity does not normally mean that the individual can be positively identified.*	
	a. Structured representations of an entity in the form of one or more credentials, identifiers, attributes, or patterns in a relevant context. Such representations can take any physical or electro-optical (digital or analog) form or syntax, and may have associated implicit or explicit time-stamp and location specifications.	ITU-T SG17 Q6 Identity CG
	b. The properties of an entity that allows it to be distinguished from other entities.	The Digital Identity Glossary by P.T. Ong
	c. The attributes by which an entity is described, recognized or known.	ITU-T Y.IdMsec
	d. The essence of an entity and often described by its characteristics.	Liberty Alliance
	e. The essence of an entity [Merriam]. One's identty is often described by one's characteristics, among which may be any number of identifiers.	OASIS SAML 2.0
	f. The fundamental concept of uniquely identifying an object (person, computer, etc.) within a context. That context might be local (within a department), corporate (within an enterprise), national (within the bounds of a country), global (all such object instances on the planet), and possibly universal (extensible to environments not yet known). Many identities exist for local, corporate, and national domains. Some globally unique identifiers exist for technical environments, often computer-generated.	Open Group
	g. A collection of attributes which helps to distinguish one entity from another.	The Information Assurance Advisory Council (IAAC)
Identity Information	All the information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses. Identity information shall take the form of either a SIP URI (see RFC 2396) or a "tel" URI (see RFC 3966).	ETSI TS 183 007 V1.1.1
Identity Layer	***NOTE:*** *An identity layer attempts to develop convergence and interoperability regarding identity, can draw from multiple data stores, selectively exposing, or concealing data and attributes, according to policy*	
	Information can be exchanged between different systems.	FG IdM
Identity Management	The structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices.	T SG17 Q6 Identity CG

Term	Definition	Source
Identity Provider	a. ***An entity that creates, maintains, and manages trusted identity information for entities. An Identity Provider may include a Trusted Third Party as well as Relying Parties and entities themselves in different contexts.***	ITU-T IdM Editors
	b. A type of service provider that creates, maintains, and manages identity information for users/devices and provides user/device authentication.	ITU-T Y.IdMsec
	c. A service provider that authenticates a user and that creates, maintains, and manages identity information for users and asserts user authentication and other identity related information to other trusted service providers.	ITU-T Y.IdMsec
	d. An entity in an AAI that performs Identity Management.	TF-AACE
	e. Kind of service provider that creates, maintains, and manages identity information for principals and provides authentication to other service providers within a federation, such as with web browser profiles.	OASIS SAML 2.0
International-ization	***NOTE:*** *The internationalization process is sometimes called translation or localization enablement.*	
	The process of planning and implementing Identity Management specifications, products, services, and administrative implementations so that they can easily be adapted to specific local technical platforms, languages, and cultures, a process called localization.	FG IdM
Internet	***NOTE:*** *The Internet originally served to interconnect laboratories engaged in Government research, and has now been expanded to serve millions of users and a multitude of purposes, such as interpersonal messaging, computer conferences, file transfer, and consulting of files containing documents.*	
	a. A worldwide interconnection of individual networks a) with an agreement on how to talk to each other, and b) operated by Government, industry, academia, and private parties.	http://www.atis.org/glossary/definition.aspx?id=4286
	b. The international computer network of both federal and nonfederal interoperable packet switched data networks. [47 USC 230]	
Interoperability	***NOTE:*** *Identifiers assigned in one context may be encountered, and may be re-used, in another place or time without consulting the assigner. Assumptions made on assignment may not be known to someone else.*	
	The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility of use in services outside the direct control of the issuing assigner.	ISO TC46/SC9 Identifier Interoperability WG
Object	***NOTE:*** *DOI = Digital Object Identifier*	
	A well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication and identity management processing. Entity within the scope of the DOI system; the entity may be abstract, physical or digital, as any of these forms of entity may be of relevance in content management (e.g. people, resources, agreements).	ITU-T X.680 and ISO Project 26324
Owner	NOTE: An entity owns an identity (and therefore its access rights) due solely to the ability to authenticate it.	
	The registered entity for an identity.	Identity Dictionary
Personally Identifiable Information (PII)	NOTE: See privacy.	
	a. The information pertaining to any person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person). Note: Information that can be used to identify an individual should be defined by national legislation.	X.rfpg
	b. Any information that identifies a person to any degree.	PRIME
Privacy	***NOTE:*** *Privacy is a legal requirement which is divided into 3 areas: (1) User privacy andpreventing unwanted intrusions; (2) User privacy and CPNI protection; and (3) User privacy and anonymity. The nature an d exercise of the legislation vary in different jurisdictions.*	

Term	Definition	Source
	a. ***The right of entities to control or influence what information related to them may be collected and stored also by whom and to whom that information may be disclosed.***	ITU-T Y.IdMsec, X.800
	b. Ensuring that information about a person is protected in accordance with national, regional, or global regulations. Such information may be contained within a message, but may also be inferred from patterns of communication; e.g. when communications happen, the types of resource accessed the parties with whom communication occurs, etc.	Based on W3C Glossary
	c. A right to control the dissemination of the attributes of an entity.	Identity Dictionary
	d. The rights and limitations of access to and processing of personal data.	OMA
	e. Proper handling of personal information throughout its life cycle, consistent with the preferences of the subject.	Liberty Alliance
Revocation	The act (by someone having the authority) of annulling something previously done.	ITU-T Y.2701
Trust	***NOTE:*** *The risk/trust relationship depends on who you are and what you want to d o at any instance. The degrees of separation between parties can decrease the trust (increase the risk). The level of trust is typically based on the technical strength of the identity, but it also includes the evaluating entity's subjective considerations (e.g. feelings) of the reliability of the entity the identity represents. Trust is at least partially transitive (as in the case of notaries).*	
	a. A measure of reliance on the character, ability, strength, or truth of someone or something.	ITU-T IdM Editors
	b. Confidence that an entity will behave in a particular way with respect to certain activities (entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.)	FG IdM based on ITU-T Y.2701
	c. A reasonable level of confidence that an entity will behave in a certain manner in a given context.	ITU-T Y.IdMsec
	d. A subjective assessment. An instance of a relationship between two or more entities, in which an entity assumes that another entity will act as authorized/expected.	Identity Dictionary
	e. Trust is an evaluation, by an entity, of the reliability of an identity when the identity is involved in interactions.	Oughome
User	***NOTE:*** *A user may have several identities / usernames / user-ids / logon-ids / sign-ons.*	
	a. ***Includes end user, person, subscriber, system, equipment, terminal (e.g. FAX, PC), (functional) entity, process, application, provider, or corporate network.***	ITU-T Y.2701 Y.2091
	b. An identity where the identifier of the identity is the public part of a paired Identity assertion.	Identity Dictionary
Verification	The process of confirming a claimed Identity. For example; any one-to-one precise matching of an identity's registered credentials, such as in a logon or any non-AFIS process. Usually performed in real-time, with a yes/no outcome.	Identity Dictionary http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html

APPENDIX D

OTHER WEBSITES CONTAINING GLOSSARIES OF IDM TERMS

APPENDIX D: OTHER WEBSITES CONTAINING GLOSSARIES OF IDM TERMS

Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity - Management - A Consolidated Proposal for Terminology - http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Digital Identity - Wikipedia entry - http://en.wikipedia.org/wiki/Digital_identity

ETSI Terms and Definitions Database - http://webapp.etsi.org/Teddi/

FIDIS Definitions of Identity - http://www.calt.insead.edu/fidis/definitions/

IAMSECT Glossary - http://iamsect.ncl.ac.uk/glossary/

Identity Commons2 Identity Schemas - a catalogue of identity-related ontology's (schemas) - http://idschemas.idcommons.net/

Identity Gang of Identity Commons - http://www.identitygang.org/moin.cgi/Lexicon

Internet 2 Glossary - http://www.internet2.edu/info/internet2-glossary.cfm

ITU-R/ITU-T Terms and Definitions - http://www.itu.int/pub/R-TER-DB/

ITU-T SG17 Compendium of Terms - http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc

Meta-Access Management System (MAMS) - https://mams.melcoe.mq.edu.au/zope/mams/kb/glossary

Modinis-IDM Common Terminological Framework for Interoperable Electronic Identity Management - https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc?code=nldsv13294

NIST IR 7298 - Glossary of Key Information Security Terms - http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

The Open Mobile Alliance Identity Management Framework - http://www.openmobilealliance.org/release_program/rd.html

OpenPrivacy.org definitions page - http://www.openprivacy.org/opd.shtml

SAML 2.0 glossary - http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

Security Guide for Interconnecting Information Technology Systems - NIST SP800-47 Appendix D - http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

The Digital Identity Glossary by P.T. Ong with links to other glossaries. - http://blog.onghome.com/glossary.htm

The Identity Dictionary Allan Milgate's 100 technical terms for the common understanding of IAM - http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html

Trusted Computing Group Glossary of Technical Terms - https://www.trustedcomputinggroup.org/groups/glossary

W3C Glossary and Dictionary - http://www.w3.org/2003/glossary/
Weaving the Web - Berners Lee Glossary - http://www.w3.org/People/Berners-Lee/Weaving/glossary.html