KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT'S COMMENTS ON THE DRAFT NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

July 19, 2010

The draft National Strategy for Trusted Identities in Cyberspace is a timely document that has the potential to contribute significantly to the development of better online identities for governmental and commercial uses – identities that can facilitate and secure a range of interactions while also protecting and enhancing privacy and other values.

The Strategy seeks to respond to a confluence of concerns over our ability to secure critical transactions and infrastructure. In recent years, there has been considerable movement in both the government and the private sector towards more effective, interoperable, and secure digital identity technologies. Now is the ideal time to develop a coherent national strategy, in order both to incentivize these efforts and to ensure that Federal and industry efforts are compatible. A national strategy should define the desired attributes for an identity ecosystem, recommend government incentives for the creation or adoption of online identity, delineate the differing roles of government and the private sector, and explicitly address how privacy, free expression and other values will be preserved. We offer here suggested amendments to the strategy to better serve these goals. Most importantly, the Strategy should specify as a guiding principle the concept of levels of assurance -- the concept that different transactions will require different levels of identity and assurance, ranging from very little to the highly secure. If the concept of levels of assurance is recognized as a guiding principle, other issues become easier to address. Also, the draft focuses to too large a degree on *government* development, use, and promotion of an identity ecosystem and on the creation and use of identities tied to physical identity. Instead, a guiding principle should be private sector leadership in the development of identity solutions for commercial transactions, with the government in an incentivizing role. Also, the Strategy should give equal attention to identities that are not tied to physical identity.

In the digital context, identity is a claim or set of claims about an entity (a person, a machine, an institution), similar to but not necessarily the same as the claims on a physical ID card. Those claims support an authorization to engage in a certain activity or transaction. The identity, when authenticated in a manner appropriate to the kinds of services and information involved, allows more trusted transactions online, just as a driver's license does ("this person is allowed to drive according to this state") or a library card ("this person is allowed to borrow books").

User-centric federated identity systems, as advocated in the draft Strategy, have the potential to improve the security and privacy of authentication and services for users;

however, if improperly designed, these systems can negatively impact users and prove a burden instead. CDT believes that user-centric federated identity has great promise to make online interactions easier, more secure, and more easily controlled by the user. There is skepticism from privacy and security advocates that user-centric federated identity will be implemented in ways that maximize the potential of these technologies for consumers, industry, and government. Including policies to protect consumers and ensure that privacy and security protections are included from the outset is key to trust from consumers and large-scale adoption.

The Strategy advocates for a user-centric identity regime, which will require the development of effective controls for consumers as well as strong protections for high levels of assurance in secure transactions. Unfortunately, the public draft of the Strategy does not adequately outline what characteristics of a trust framework would create a trusted ecosystem online. Instead, it outlines several case studies that do not point towards a coherent identity development regime. In order to develop an identity ecosystem that will become widely adopted, the Strategy must recommend a system that is developed in cooperation with industry and third parties rather than developed by the government. Ensuring a public-facing, public-private partnership will help assuage concerns over government control of citizen identity online. In addition, describing the characteristics of a trust framework that are adequate for different levels of assurance for government will allow industry and others to develop compatible frameworks and technologies.

Federal adoption of user-centric identity management for the authentication of both government employees and U.S. citizens will prove to be a key accelerator for the development and adoption of identity technologies. However, the Strategy does not outline how this might happen, but instead assumes that many of the challenges of developing ubiquitous and interoperable identity are adequately addressed simply by mentioning them, rather than discussing them (for example, the importance of preserving anonymity and user choice). In addition, the Strategy notably lacks discussion of how it integrates with existing initiatives within and outside of government, thereby lacking the context to provide a viable map forward.

Overall, the focus of the Strategy should be ensuring the ease of trusted identity transactions online rather than pervasive online authentication. We would encourage ensuring that developing ways to provide "trusted identity at various levels of assurance, when necessary" is the goal. We will mention several portions of the Strategy that we find incomplete, as well as important aspects that we think should be added to the final Strategy. The creation of an achievable Strategy is entirely possible, but requires addressing issues rather than simply glossing over the challenges in favor of stories about using identity online. This would help to create a real marketplace for identity services rather than a mandate from the Federal government.

Strategy should focus on governance layer and policies

The Strategy, while laying out several possible use cases for an identity ecosystem, fails to discuss important aspects of a trust framework that will establish a successful process. Creating an identity ecosystem requires standards, interoperability, and well-understood responsibilities and roles within the system. These governance layer

decisions can be set, in part, by the Federal government in order to establish the ground rules for participants in the Identity Ecosystem. In referencing the creation of an Identity Ecosystem Framework, the Strategy seems to acknowledge this need but does not discuss the factors that should be included to guide the creation of each private sector Trust Framework within the Ecosystem. By inadequately addressing the necessary practices and governance issues within trust frameworks, the Strategy offers no guidance for actual implementation. While there is discussion of securing the network and enabling a trusted identity system, there must also be discussion of how a trust framework can effectively secure the policies created around identity management.

Strategy should include a diverse set of examples to illustrate substance

The Strategy largely outlines uses cases for consumers outside government and industry. Rather than numerous hypothetical scenarios, the Strategy should diversify the use cases and affected parties. If the Strategy is to bring together diverse stakeholders to work toward strong online identity management, it should instead explore the goals and requirements of the use cases for each stakeholder group. For example:

- Commercial entities may use the system to authenticate a partner's employees or temporary contractors.
- Government agencies may use the system to deliver services and interact with citizens online.
- Health care providers may authenticate each other before transmitting patient data over the network for treatment purposes.
- Privacy groups may develop and implement frameworks and identity systems that both protect user data effectively and comply with overarching standards.

Each of these stakeholders may have unique needs and circumstances that a comprehensive identity system must address. This cannot be accomplished by focusing too heavily on use cases for consumers or health care. Instead, the government should collaborate with different bodies – such as agencies, commercial entities, health care providers, privacy advocates and others – to articulate the standards and policies that will properly support the broad range of users accessing the system.

Strategy should direct government incentives and standards

It is obvious that commercially available online identity is not yet ready to provide strong assurance to government and business about the identity of the holder. There are logistical, policy, and technological challenges that must be solved before online identity can be used. However, moving the identity management industry forward is the most effective way to ensure that identity services are available nationally, for uses both within and outside the Federal government. The National Strategy aims to make available "an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy."[1] The most effective way to move the identity management space forward is to establish a set of incentives and standards for companies in the identity space. Effectively, this both allows companies to accurately

[1] "Cyberspace Policy Review." The White House, May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

assess the expectations of participants and to compete on equal footing, avoiding the possible uncertainty of expanding into a space that has not been well defined.

Eliminating the weaknesses inherent in "shared secret" identity online is a key element to creating more effective and trustworthy relationships online using robust credentials. However, proscribing technologies and driving the approach to identity will not create a more protective or secure ecosystem. The government does not need to implement these technologies, but does need to assess their outcomes and evaluate which provide adequate assurance and protection for data. The Federal government may be more effective here if it harnesses its ability to create guidelines and endorse market-driven schemes and implement a certification/audit regime.

The National Strategy should focus discussion on the ways to create trust using standards and binding agreements among all players in the ecosystem. The draft Strategy mentions the role of the government in the identity ecosystem many times, implying that the government will play a leading role in development of a trust framework for online identity. However, this draft does not point to any of the other players in the space and the role that they can and should play in the development of digital identity. In addition, it does not mention the important role of government for setting standards that will guide, but not dictate, innovation in the identity management space.

The Strategy seems to shy away from the idea of collaborating with other identity ecosystem stakeholders to develop standards and technologies that provide adequate assurance for different kinds of transactions. Instead, the Strategy delegates the work of developing a trust framework and qualifying implementations to the government. Developing identity solutions within government will not inspire trust in the overall project, or inspire confidence among the private sector and advocates.

By establishing best practices and minimum standards for the space, the government can enable the private sector to innovate and develop new, more effective technologies and protocols that create the trusted identity needed for all types of transactions.

Strategy should suggest ways to manage and allocate liability

Standards and best practices set by the government should provide mechanisms to create mutual acknowledgement of appropriate liability for participants in the system and recourse for users. This is one of the most important things that the Federal government can do in order to encourage a healthy identity ecosystem. Without outlining these elements, adoption of identity management will be tepid at best. Creating well-understood expectations for participants in the Identity Ecosystem will allow users to assess the risks and balance them appropriately. The Strategy should ensure that these practices are included as part of the Identity Ecosystem Framework.

In addition, the Strategy should suggest ideas for legislation to help establish a fair allocation of liability in the Identity Ecosystem. One idea, from the National Broadband Plan[2] is to establish an insurance regime modeled on the FDIC that will manage best practices for the identity space. An insurance regime, possibly paired with a legislative

[2] National Broadband Plan, Federal Communications Commission, http://download.broadband.gov/plan/national-broadband-plan.pdf

safe harbor, for the Identity Ecosystem could provide privacy and security safeguards to consumers while protecting companies that engage in the Identity Ecosystem under best practices. Private entities, backed by government, could provide insurance to protect consumers in the identity ecosystem similar to the way the government ensures that individual bank deposits are protected, providing confidence that the money entrusted with a private bank is insured in case the bank fails. As part of this program, the insurance entity creates rules and regulations for ecosystem participants in order to effectively manage the risk taken in insuring these providers. Essentially, this insurance would underpin the basic trust framework – establishing a minimum set of policies and rules for entities in identity transactions that will create and preserve trust.

Since insurance for identity management is often tied to cybersecurity, it is worth pointing out that there are many aspects of identity management that should be insurable, including consumer privacy, data security, and other concerns. Insurers may wish to develop best practices for additional areas, and this should be encouraged. Insurance should be in place to ensure adequate redress or protections in the event of a data breach, for example, or in the event that a relying party breaks the framework requirements. Allocating liability is an important part of establishing an effective governance layer as part of the Identity Ecosystem as part of the strategy. The Strategy should include further discussion of the role of liability for all participants in the ecosystem.

Strategy is unfocused and does not provide context to the problem

On reading the Strategy, a reader may finish without a clear understanding of the problem that is being addressed. While it makes clear that online health transactions could be made easier, many other use cases remain unaddressed– especially the potential uses for government agencies, both in delivery of online services to citizens and for internal authentication and security. The Strategy does not enumerate ways that identity services could ease the burden of delivering government services, protecting data, or preserving privacy. There are many interesting use cases for widely adopted identity services, but the Strategy focuses on only a few.

The Strategy should outline the current weaknesses in cybersecurity that trusted identity systems could address and how, in addition to expounding on visions of the future. For example, there is a push towards the protection of critical infrastructure using, in part, strong identity - but this possibility is not mentioned in the Strategy. Tying the Strategy back to concrete problems will make solutions more relevant and encourage development of new innovations.

The Strategy should also acknowledge and incorporate existing efforts underway to move towards these goals within government, and possibly within industry as well, in order to give these efforts context and address current problems. By ignoring the work that has been done, both by the Federal government, industry (especially in the health space) and international players, the Strategy lacks the context that could give the public a realistic idea of how the Strategy fits in to the ecosystem. In particular, adding the work done by ICAM in the U.S., STORK in the E.U.[3], the Open Identity Exchange, and the

[3] Secure Identity Across Borders Linked(STORK), https://www.eid-stork.eu/

U.S. National Health Information Network would add invaluable context to the Strategy and avoid redundant work.

Including progress made in government development of identity management services and international developments will give important context to the National Strategy. Trusted identity will not emerge from a vacuum, but instead must be built from the Federal, international, and private sector innovations that are already well underway. The National Strategy should fully discuss each of these spaces in order to provide this context as we work towards trusted identity online.

Incorporate guidance on levels of assurance for current Federal authentication

An Office of Management and Budget memo from 2004 outlines Levels of Assurance for online identity and the situations in which it is appropriate to require stronger assurances. These Levels of Assurance have guided government authentication for six years, but the National Strategy for Trusted Identity in Cyberspace is not well-suited for developing trust frameworks that will be acceptably secure for use at various Federal Levels of Assurance.[4] In fact, it does not mention the Levels of Assurance outlined in M-04-04 at all, even though they form much of the policy framework around how the Federal government authenticates employees, contractors, and the public. These levels of assurance guide the kind of authentication a service should ask for, based on the risk of inaccurate authentication.

These levels of assurance, and the concept that different kinds of transactions require different assurances are critical for discussion of identity. Without a set of strong guidelines on the appropriate use of identity, the scope of the transactions that require strong identity will increase unbounded. This kind of "scope creep" will both decrease trust in the system and lead to the increased exchange of identity information unnecessarily, placing the information at risk.

The appropriate degree of data protection for the Levels of Assurance is another key discussion for the Strategy to address. This concept has been called Levels of Protections, and could provide guidance on the kinds of protections that should be placed on different kinds of data. For example, identity to access an electronic health record requires different protections than the pseudonym associated with an anonymous blog post. While there are baseline protections that should be afforded to all personal information online, many kinds of transactions will require an increased Level of Protection.

Identity for Health Space

We are pleased to see the Strategy devote attention to the issue of identity assurance for the exchange of personal health information. However, the health examples fail to give equal attention to the identity and authentication needs of health care providers, rather than patients. In order to foster greater electronic health information exchange,

[4] E-Authentication Guidance for Federal Agencies, Office of Management and Budget, December 16, 2003 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

providers and patients both must have confidence that electronic health information is sent and received by trusted, authorized sources.

Further, the Strategy's current health examples jump to more advanced health identity scenarios without first addressing the basics. The nation's health information technology initiatives will require that health care providers begin exchanging electronic personal health information by 2012, which requires us to have a strategy in place for assuring the physical identity of providers in less than two years. The more complex health information transactions that require authentication of other credentials (for example, authorization to access a record) can be built on this initial foundation.

Finally, the Strategy repeatedly uses health care examples without mentioning identity management work that is already underway is that area. Specifically, groups working on the National Health Information Network are grappling with the issues of trust and security and exploring the role of intermediaries in authenticating senders and receivers of data. See the NHIN Direct Workgroup Security and Trust Consensus Protocol as a starting point for this ongoing discussion.

Strategy should include globally acceptable, interoperable standards

Developing an identity ecosystem that is scalable internationally will require more than a National Strategy, industry momentum, and U.S. regulation. Working with groups in the EU that are already implementing these ideas and with others internationally will both aid interoperability with existing systems and ensure that we do not lock the U.S. in to a system that is incompatible with the rest of the ecosystem.

An ideal way to drive development of internationally compatible identity systems is for trusted frameworks to establish guiding policies. Mandating technologies or regulating the U.S. identity industry will not result in a global ecosystem. Rather, creating a set of policies that trusted players must abide by is entirely compatible with a global identity regime; players can agree to this set of standards contractually, whether or not they are under U.S. jurisdiction.

Physical identity can be distinct from online identity

The Strategy focuses largely on digital identities tied to a person's physical identity. The definition of "identity" in the Strategy is tied directly to physical identity, rather than embracing the concept of identity as a set of identifiers and information about an individual or group.[5] Tying the definition of an identity to a physical person is overly burdensome for many transactions at lower levels of assurance.

Some use cases will require physical identity. This is particularly true in the health context, where establishing physical identity is a basic step and other attribute credentials (including current valid license to practice medicine, enrollment in a specific health plan) can then build on and strengthen the value of an identity management system. However, health care is one of many specialized use cases with considerations

[5] In *Who Goes There?*, a National Research Counceil book on Identiy is defined as "The identity of X is the set of information about individual X that is associated with that individual in a particular identity system Y. However, Y is not always defined explicitly." Importantly, this definition does not require physical proofing for identity. High assurance proofing for transactions at low levels of assurance do not lend efficiency nor security to the system.

that are distinct from other fields. A challenge for the developers of the identity management systems is to delineate which use cases require physical identity and which do not, and to ensure that both use cases are adequately supported in all levels of implementation – at the governance, management, and technology layers. The Strategy should include this as part of the standards and best practices that will be established.

There is not a need for physical identity for many identity transactions online. For example, the Strategy uses anonymous blogging as a use case; truly anonymous blogging would in fact preclude a tie to physical identity in many cases. There are additional ways to establish trust at the level of assurance necessary for a transaction, without the kind of in-person proofing required to tie digital and physical identity together. Often, attribute credentialing will be more appropriate, or simple pseudonymous authentication will suffice for online identity.

The model introduced by the Strategy is nominally user-centric, but there is a strong emphasis on securing the hardware and network. The Strategy devotes significant attention to authentication of devices that are part of a transaction, and tying credentials to devices. These examples imply that the only way to secure a transaction – or to establish trusted identity – is to ensure that the entire transaction takes place on trusted hardware. However, this is not essential for online identity in most cases, and the Strategy should make that clear.

Focusing too heavily on trusted hardware used across the network as a consumer authentication strategy is overly proscriptive. Instead, the Strategy should set forth requirements that technologies, protocols, policies, and management must meet in order to be considered trusted and allow innovation to meet those standards. This strategy could be combined with a certification program. There is more than one way to secure the network, and focusing on trusted hardware rather than the level of security necessary for transactions across government and commercial spaces is detrimental to innovation.

Strategy should continue to focus on user-centric, private sector identity

The model espoused in the Strategy - moving from credentials on an application-to-application basis to credentials centralized from an identity provider - is a strong move in the right direction, but the risks must also be identified and addressed. For example, centralizing credentials and identity information will make the risk of phishing much stronger and possibly enhance the degree of damage dealt if the centralizing entity is compromised. In addition, it will require clarifications to law enforcement access to centralized identity information stored and generated by using identity providers across the Internet.

Movement towards user-centric identity, where a user controls their own data, is a boon to privacy and security as long as the technology to enable user-centric identity transactions is easily accessible to the public. However, a “unique digital identity” that is tied to a unique physical identity is not an effective way to enhance user control of their identity online. In addition, authenticating every aspect of the transaction may be necessary for some very high-level assurance transactions, but is not appropriate on a regular basis for typical transactions.

Given the Strategy's focus on government credentials and authentication, it is worrisome that the secondary focus is on the use of government credentials for private transactions. It is a much better strategy to allow private, but trusted, credentials to be used in government transactions. Assuming that credentials, distributed and maintained by the government, will be built into trusted hardware in the form of cell phones and computers does not imply a voluntary identity regime, but rather a pervasive use of government credentials in the private sector, which raises numerous troubling issues.

Lead agency within government

In order to build consumer trust, the Strategy should recommend a lead agency (or set of lead agencies, or an interagency lead) that focuses on the public. While DHS has considerable knowledge in authentication, driving a market for consumer identity in addition to internally focused identity is not a job for DHS. There are many agencies that have expertise in working with industry and identity issues; the GSA, FTC, and Department of Commerce are reasonable choices. The branding associated with the lead agency should be one of serving the public, rather than security that is internally facing and focused on data mining.

Conclusion

Pervasive identity online will not solve the cybersecurity problem. There are many recognized barriers to security online, from bugs in programs meant to secure transactions to legacy systems that cannot be upgraded with security fixes. Trusted identity – matched with an ecosystem guided by appropriate polices – is an important part of creating a more secure online infrastructure. However, the role for government to play is the creation of standards and best practices rather than driving the identity ecosystem for the United States.