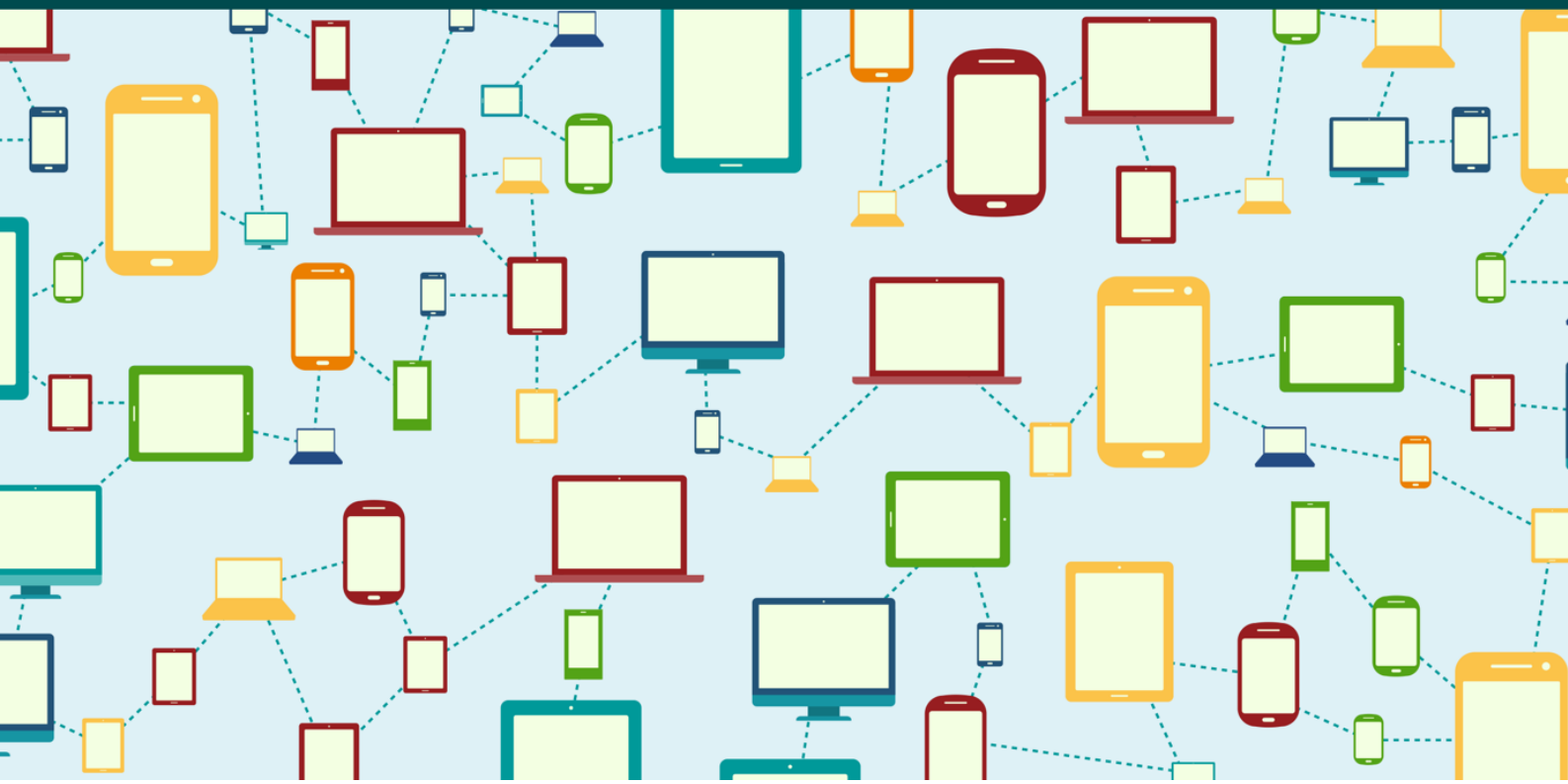
fido alliance | simpler stronger authentication



Input to the Commission on Enhancing National Cybersecurity

September 9, 2016

Executive Summary

Topics Addressed: Identity and Access Management (IAM) is the primary focus – particularly Authentication. Our response also touches on Critical Infrastructure, International Markets, and Public Awareness and Education.

Challenges

Eight years ago, the Commission on Cybersecurity for the 44th Presidency flagged the importance of Identity and Access Management (IAM) in addressing cyber threats, stating: *"We recommend that the United States adopt regulations that require robust authentication for access to critical infrastructures,"* and added that *"As part of an overall cybersecurity strategy, the government can accelerate the adoption of authentication."* [1]

Despite a number of efforts to accelerate the adoption of more robust authentication solutions, the password continues to be the primary tool of authentication and the primary vector of attack in cyberspace. It is hard to find a major breach over the last few years where a compromised password did not provide the attack vector for an adversary to compromise a system; Verizon's 2016 annual Data Breach Investigations Report (DBIR)[2] found that "*63 percent of confirmed data breaches involve using weak, default or stolen passwords.*" The password has proven hard to dislodge, in large part due to cost and user experience problems with the alternatives.

There are many problems with passwords, but the first among them is that passwords are a "shared secret" – and as such, there are many ways for adversaries to compromise this secret. As we document in this response, the ability for adversaries to easily crack shared secret authentication now extends not just to passwords, but also to some "first generation" multi-factor authentication (MFA) solutions such as one-time passwords (OTP) that also rely on shared secrets. The evidence is clear that the value of shared secret authentication solutions has not only waned – it has also become the major cybersecurity vulnerability. Better alternatives are needed to stop the wave of authentication-focused attacks.

Solutions

The Fast Identity Online (FIDO) Alliance was formed in 2013 to revolutionize online authentication by developing open, interoperable industry standards that leverage proven public key cryptography for stronger security and device-based user verification for better usability. Today FIDO has more than 250 members representing a "who's who" in information technology, communications, hardware and software manufacturers, finance, health care, government and other sectors.

Through the collaborative efforts of FIDO, new standards and specifications have emerged that enable strong, easy-to-use authentication to be built into devices such as computers, tablets and smartphones. Today, thanks to the FIDO specifications, many devices running major operating systems such as Windows, Android and iOS can support issuance of a strong, multi-factor credential as part of the device itself.

Recommendations

1. **The United States should make it a national priority to replace passwords and other "shared secret" authentication approaches with more secure solutions.** Every month that brings news of yet another password-focused breach drives this point home. More robust authentication solutions are needed, especially for access to critical infrastructure.

2. **The U.S government should promote the use of new authentication standards such as FIDO as a best practice for authentication.** Much as the U.S. government promotes the use of certain encryption standards and discourages use of outdated standards, so should the government with authentication. Given that the key to decrypting ciphertext is often a password, it is especially

[1] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf

[2] http://news.verizonenterprise.com/2016/04/2016-verizon-dbir-report-security/

important for government to ensure that strong encryption cannot be undermined by weak authentication.

3. **The U.S. government should accelerate the adoption of strong authentication through actions that will help create demand for these solutions.** Industry has stepped up to address the supply side, as evidenced by more than 100 FIDO certified products and the embedding of FIDO specifications into major browsers and operating systems – all with a focus on producing a solution that aligns with recommendations from the 2008 Commission, as well as the 2011 National Strategy for Trusted Identities in Cyberspace (NSTIC). The government should respond by taking specific steps to accelerate demand for, and use of, these solutions.

Introduction

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to provide input to the Commission on Enhancing National Cybersecurity as it considers recommendations to strengthen cybersecurity across the United States.

Eight years ago, the Commission on Cybersecurity for the 44th Presidency flagged the importance of Identity and Access Management (IAM) in addressing cyber threats, noting that *"Intrusions into DOD networks fell by more than 50 percent when it implemented the Common Access Card"* - a strong authentication solution that replaced passwords. Based in part on this experience, the Commission stated: *"We recommend that the United States adopt regulations that require robust authentication for access to critical infrastructures,"* and added that *"As part of an overall cybersecurity strategy, the government can accelerate the adoption of authentication."* [3]

The recommendations from the Commission were heavily influential in the 2009 White House *Cyberspace Policy Review,* as well as the White House's launch in 2011 of the *National Strategy for Trusted Identities in Cyberspace (NSTIC).*

Looking back over the last 8 years since the CSIS commission reported, the threats we face in cyberspace have been amplified and the threat to the nation has become more acute and complex.

One thing that has not changed, however - despite no shortage of industry and government efforts - is that the password continues to be the primary vector of attack in cyberspace. As we detail in our response, it is time to for the United States to take definitive steps to address this problem.

Current and Future Trends and Challenges

As the table below details, it is hard to find a major breach over the last few years where a compromised password did not provide the attack vector for an adversary to compromise a system.

Breach	Date	Attack Vector
Oracle/MICROS	August 2016	Compromised Password
OPM (2 breaches)	May 2015	Compromised Password
Anthem	February 2015	Compromised Password
IRS	May 2015	Inadequate Authentication (Compromise of "Knowledge-Based" Questions)
JP Morgan Chase	July 2014	Compromised Password
Target	December 2013	Compromised Password
Apple iCloud	August 2014	Compromised Passwords
Home Depot	September 2014	Compromised Password
Sony Pictures	December 2014	Compromised Password
Heartbleed	April 2014	Bug that exposed passwords
1.2 billion passwords (Russian CyberVor hacker gang)	August 2014	Multiple – target was passwords to be used for other potential attacks
NSA (Snowden)	June 2013	Insider Threat – Privileged User Exploiting Access
Wikileaks (Chelsea/Bradley Manning)	2010	Insider Threat – Privileged User Exploiting Access

[3] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Verizon's annual Data Breach Investigations Report (DBIR) has also helped to make this point clear. The 2016 DBIR found that "*63 percent of confirmed data breaches involve using weak, default or stolen passwords.*" No other attack vector comes close.

Why does this security hole remain unclosed in 2016? The primary issue has been that passwords, loathed as they are by most of the population, have continued to be difficult to displace as the dominant means of authentication. The security benefits offered by the first generation of stronger authentication solutions using multi-factor authentication (MFA) have, to date, generally been offset by significant degradation of the user experience (UX) in many applications. These issues have dissuaded companies and consumers alike from widely embracing them. Particularly in consumer-facing applications, companies have been loath to push any solution that slows down or otherwise degrades the customer experience.

To understand the deficiencies of passwords-as-credentials, it is important to look at the password's fundamental security and usability characteristics:

From a security perspective, the password is what we call a "shared symmetric secret," which means both parties in a password authentication system – and only those two parties – must know the secret. This requires online applications to store these secrets on their servers, which means a data breach of one online server results in an increased risk to the rest of the ecosystem, because the attacker now has credential "secrets" to use against other servers. This has happened so often in the past few years that we literally know of over a billion stolen passwords that are in circulation, making these credentials not very "secret" anymore.

The data breach is the most widely reported vulnerability of password-based security systems, but there are many other vulnerabilities. For instance, a user can be tricked by "social engineering" into revealing his/her password through phishing attacks that spoof the online service's identity, installing malware on the user's device to record their keystrokes, or simply brute force "guessing" attacks to get into accounts protected by very weak passwords. The recent Verizon Data Breach Report showed 23 percent of recipients now open phishing messages and 11 percent click on the attachments. These vulnerabilities exist because of the inherent properties of passwords being human-readable shared secrets.

From a usability perspective, the password puts users into a no-win situation, where they either create different, complex passwords for all of their accounts – in which case they cannot remember them when they need them, or they have to store them (typically somewhere that is not safe) – or they create only one or very few simple passwords that are easy to remember, which puts them at greater risk of having a single stolen or broken password result in many account takeovers, identity theft, and fraud. The usability problem has only gotten worse in recent years through the ubiquity of smaller keyboards (mobile devices), more complex requirements for "password strength" at many sites, and the introduction of one-time-passcodes as a second factor "secret" that forces the users to type not one, but two passcodes every time they authenticate.

This is not only a problem for online services in the consumer market. When password-based credentialing extends among an enterprise, its partners, and contractors, the attack surface increases, allowing attackers to infiltrate at the weakest point in the chain and work their way into and among organizations.

In summary, passwords are quickly evolving into an untenable credentialing system because of their fundamental security and usability characteristics. That evolution is being accelerated by the global shift to mobile computing and the ever-rising tide of data breaches. We need a fundamentally new credentialing technology, one that is based on open standards so it can become as ubiquitous as passwords, and one that does not share the security or usability flaws of shared secrets.

Progress Being Made to Address the Challenges –Details on the Most Promising Approaches

Amidst all the bad news surrounding passwords, there is now some good news: industry has stepped up to address these authentication challenges. Today, thanks to efforts like the FIDO Alliance, there are new ways to deliver strong authentication, with models that eliminate the use of shared secrets and are easier for people to manage and use. These solutions are based on open standards for next-generation authentication that are widely embraced by industry across the globe.

The FIDO Alliance was launched in 2013 with a mission to change the nature of online strong authentication by:

- Developing technical specifications defining open, scalable, interoperable mechanisms that supplant reliance on passwords to securely authenticate users of online services.
- Operating industry programs to help ensure successful worldwide adoption of the specifications.
- Submitting mature technical specifications to recognized standards development organizations for formal standardization.

At its core, FIDO specifications were crafted with a simple premise: to address the common but flawed assumption that easy-to-use authentication must be weak, and strong authentication must be difficult to use. For years, the uptake of strong authentication solutions has been inhibited by this assumption (as noted in Figure 1, with solutions in the marketplace falling on one end of the curve or the other).

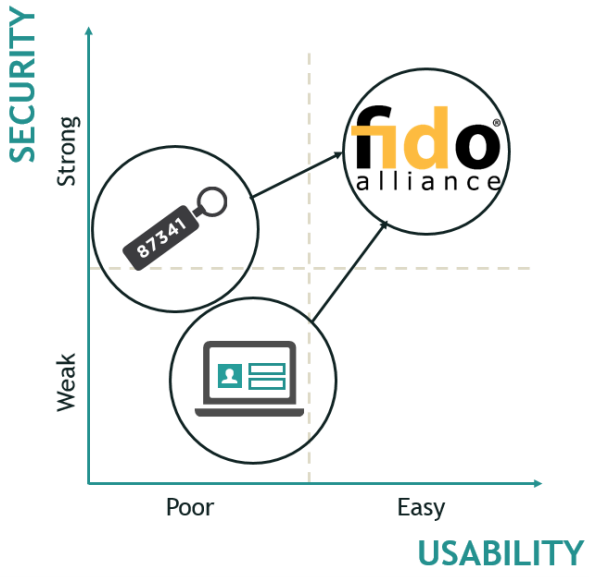


Figure 1: FIDO Authentication changes the paradigm – enabling excellent security and usability

Too many times, products have been engineered to prioritize security over usability, with the assumption that individuals would use the solution; the reality, however, has been that consumers have rejected using solutions that are hard to use – leading to a growing number of data breaches and other security exploits. In order for authentication to be broadly accepted by both online service providers and their users, it must be affordable to deploy and easy to use while providing improved security.

This approach is supported today by more than 250 FIDO Alliance members, including companies and organizations from many critical infrastructure sectors, including: Communications, Financial Services, Government Facilities, Information Technology, Healthcare and Public Health, Commercial Facilities and Defense Industrial Base.

Our board members, listed below, comprise key industry leaders across services, apps, devices, platforms, and vendors from across the globe.

Our efforts have focused on improving online authentication by developing open, interoperable industry specifications that leverage proven public key cryptography for stronger security and device-based user verification for better usability.

These simpler user experiences are secured by FIDO's use of long-proven asymmetric public key cryptography, where the private key is the only "secret," and it is stored on the user's device. Only the public key is ever shared with the online service, resulting in no credential secrets ever being shared with servers, which renders the threat of credential theft from a data breach moot.

The only way to attack a FIDO credential/private key is to attack the user's personal device. When that device leverages modern technology for the protection of the private key, such as secure elements and/or trusted execution environments (which is the trend with consumer electronics today, especially mobile devices), the attacker must actually gain physical possession of that user's device to even attempt an exploit. This type of attack does not scale and is not economical from a cybercrime perspective. In summary, FIDO standards are a game changer from both a security and usability perspective.

The FIDO specifications were specifically designed in a manner that aligns to the four Guiding Principles called for in the NSTIC, with an eye toward transforming these principles from little more than a hopeful vision of the future to a vital ecosystem of commercially available identity solutions supported by market leaders around the world.

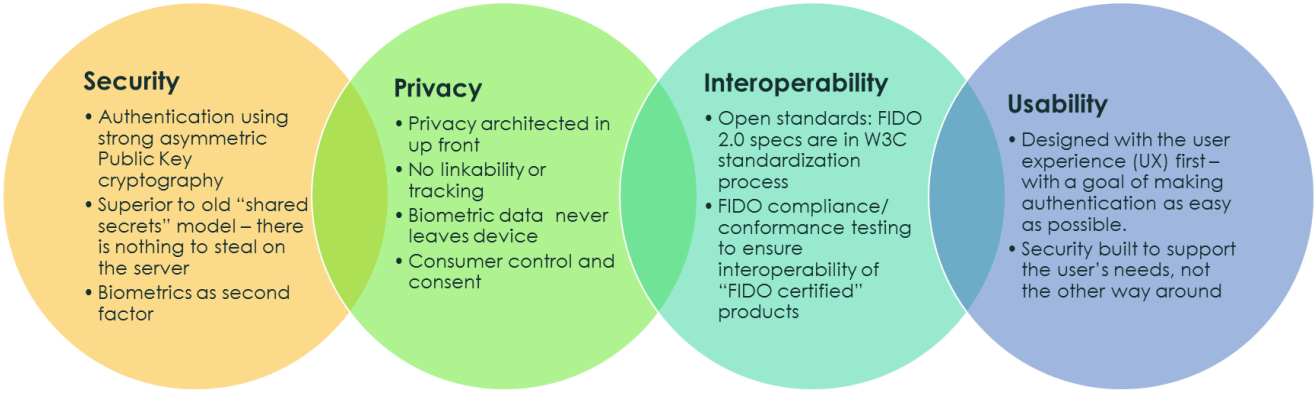
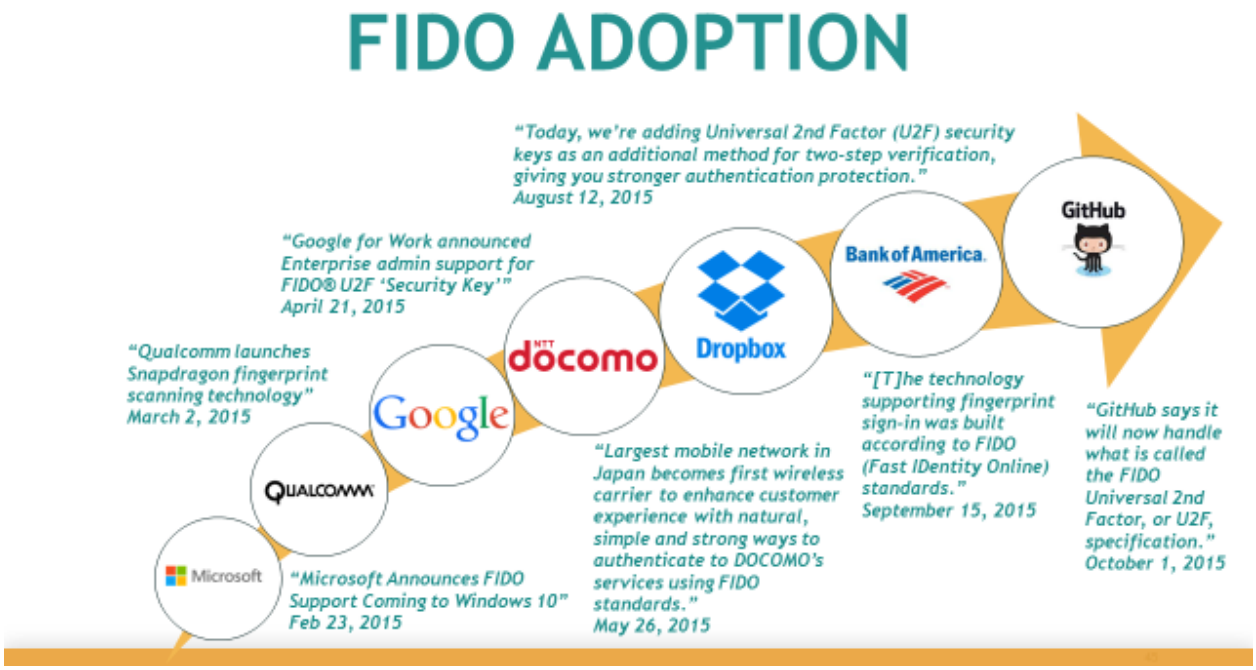


Figure 2: FIDO is designed to implement the NSTIC Guiding Principles

As the graphic below details, FIDO specifications have been adopted by a number of leading firms as the preferred way to offer their customers simpler, stronger authentication.



The emergence of FIDO reflects many changes over the last eight years – not just in authentication, but in the broader IT industry as well. The following table outlines the state of the market eight years ago – detailing the challenges – and lays out how much the market has evolved since that time with the emergence of new solutions such as FIDO, focused on addressing these challenges.

Evolution of the Authentication Market

Issue	2008	2016
Issuance of a strong credential	Requires service provider to issue a physical token, such as a smart card or one-time password (OTP) token. Integration of tokens is complicated and costs are high.	Modern smartphones and laptops increasingly ship with strong authentication capabilities embedded, such as biometric sensors and embedded security hardware. This removes the need to procure, ship and activate a separate, single-purpose authentication device.
Security vs Usability tradeoffs	Use of strong authentication technologies generally requires user to carry a separate physical token – each time they use it, they have to "break stride" to find the token, activate it and then often (with OTP), enter information. Cost of issuing tokens is significant. Authentication solutions can generally only be used with a single application, increasing costs	Next generation authentication technologies are designed from the start to address user experience (UX). Security and usability are no longer at odds with each other; a passwordless experience is feasible in most applications. Strong authentication can be delivered without need to issue a standalone token, as major operating systems can support issuance of a strong, multi-factor credential as part of the device. Legacy devices can be enabled through standards-based "security keys" that can communicate through USB, NFC or Bluetooth. Authentication solutions can be used across multiple applications.
Security of "strong" authentication technologies	OTP is considered to be a secure technology, though 2007 emergence of Zeus malware exposed flaws.	SMS and OTP are both viewed as increasingly vulnerable, as adversaries develop attack methods to compromise the technologies. These have been documented by firms like Google, who publicly flagged the extent of the problem in 2015, noting that these days, a "phisher can pretty successfully phish for an OTP just about as easily as they can a password" and noted their shift to hardware-based solutions using the FIDO Alliance specifications as the way to stop these targeted phishing attacks.[4] Likewise NIST has proposed to deprecate use of SMS authentication in its latest version of SP 800-63-3, "Digital Authentication Guidance," due to a variety of documented weaknesses in use of SMS as a second factor.[5] The takeaway: any Authentication solution that relies on the use of a

[4] Speech at 2015 Cloud Identity Summit, see https://www.youtube.com/watch?v=UBjEfpfZ8w0 Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflect their experience with this technology.

[5] See: http://nstic.blogs.govdelivery.com/2016/07/29/questionsand-buzz-surrounding-draft-nist-special-publication-800-63-3/

		"shared secret" – even one that is only good for a short time – is vulnerable to increasingly common and effective phishing attacks. The market needs to move away from this toward other solutions.
Ease of use and deployment for authentication solutions using Public Key cryptography	Use of public key cryptography means full Public Key Infrastructure (PKI) technology, posing significant costs and complexity including an inherent dependency on certificate authorities.	New specifications such as FIDO enable strong authentication through a simplified, more lightweight approach to Public Key cryptography that removes the dependency on certificate authority infrastructure.
Applicability of biometrics	Biometric sensors, if used at all, require standalone devices. Reliability of biometric devices is spotty. NIST does not recognize use of biometrics as an authentication technology, due to fact that biometrics are not a secret, and thus can't be changed if compromised.	Biometric sensors are increasingly embedded in consumer-grade hardware; typical smartphone contains sensors capable of reliably performing 1:1 matches of fingerprint, face and iris. NIST recognizes value of use of biometrics as one factor in a multi-factor authentication protocol, has launched biometric "Strength of Function for Authenticators (SOFA)" effort to apply measurement science and standards to biometrics in authentication.
Privacy implications	Many strong identity solutions present significant privacy concerns, as first-generation solutions are architected in a way that enables tracking and aggregation of user data. These concerns include: • Solutions that require the transmission of sensitive PII with each authentication • Solutions that enable a user to be tracked across multiple applications as they use the same credential to access those applications • Solutions that require sensitive PII to be stored and accessed with each authentication • PII is often released without consent	Next-generation identity solutions and standards using FIDO are architected with a "privacy by design" approach, addressing the limitations of first-generation solutions.[6] Key features include: • There is no third party in the protocol • There are no "secrets" generated or stored on the server side • Biometric data (if used) never leaves the device • There is no linkability or tracking between services and accounts • Users can de-register at any time • There is no release of PII as part of the authentication

[6] For example, see details on the FIDO Alliance specifications' approach to privacy at https://fidoalliance.org/there-is-no-privacy-without-security/

What should be done now (or within the next 1-2 years) to better address the challenges?

1. **The United States should make it a national priority to replace passwords and other "shared secret" authentication approaches with more secure solutions.** Every month that brings news of yet another password-focused breach drives this point home. More robust authentication solutions are needed, especially for access to critical infrastructure.

   The country needs a fundamentally new authentication technology, one that is based on open standards so it can become as ubiquitous as passwords, and one that does not share the security or usability flaws of shared secrets.

   Efforts in the current Administration to jumpstart this, such as the National Strategy for Trusted Identities in Cyberspace (NSTIC), the OMB "Cyber Sprint" and the issuance of Executive Order 13681 have been helpful, but they have not in and of themselves been enough to solve this problem. Among other things, these efforts have been under-resourced or subject to lengthy delays in implementation. The next Administration should create a plan to build off of these initiatives, with a focus on removing our dependence on password security as a national priority.

2. **The U.S government should promote the use of new authentication standards such as FIDO as a best practice for authentication.** Much as the U.S. government promotes the use of certain encryption standards and discourages use of outdated standards, so should the government with authentication.

   Security technology constantly evolves – and as it does, the government has a history of making recommendations as to which technologies should and should not be used. NIST, for example, withdrew support for the Data Encryption Standard (DES) in 2004[7], after it became clear that DES was increasingly vulnerable, and steered agencies toward use of the faster, stronger Advanced Encryption Standard (AES). Likewise, NIST guided agencies to stop using the SHA-1 family of hash functions in 2006, instead recommending the more secure SHA-2 algorithms[8].

   NIST should play an important role here as well in flagging potential vulnerabilities in authentication technologies and protocols and making recommendations on which ones should be used to protect critical systems. Given that the key to decrypting ciphertext is often a password, it is especially important for government to ensure that strong encryption cannot be undermined by weak authentication.

3. **The U.S. government should accelerate the adoption of strong authentication through actions that will help create demand for these solutions.** Industry has stepped up to address the supply side, as evidenced by more than 200 FIDO certified products and the embedding of FIDO capabilities into major browsers and operating systems – all with a focus on producing a solution that aligns with recommendations from the 2008 Commission, as well as the 2011 National Strategy for Trusted Identities in Cyberspace (NSTIC). The government should respond by taking specific steps to accelerate demand for, and use of, these solutions.

   The government has several different roles to play in accelerating the adoption of strong authentication:

   i. **Government as an operator of IT infrastructure:** With an annual IT budget of nearly $90 billion, the U.S. government operates one of the largest and most sophisticated set of IT

[7] https://www.gpo.gov/fdsys/pkg/FR-2004-07-26/html/04-16894.htm

[8] http://csrc.nist.gov/groups/ST/hash/policy_2006.html

systems in the world. The government has policies in place mandating use of strong authentication on government systems (such as HSPD-12), however, as was demonstrated after the OPM breach[9], most agencies have not heeded these policies – or in many cases, have found the specific types of authentication solutions that were mandated to be difficult to deploy or integrate.

12 years have passed since the creation of HSPD-12 and the Personal Identification Verification (PIV) card standard; as detailed in the 'Evolution of the Authentication Market" table above, the types of hardware-based cryptographic authentication capabilities that 8 years ago required issuance of a smart card are now being built into many COTS devices. With this change, the U.S. government should look to embrace new standards such as FIDO that can deliver public key cryptographic authentication solutions without the cost or overhead of a traditional smart card solution. FIDO can be particularly helpful in addressing use cases where a traditional PIV card is challenging to deploy but there is still a need for public key cryptographic authentication.

The Office of Management and Budget (OMB) should also be empowered to do more to enforce IT security policies, including those for strong authentication. While OMB has the authority in theory to hold agencies accountable, in practice these powers have not been fully applied, with the result being that many government IT security policies (such as HSPD-12 and M-11-11) have gone unimplemented by agencies. This leads to an inconsistent approach to cybersecurity that leaves Federal systems open to many vulnerabilities. The OPM breach was just one example of the consequences of this approach.

ii. **Government as a provider of citizen services:** Simple, easy-to-use strong authentication is key to the delivery of online citizen services. This point was recognized in both the 2011 NSTIC, as well as Executive Order 13681, issued in 2014. The latter included a provision entitled *Securing Federal Transactions Online* which stated:

> To help ensure that sensitive data are shared only with the appropriate person or people, within 90 days of the date of this order, the National Security Council staff, the Office of Science and Technology Policy, and OMB shall present to the President a plan, consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.

To date, many agencies have not yet complied with this Executive Order. The U.S. government should make it a priority to ensure citizen facing digital services properly protect sensitive data and look to next-generation authentication solutions such as FIDO to do so. As noted earlier, many consumer electronic devices such as laptops and smartphones are being shipped with FIDO authentication solutions embedded, removing a major barrier to citizen use of strong authentication to access government applications. This means that government does not need to be an issuer of authentication solutions for citizen-facing applications – technology that is widely in use in the marketplace today that allows Americans to "bring their own authenticator" to different sites and applications.

iii. **Government as a policymaker and regulator:** Eight years ago, the Commission on Cybersecurity for the 44th Presidency flagged the importance of Identity and Access Management (IAM) in addressing cyber threats, stating: "*We recommend that the United States adopt regulations that require robust authentication for access to critical infrastructures.*"

[9] Less than 43% of agencies had implemented HSPD-12 requirements for strong authentication as of June 2015, as detailed at https://www.performance.gov/downloadpdf?file=Sprint%20Results%20Report%20FY15_Q2.pdf

Today, only the financial services sector has a comprehensive set of regulations for strong authentication; other critical infrastructure sectors have not addressed this topic in a holistic manner.

While we are not advocating for specific new regulations in any one sector, we do note that any infrastructure that is "critical" but being protected with only a password is vulnerable to a wide array of attacks.

The voluntary Cyber Security Framework (CSF) for Critical Infrastructure published by NIST has been a very useful tool for improving cyber risk management across all critical infrastructure sectors. The Framework did not, however, include any requirements for strong authentication or advise against use of passwords.

This was in part – according to the Roadmap for Improving Critical Infrastructure Cybersecurity – due to concerns at the time of publication in 2014 about an inadequate framework of standards to promote security and interoperability, as well as concerns about the challenges in integrating authentication into many control systems.[10]

The leadership of the FIDO Alliance took this Roadmap statement quite seriously, and we are pleased to report that in 2016 – two years after the Framework was first issued – significant progress has been made in addressing the challenges outlined, including the creation of authentication standards that deliver strong security, usability and interoperability.

We believe it is imperative that the next update of the CSF include requirements for strong authentication. As helpful as the CSF is, today it is possible for an organization to fully implement the CSF and use only passwords for authentication – a set of circumstances that, given the data we have on passwords from the Verizon DBIR and other studies, means that this organization would be highly vulnerable to an increasingly trivial and effective phishing or malware attack.

The Commission should also note that some regulators have shied away from issuing regulations around strong authentication – despite the documented security vulnerabilities around authentication solutions rooted in passwords – given concerns that legacy MFA solutions were expensive, clunky, and created burdens for the end-user.[11]

FIDO changes the game – it is a technical advancement that specifically addresses these cost and usability issues. FIDO enables simpler, stronger authentication capabilities that businesses and consumers can adopt at scale. The government should recognize that with this evolution of the market and the emergence of FIDO, requirements for use of multi-factor authentication no longer push higher burdens or costs onto implementers or end-users.

iv. **Government as an influencer:** The NSTIC was influential is setting a high bar for industry, as well as a vision for the future of identity and authentication. More recently, the Administration's Cybersecurity National Action Plan (CNAP) included an initiative to launch a public-facing campaign in partnership with the private sector to promote the adoption of strong authentication amongst consumers and businesses; the "Lock Down Your Login" campaign will launch in late September.

[10] The Framework's Roadmap contains an extensive discussion on authentication and flags it as an area to be addressed in future iterations of the framework. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[11] HHS, for example, opted in 2015 to refrain from any new mandates for strong authentication in Health IT systems, citing a commenter who argued that "current approaches to multi-factor authentication are costly and burdensome to implement." See https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base

The U.S. government should continue to support efforts such as the "Lock Down Your Login" campaign, and look to launch other efforts to promote the use of strong authentication.

Additional items for the Commission to consider

1. **FIDO does not solve the "identity proofing" issue** – much work remains to be done here. As background, "authentication" is one component of "identity." Issuance of a strong identity credential involves two components:

   1) An identity proofing process that validates that someone is who he or she claims to be.
   2) Issuance of an authentication token that can be used in the future to authenticate that person.

   FIDO standards are focused on the authentication token; FIDO solutions must be integrated with identity proofing solutions to create a strong identity credential.

   As the authentication problem becomes easier to solve, we believe more attention will need to turn to the identity proofing process – particularly as challenges with legacy remote identity proofing solutions such as "Knowledge Based Authentication" and "Knowledge Based Verification" become clearer[12]. We note that NIST, through its NSTIC pilots, has awarded some pilots that seek to pioneer new types of identity proofing solutions which, in some cases, can then be easily bound to FIDO solutions. This "componentization" of the identity space – allowing for the separation of identity proofing from token issuance – is helping to stimulate new models in the identity and credentialing market.

2. **Education is one of the most important elements of promoting uptake of strong authentication.** To that end, it will be important to continue building momentum on existing efforts like the *Lock Down Your Login* campaign (launching September 2016), *STOP. THINK. CONNECT.*, and *National Cyber Security Awareness Month* (NCSAM) by having the new president and key Administration officials from the U.S. Department of Homeland Security (DHS), the Department of Commerce, the Federal Trade Commission (FTC) and other federal agencies speak out early on the need for individuals and businesses to take steps to be safer and more secure online.

We would welcome the opportunity to engage further with the Commission on this topic. Our executive director, Brett McDowell, can be reached at brett@fidoalliance.org.

[12] KBA and KBV are identity proofing tools where consumers are asked several questions tying back to their credit reports or other databases of personal information, with the idea that only the consumer will be able to successfully answer them. Recent attacks such as last year's hack of the "Get My Transcript" application at the IRS have made clear that adversaries are increasingly able to circumvent these tools. (see http://krebsonsecurity.com/2015/05/irs-crooks-stole-data-on-100k-taxpayers-via-get-transcript-feature/)