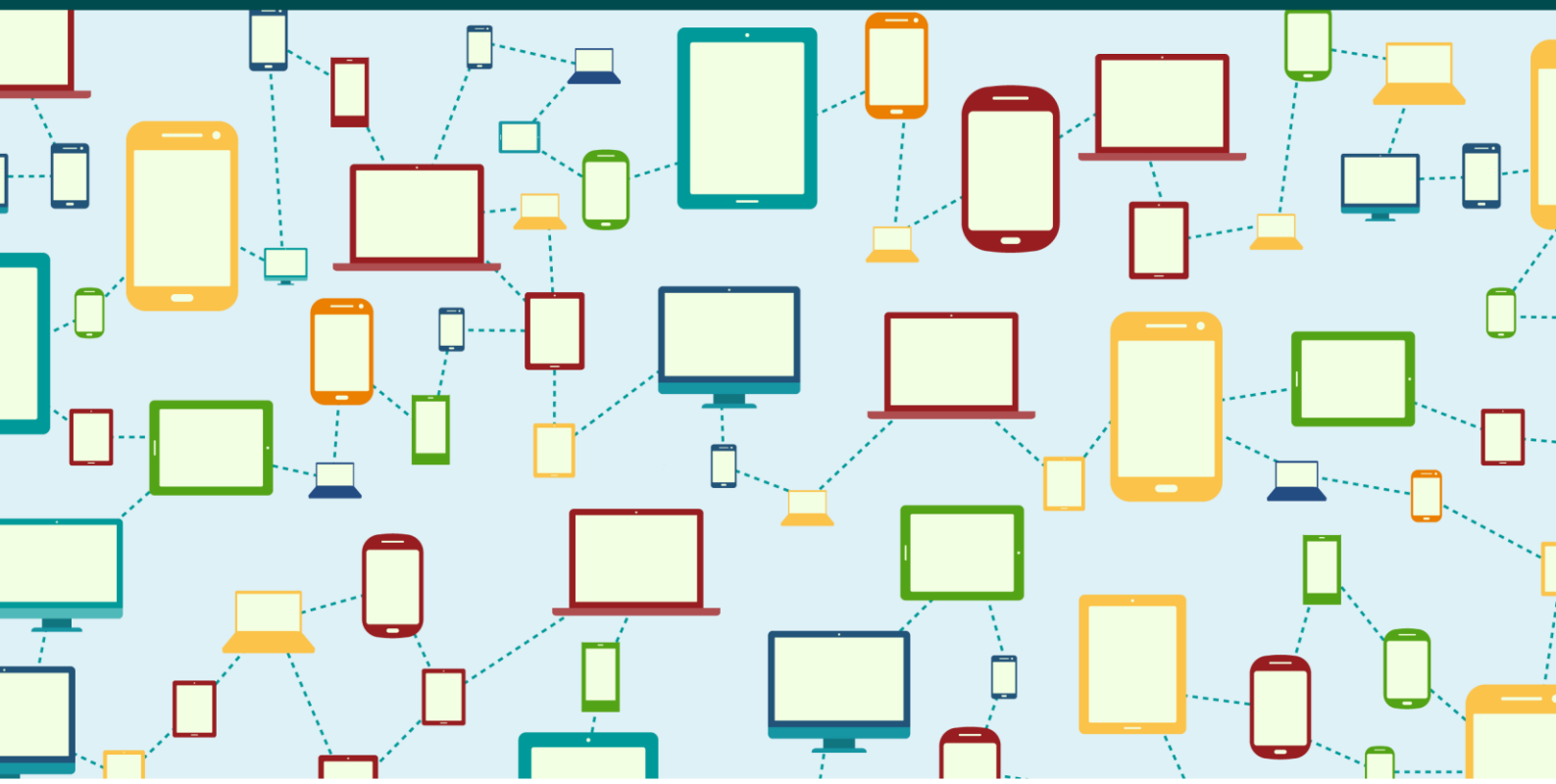
fido alliance | simpler stronger authentication



FIDO Alliance Input to the National Institute of Standards and Technology (NIST):

Request for Information (RFI) on the Framework for Improving Critical Infrastructure Cybersecurity

April 2017

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the National Institute of Standards and Technology (NIST) Request for Information (RFI) on the Framework for Improving Critical Infrastructure Cybersecurity.

Three years ago, NIST laid out a number of challenges in the "Roadmap for Improving Critical Infrastructure Cybersecurity" that accompanied the release of the Framework. The roadmap flagged Authentication as the first "high priority" area for Development, Alignment, and Collaboration – noting that while *"poor authentication mechanisms are a commonly exploited vector of attack by adversaries"* and that *"Multi-Factor Authentication (MFA) can assist in closing these attack vectors,"* NIST did not include recommendations on MFA in the Framework because:

> *"There is only a partial framework of standards to promote security and interoperability. The usability of authentication approaches remains a significant challenge for many control systems, as many existing authentication tools are for standard computing platforms. Moreover, many solutions are geared only toward identification of individuals; there are fewer standards-based approaches for automated device authentication."*

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to creation of standards for Multi-Factor Authentication (MFA).

Our 32 board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership.

Naturally, the members of the FIDO Alliance took NIST's statement quite seriously.

We are pleased to report that in 2017 – three years after the Framework was first issued – the global Information Technology industry represented in the FIDO Alliance has delivered a comprehensive framework of open industry standards for MFA, fundamentally changing the landscape and closing the gap originally observed by the NIST authors of CSF. These standards have delivered improvements in online authentication by means of open, interoperable technical specifications that leverage proven public key cryptography for stronger security and device-based user verification for better usability. The impact of FIDO standards, and formal certification testing to those standards, is notable:

- Firms including Google, Microsoft, Bank of America, PayPal, eBay, Facebook, Dropbox, Salesforce and NTT DOCOMO have deployed authentication solutions based on the FIDO standards; in total, FIDO solutions are available to protect more than 3 billion accounts worldwide

- The W3C is on pace to finalize a formal new Web Authentication standard based on FIDO specifications later this year. Once finalized, FIDO functionality will be embedded in most major browsers (i.e., Chrome, Edge, Firefox).

- More than 300 products have been FIDO-certified – demonstrating a mature, competitive, interoperable authentication ecosystem.

FIDO is not the only advancement in authentication since the publication of the CSF, but it is an important example of how a major, industry-led initiative has changed the landscape in a substantial way.

While industry has made significant progress on addressing the authentication issues laid out in the Roadmap since the publication of the original CSF, the problems caused by inadequate authentication have only gotten worse.

At the time the Framework was published, in early 2014, the United States was just getting its arms around the scope of the Target breach, which was caused by adversaries leveraging a stolen password-based credential from one of Target's HVAC contractors.

Since that time, the world has seen a wave of major breaches where passwords provided the entry point. Indeed, it is hard to find a major breach over the last few years where weak authentication did not provide the attack vector, a point noted by the Commission on Enhancing National Cybersecurity, who stated in December 2016:

> *"A review of the major breaches over the past six years reveals that compromised identity characteristics have consistently been the main point of entry."*[1]

The Commission was spot-on in its comments here, as evidenced by the list of major breaches over the last three years detailed in the table below.

Breach	Date	Attack Vector
Oracle/MICROS	August 2016	Compromised Password
DNC	July 2016	Compromised Passwords
Bangladesh Bank Heist	February 2016	Compromised Passwords
OPM (2 breaches)	May 2015	Compromised Password
IRS "Get My Transcript"	May 2015	Inadequate Authentication
Anthem	February 2015	Compromised Password
Sony Pictures	December 2014	Compromised Password
Home Depot	September 2014	Compromised Password
Apple iCloud	August 2014	Compromised Passwords
JP Morgan Chase	July 2014	Compromised Password
Target	December 2013	Compromised Password

This series of major breaches tied to passwords is nothing short of a cyber epidemic, targeting both private sector and government systems. And it makes clear that any system protected by passwords alone cannot properly mitigate cyber risk.

[1] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

As the Commission report noted:

> *"Stronger authentication of identities for interactions that require such proof must also be a key component of any approach for enhancing our nation's cybersecurity. Identity, especially the use of passwords, has been the primary vector for cyber breaches— and the trend is not improving despite our increased knowledge and awareness of this risk. Our reliance on passwords presents a tempting target for malicious actors. Despite the technical and demonstrated real-life success of a variety of novel approaches for improving identity management, individual users and the nation are still lagging significantly. Consequently, we are making it too easy for those who seek to do harm, whether they be nation-states, well-organized criminal groups, or online thieves."*
>
> *"An ambitious but important goal for the next Administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack."*

With this in mind, we have three specific comments and recommendations:

1. **Authentication must be explicitly addressed in updates to the Framework Core**.

   If the Framework is to meet its goal of helping critical infrastructure entities across both government and industry better manage cyber risk, then the risk caused by inadequate authentication mechanisms must specifically be addressed in the Framework core. No other cyber-attack vector has been exploited as much in the three years since the CSF was published.

   Without a reference to this critical control, organizations following the CSF will continue to interpret its absence as an inferred recommendation by NIST to de-prioritize strong authentication relative to other cyber risk mitigation practices, and will therefore continue to deploy authentication measures that undermine all other mitigations by leaving a hole in their defenses.

   In addition to the report from the Commission on Enhancing National Cybersecurity, the impact of weak authentication has been documented in Verizon's 2016 Data Breach Investigations Report (DBIR), which noted: "*63 percent of confirmed data breaches involved weak, default or stolen passwords*," and recommended that every organization "*Use two-factor authentication: This can limit the damage that can be done with lost or stolen credentials.*"[2]

   In addition, the National Cyber Security Alliance (NCSA), has stated: *"Your usernames and passwords are not enough to protect key accounts."*[3]

   Given the extensive documentation about the ways in which systems with inadequate authentication are vulnerable to attacks that are inexpensive to launch – and that have a very high success rate – it is time to address this issue.

   We strongly urge NIST to add a new PR.AC Subcategory for Authentication, reading:

   "Authentication of authorized users is protected by multiple factors."

   Such language would make clear what evidence has already documented: that use of passwords alone to manage access for authorized users is not sufficient for any organization looking to properly mitigate cyber risk.

[2] http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf
[3] https://staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securing-your-accounts

Addition of this language is consistent with:

1. What was called for in the CSF Roadmap two years ago
2. What was recommended by a number of the 2016 RFI respondents – not just FIDO Alliance, but also several other respondents to the RFI
3. NIST's own report from June 9, 2016 on the 2016 CSF workshop, which stated: "*Participants generally felt that the Framework Core could be updated to include authentication, with many singling out the Protect Function specifically.*"[4]
4. The Framework's focus on driving an approach to cyber risk management that leads to better cybersecurity outcomes.

The need for strong authentication has become so acute that the National Cyber Security Alliance (NCSA) launched a major "*Lock Down Your Login"* campaign last year targeting consumers and businesses.[5] The message has extended well beyond the security and IT communities; publications such as Teen Vogue are urging their readers to turn on MFA.[6]

2. **The draft Framework Version 1.1 is confusing on this topic and must be clarified.** The "Notes to Reviewers" section of the new draft seems to suggest that authentication is addressed, yet the core itself does not include the word "authentication."

Specifically: the "Notes to Reviewers" section on the update states that the changes to Framework Version 1.1 includes refinements to better account for authentication. Per the "Notes" section:

Update	Description of Update
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to account for authentication, authorization, and identity proofing. A Subcategory has been added to that Category. Finally, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.

However, this language is not reflected in the Framework Core itself. While the PR.AC section of the updated Framework Core (on page 32) has been renamed *"Identity Management, Authentication and Access Control (PR.AC),"* the word "Authentication" does not appear in any of the six PR.AC Subcategories.

The new Framework Core is thus both confusing and functionally incomplete. If Authentication is intended to be part of the PR.AC core, it needs to be described in a Subcategory for the sake of clarity and completeness.

Again, we strongly urge NIST to add language to add a new PR.AC Subcategory around Authentication, reading:

"Authentication of authorized users is protected by multiple factors."

[4] See NIST's June 9, 2016 report at https://www.nist.gov/sites/default/files/documents/cyberframework/Workshop-Summary-2016.pdf

[5] https://www.lockdownyourlogin.com/

[6] http://www.teenvogue.com/story/why-two-factor-authentication-is-important

While we would welcome the inclusion of the FIDO standards[7] in the Informative References section of the subcategory, we believe inclusion of a reference to the soon-to-be-finalized SP 800-63-3 is an absolute requirement. The updated SP 800-63-3 quite artfully lays out a set of guidelines for digital identity that will help organizations select identity solutions that reflect both the state of the market and threat level, and also are appropriate to the level of risk of the transaction. Indeed, while the document is still in draft, we can report that a number of organizations – including many of our members – are already starting to look to the new draft guidance when crafting digital identity solutions. Even in draft form, it has been viewed as something that is more helpful than the legacy guidelines.

As a whole, the FIDO Alliance believes NIST has approached the revision of SP 800-63 in a manner that is thoughtful and forward-leaning, with a focus not only on updating the document to reflect the most current threats and vulnerabilities, but also crafting the document in a way that will make it easier for implementers to use.

3. **While the primary focus of our comments is authentication, we are highly supportive of other identity-centric changes to the PR.AC function, including:**

   - Updating PR.AC-1 to reflect not just how identities are "managed," but rather detailing the full identity governance lifecycle – looking at issuance, management, verification, revocation and audit. Proper enterprise identity security requires that enterprises take a holistic view that looks at a full lifecycle approach.

   - The change in PR.AC-4, which adds the words "and authorizations" to the list of things that need to be managed. Again, this change will make clear that organizations need to focus not only on a full lifecycle approach to identity management, including what users are authorized to do with their credentials.

   - The addition of a new control – PR.AC-6 – focusing on ensuring that "Identities are proofed and bound to credentials, and asserted in interactions where appropriate."

   We are encouraged that NIST recognizes the importance of identity in cybersecurity enough to support the addition of one new subcategory and the substantial rewrite of two more in the PR.AC group. Now is the time to complete a proper update to the PR.AC function by including language to address risks caused by weak authentication.

We look forward to further discussion with NIST on this topic, and would welcome the opportunity to answer any questions. Please contact our Executive Director, Brett McDowell, at brett@fidoalliance.org.

[7] FIDO standards are available at https://fidoalliance.org/download/