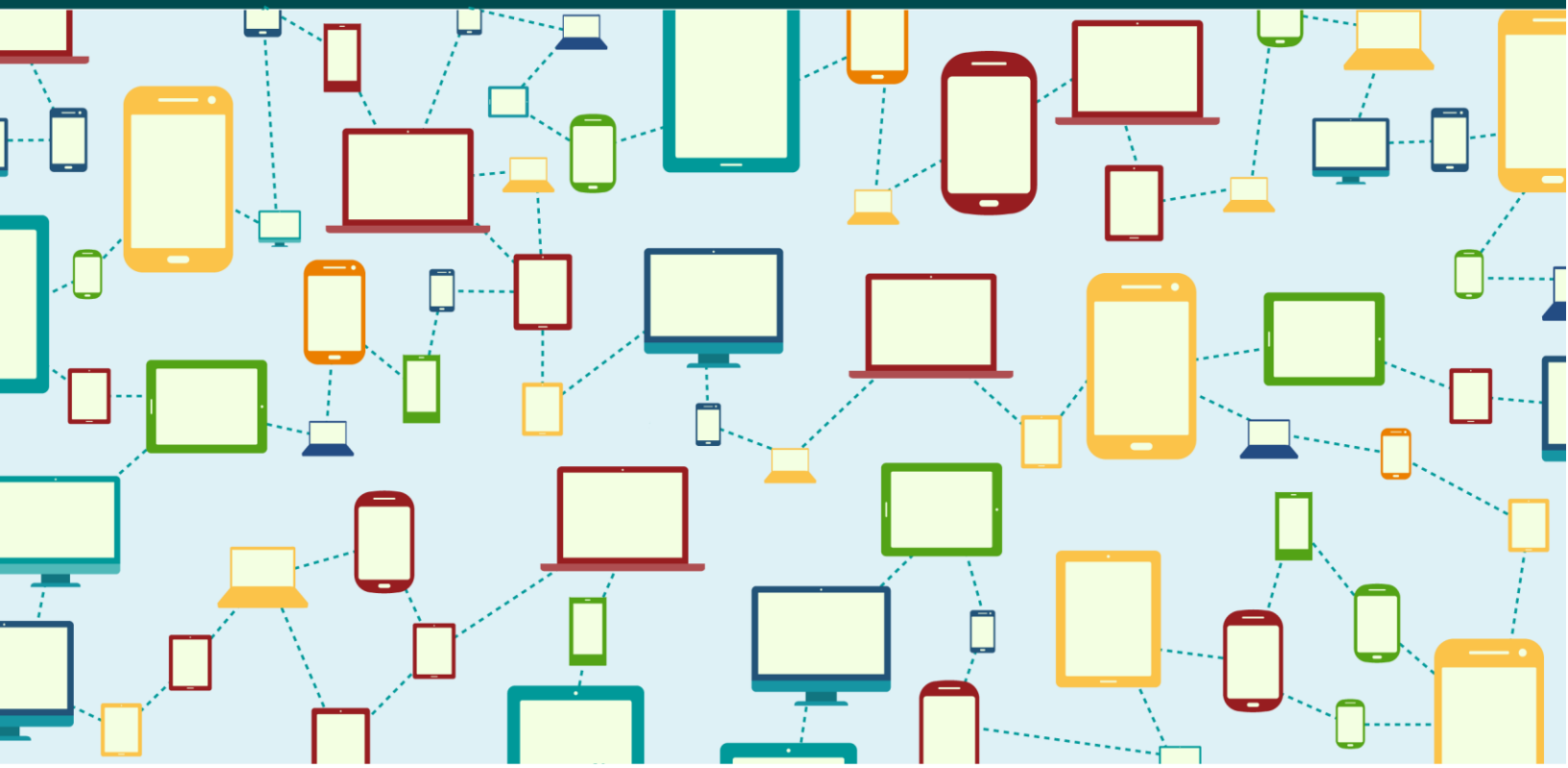
fido ALLIANCE | simpler stronger authentication



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

Request for Information (RFI) on the Framework for Improving Critical Infrastructure Cybersecurity - Framework Version 1.1 Draft 2

January 2018

Copyright © 2018 FIDO Alliance All Rights Reserved.

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 - Framework Version 1.1, Draft 2.

Four 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 34 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 2018 – nearly four 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.

©FIDO Alliance 2018

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 their peers around the world such as NTT DOCOMO and Bank of China 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 soon finalize a formal new Web Authentication standard based on FIDO specifications. Once finalized, FIDO functionality will be embedded in most major browsers (i.e., Chrome, Edge, Firefox).

- More than 380 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.

Comments on Draft 2 of CSF Version 1.1

As a whole, we are pleased by the direction NIST took in Draft 2 of Framework Version 1.1. The draft finally, formally recognizes the importance of strong authentication, particularly the importance of MFA.

As background, last April, FIDO responded to NIST's RFI with three specific comments and recommendations:

1. **Authentication must be explicitly addressed in updates to the Framework Core**. To this point, we recommended that NIST add a new PR.AC Subcategory for Authentication.

2. **The draft Framework Version 1.1 was confusing on this topic and must be clarified.** This was because the "Notes to Reviewers" section of the Draft 1 of version 1.1 seemed to suggest that authentication is addressed, yet the core itself did not include the word "authentication."

3. **We were 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.

©FIDO Alliance 2018

- The change in PR.AC-4, which adds the words "and authorizations" to the list of things that need to be managed.

- 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 appreciate that NIST directly addressed all three of our comments in Draft 2.

The new language directly recognizes the importance of strong authentication and is much improved over the previous version.

Our concern with the previous draft was simple: without a reference to authentication as a critical control, organizations following the CSF would continue to interpret its absence as an inferred recommendation by NIST to de-prioritize strong authentication relative to other cyber risk mitigation practices, and would therefore continue to deploy authentication measures that undermine all other mitigations by leaving a hole in their defenses.

By creating a new Subcategory for Authentication (PR.AC-7), NIST has addressed this concern. While we continue to believe that this language could be stronger (our recommendation was for language that stated "Authentication of authorized users is protected by multiple factors"), we believe that the new language will go a long way to mitigate concerns about the previous Framework draft.

We do have two additional comments for NIST's consideration:

1. **NIST should add a reference to NIST SP 800-63-3 to the list of Informative References for PR.AC-6 and PR.AC-7**

   We were surprised that SP 800-63-3 was not included in the new Draft, given the July, 2017 report from NIST's 2017 Cybersecurity Framework Workshop Summary[1] that stated:

   > *With the addition of more content to the Access Control Category and the potential inclusion of language around authentication, participants suggested the inclusion of more references specific to managing identity and stated the importance of references that reflect guidance to address challenges of identity proofing, authentication, and authorization.*
   >
   > *Participants specifically requested the addition of NIST SP 800-63, Digital Identity Guidelines and other internationally recognized identity standards and guidance (e.g., ISO 29115, Good Practice Guide 44 & 45) to the Informative References.*

   From our perspective, inclusion of a reference to SP 800-63-3 is an absolute requirement. The updated SP 800-63-3 quite artfully lays out a set of risk-based guidelines for digital identity that helps organizations select identity solutions that reflect both the state of the market and

[1] https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf

threat level, and also are appropriate to the level of risk of the transaction. We can report that a number of organizations – including many of our members – are already using SP 800-63-3 when crafting digital identity solutions.

Moreover, the other standards listed under informative references for PR.AC-6 and PR.AC-7 are older, and do not reflect the more modern set of risks associated with identity in cyberspace today. The practical impact of this exclusion is that NIST will be referring implementers to standards that are arguably outdated, and not geared toward addressing the most recent attack vectors against identity solutions.

As a whole, the FIDO Alliance believes NIST 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.

The updated Framework Core is incomplete without including it as a reference.

2. **We were pleased to see an updated Roadmap for the CSF that covered challenges in identity – and acknowledged some of the progress made by the public and private sectors since the initial launch of the CSF.**

   We appreciate recognition in the new Roadmap of the work being done in FIDO Alliance as well as the W3C – both are highly important efforts to eliminating threats in cyberspace caused by use of passwords. We also appreciate the Roadmap's reference to the continued challenges organizations face in cybersecurity due to attacks that leverage weak or stolen passwords.

   The updated Roadmap lays out a number of important activities where NIST plans to engage, focused on driving progress through partnerships with industry. FIDO Alliance and its members look forward to continuing to work with NIST to improve identity and authentication standards, as well as helping organizations leverage these standards to better mitigate cyber risk.

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.