DIGITAL INSANITY: EXPLORING THE FLEXIBILITY OF NIST DIGITAL IDENTITY ASSURANCE LEVELS

Dr. Kenneth Myers, DSc

Marymount University

May 19, 2023

https://doi.org/10.34190/iccws.18.1.1032

THE CHALLENGE - NIST DIGITAL RISK MANAGEMENT (2017)

Level	Identity	Authenticator	Federation
1	Self Attest	Single Factor	Signed
2	Remote Proofing	SW Multifactor	Signed/Encrypted
3	Supervised Proofing	HW Multifactor	Sign/Encrypt/Verify

RQ1) Provides flexibility to determine assurance levels?
RQ2) Is MFA always required?
RQ3) Does a risk assessment for using phishable MFA match current threats?

"The ability to combine varying xALs offers significant flexibility to agencies, but not all combinations are possible due to the nature of the data collected from an individual and authenticators to protect that data" (Grassi et al., 2017, p.33)

RISK ASSESSMENT

1. Potential for inconvenience, distress, or damage to standing or reputation.
2. Potential impact on financial loss.
3. The potential impact of harm to agency programs or public interest.
4. The potential impact of unauthorized sensitive information release.
5. Potential impact on personal safety.
6. The potential impact of civil or criminal violations.

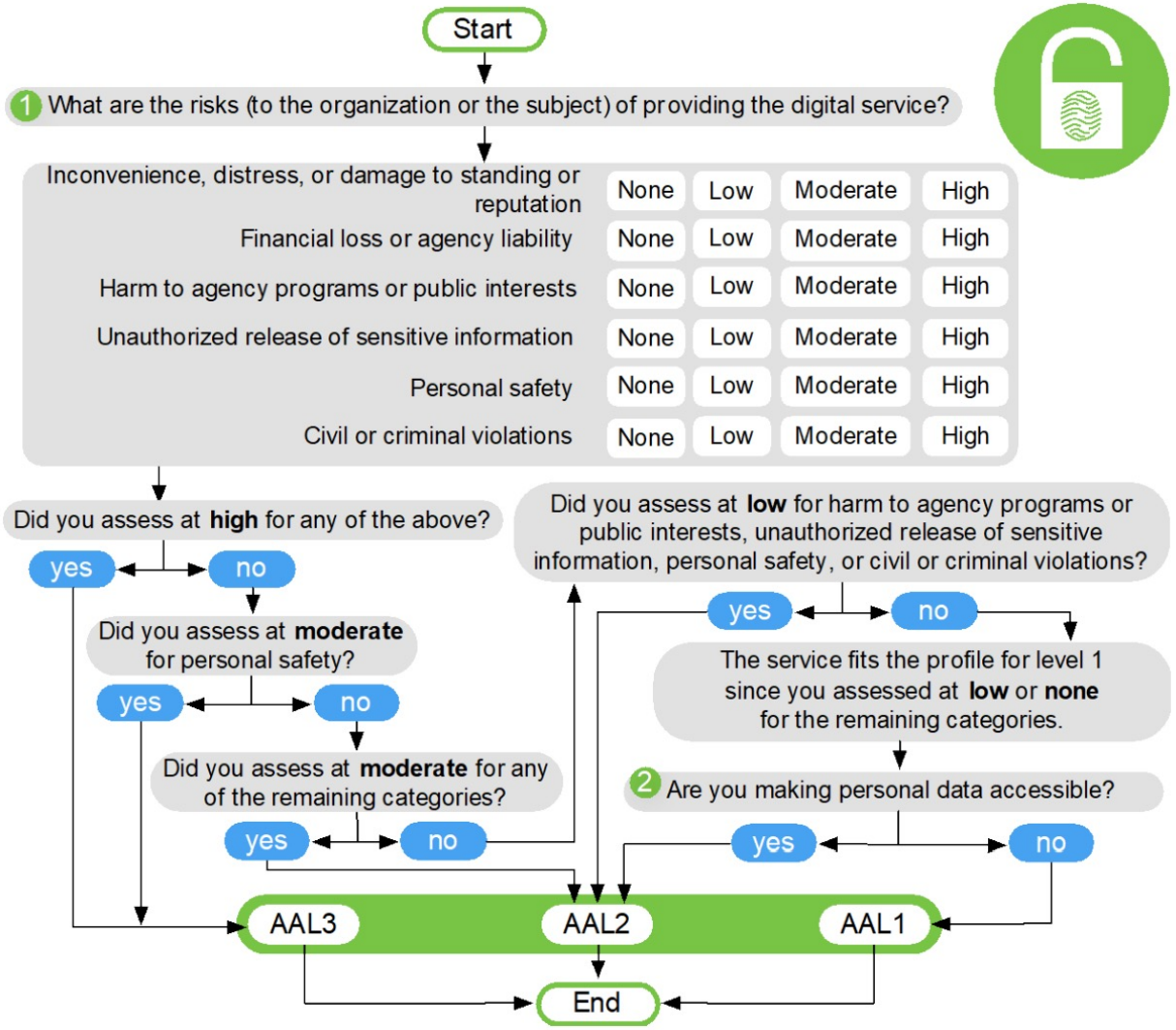
ADOPTION?

- Other NIST risk management frameworks have multiple adaptations (e.g., NIST CSF translated into nine languages). No similar evidence for DIRM.
- Many federal public websites still use username and passwords.
- Mentioned for federal government adoption in OMB Memo 19-17, FICAM Risk Assessment Playbook, NSA Fact Sheet, and DOD Identity Reference Architecture. MITRE, Microsoft, and Forgerock have configuration guidance aligned to assurance levels.

Findings:

1. Publication is hard to understand if you're not a risk management or identity professional. Even hard if you are…
2. Few examples of how to apply conformance criteria.
3. Little guidance to help explain how to determine an assurance level.

THE QUESTION - DOES IT OFFER FLEXIBILITY?



THE METHOD - DEVELOPED A TOOL

- Developed five test cases to test component and assurance level flexibility.

Test 5 - PII Yes, Personnal safety moderate				2	1	1
Is PII or PHI collected and does it need to be validated?	*Yes & I Don't Know*			2		
Impact Category	**Select Impact Definition***	**Impact Level**		**IAL**	**AAL**	**FAL**
Inconvenience, distress, or damage to standing or reputation to the agency	*t worst, limited, short-term inconvenience, distress, or embarrassment to any part*	Low		1	1	1
Financial loss or agency liability	*r inconsequential financial loss to any party, or at worst, an insignificant or incons*	Low		1	1	1
Harm to agency programs or public interests	*Not Applicable*	Not Applicable		1	1	1
Unauthorized release of sensitive information	*Not Applicable*	Not Applicable		1	1	1
Personal safety to users	*Not Applicable*	Not Applicable		1	1	1
Civil or criminal violations	*Not Applicable*	Not Applicable		1	1	1

THE RESULTS

✓ Component Flexibility

✗ Level Flexibility

Test Case	Identity Assurance Level	Authenticator Assurance Level	Federation Assurance Level
#1. Includes PII, All categories low or N/A	2	2	1
#2. No PII, Any category moderate except personal safety.	2	2	2
#3. Includes PII, Sensitive information high	3	3	3
#4. Includes PII, Financial Loss high	3	3	3
#5. Includes PII, Personal safety moderate	3	3	3
#6. No PII, All categories low or N/A	1	1	1

Additional findings:

- All enterprise uses cases should enforce MFA and most likely phishing-resistant MFA.

Abstract accepted to 18th International Conference on Cyber Warfare and Security (ICCWS) – March 2023

ADDITIONAL RECOMMENDATIONS

1. If the federal government wants wide adoption, consider a public law, executive order, or FIPS that requires federal agencies to implement digital identity risk management.
2. Given the phishing susceptibility of most Authenticator Assurance Level 2 authenticators, NIST should update their guidelines only to specify phishable MFA options for non-enterprise use cases. In contrast, phishing-resistant MFA should be used for all enterprise or low to moderate-risk transactions.
3. Since the harm categories are consistent across each assurance level, consolidate the risk determination flow charts.

- ❑ Convert the spreadsheet into a website.
- ❑ Include a narrative section to explain the harm category and post on a public website to further understanding and adoption.
- ❑ Further explore use cases if all enterprise MFA should be phishing-resistant MFA or specific use cases (could change with new NIST SP).
- ❑ NIST SP 800-63 is about to release a Rev 4 very soon. Proposed changes based on this.

WHAT'S NEXT?