kyndryl

Kyndryl
One Vanderbilt Avenue
15th Floor
New York, NY 10017 USA

October 7, 2024

Laurie Locascio
Under Secretary of Commerce for Standards and Technology
Director of the National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Dear Under Secretary Locascio,

On behalf of Kyndryl, we welcome this opportunity to submit our input on NIST 800-63b-4.

Kyndryl appreciates the balance that NIST is attempting to strike between the advantages in security from password complexity and rotation and the disadvantages of encouraging lax user security hygiene. NIST's balancing is premised, in part, on assumptions about the probability and extent to which users in the general public will engage in poor security practices to avoid the burden of complying with the security requirements.

Such assumptions, however, do not apply in all instances. Notably, such assumptions do not apply when the set of users is more security-conscious than the general public or when the credential service provider (CSP) can directly influence the behavior of the users. In such circumstances, NIST's guidance should permit organizations to have flexibility to use complexity and frequent rotation to harden their security.

Kyndryl, like with other managed services providers and many other large enterprises with experienced and skilled IT staff, has significant influence over the security consciousness of its employee-users. Kyndryl employees participate in regular security training and awareness programs. Kyndryl also makes available to employees, and strongly encourages the use of, password vaults and similar tools to simplify the management of multiple, complex passwords that are changed frequently. In addition, Kyndryl and other managed services providers often manage credential systems for sophisticated enterprise clients; many of these enterprise clients operate in industries accustomed to heightened security requirements and with employees possessing a security consciousness above that of the general public. The new draft guidance proposes a mandatory bar that would serve to make such entities less secure.

Furthermore, previous guidance by NIST (as well as other organizations, such as CISA), encouraged password complexity as well as regular changing of passwords. Such guidance is in line with current standard industry security practices and often is included in business to business industry contracts. Such contracts often include both specific provisions that explicitly require a mix of letters, numbers, and punctuation, as well as 60- or 90-day change periods. Such these contracts also often include requirements to comply with NIST and other international standards. NIST's proposed guidance thus may impose conflicting obligations on managed services providers and their enterprise customers.

Kyndryl suggests that NIST alter its proposed rules in 3.1.1.2 (5) and (6) from a mandatory "SHALL NOT" to a disfavored-but-permissive "SHOULD NOT". We believe this adjustment would still provide proper guidance for the provisioning of credentials to the general public, while allowing flexibility for when different user pools permit more stringent measures. As such, we propose:
3.1.1.2 (5) "Verifiers and CSPs SHOULD NOT impose other composition rules […]"
3.1.1.2 (6) "Verifiers and CSPs SHOULD NOT require users to change passwords periodically. […]"

Kyndryl welcomes the opportunity to submit this input and likewise would welcome the opportunity to engage further with NIST on this topic.

Best,

Cory Musselman

Cory Musselman
Chief Information Security Officer