NIST Password Guidelines – What You Need to Know

Passwords have always been a hot topic of discussion both in and out of security circles. Users have always hated being forced to come up with schemes to meet the complexity rules or change their password at defined intervals. The multitude of password requirements of the past have frustrated users and have led to bad behaviors which time after time led to compromised passwords and resultant data breaches.

The changes in direction for passwords as outlined in NIST 800-63-3 and are significant as they contradict the decades-old password requirements that drove everyone crazy, and they relieve users of much of the pain when dealing with passwords.

What Are NIST Guidelines?

The National Institute for Standards and Technology (NIST) is a governmental organization under the Department of Commerce. The NIST is essentially a scientific organization that focuses on measurement science, the development of scientific and other standards, and technology development. As part of their responsibilities, NIST creates guidelines and standards supporting the measurement and technology fields such as health and bioscience, advanced manufacturing, advanced communications, forensic science, and cybersecurity.

Under the Federal Information Security Management Act of 2014, NIST was charged with developing information security and privacy standards and guidelines. Their standards and technology publications in the cybersecurity realm are extensive. They include topics such as encryption, zero trust architectures, risk management, application container security, identification and authentication, etc.

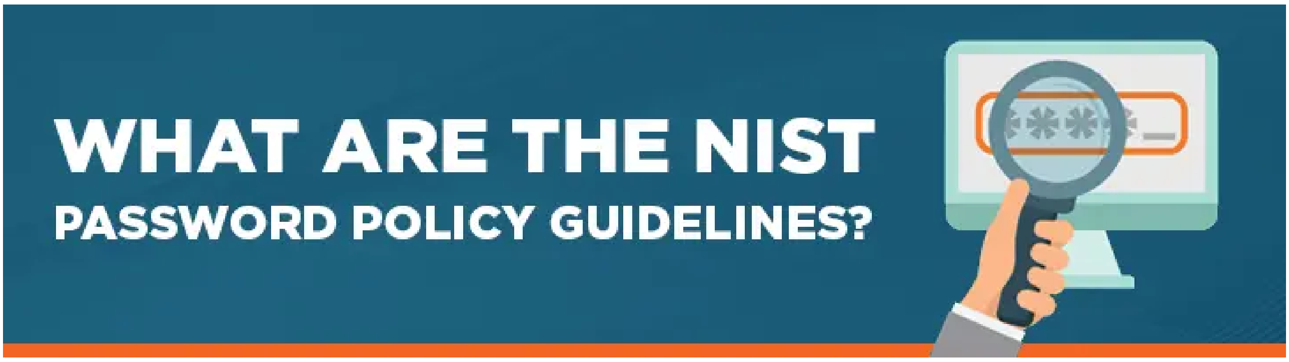
One of the most well-known of their security publications is Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. It is at the heart of the various Risk Management Frameworks and is a comprehensive guide to security control definitions and supporting information.

What is the Industry Standard for Password Policy?

There is no one organization that defines password policy for commercial organizations. NIST develops the standards for the federal government and their password guidelines are mandatory for federal agencies. NIST password guidelines are also extensively used by commercial organizations as password policy best practices.

The new NIST password guidelines are defined in the NIST 800-63 series of documents. There are four volumes that comprise the NIST 800-63 *Digital Identity Guidelines*. NIST 800-63-3 provides "technical requirements for Federal agencies implementing digital identity services" and covers areas such as "identity proofing, registration, authenticators, management processes, authentication protocols, and related assertions."

Volumes A, B, and C get more into the details of managing digital identities. Volume A covers enrollment and identity proofing. Volume B covers authentication and lifecycle management, and Volume C covers federations and assertions. NIST 800-63 Volume B received a lot of attention in the security world because it broke with the norms of the previous decade's (or more) guidelines/requirements for password management.



What are the NIST Password Policy Guidelines?

NIST did not recommend undoing everything we've known regarding passwords and leave it at that – that approach would be negligent. Some of the changes introduced in SP 800-63B are based on studies and research which indicated that the password requirements of the past encouraged the creation of bad passwords. See below for a summary of the NIST password guidelines:

1. **Password length:** Minimum password length (for user-selected passwords) is 8 characters with up to 64 (or more) allowed.
2. **Password complexity (e.g. requiring at least one upper- and lowercase, numeric, and special character):** NIST recommends password complexity not be imposed.
3. **Character sets:** The recommendation is all printing ASCII and UNICODE characters be allowed.
4. **Password "hints"/authentication questions (e.g. what was your first car?):** Password hints/authentication questions shouldn't be used.
5. **Check for "known bad" passwords:** New and changed passwords are to be checked against a list of common or previously compromised passwords (e.g. from dictionaries, previous breaches, keyboard patterns, and contextual words [e.g. the user's username]).
6. **Throttling:** Implement throttling to limit failed authentication attempts.
7. **Password expiration:** Organizations shouldn't require users to change their password at defined intervals (e.g. 45, 60, or 90 days).
8. **Using SMS for MFA:** NIST "discourages" the use of SMS as an out-of-band authenticator and is considering removing its use in future versions of the SP 800-63 series.

SHOULD MY ORGANIZATION IMPLEMENT
THE NIST PASSWORD GUIDELINES?

Should My Organization Implement the NIST Password Guidelines?

The short answer is – it depends. It depends on which changes are made, how they are implemented within your organization, and the other compensating controls in place in your organization. Below are a few things to consider regarding each of the NIST password recommendations:

1. **Password length:** How long should a password be? Allowing a 64 character (or greater) passwords is a great move on NIST's part. It was surprising, though, that the minimum password length requirement was only 8 characters. To me, an 8-character minimum password length is insufficient. As we all know, users will do the minimum, so 8-character passwords will become the norm. Also, in today's computing environment, brute-forcing an eight-character password is trivial. I would recommend at least 15-character passwords for general users. With the removal of password complexity, this simplifies coming up with a longer password. NIST argues that in conjunction with No. 5 (checking for known bad passwords) and No. 6 (throttling), there was not a need to increase the minimum length. It may also be with the push toward MFA, an 8- character, non-complex password is sufficient. Why, though, encourage one of the two factors in an MFA solution to be weak?
2. **Password complexity (e.g. requiring at least one upper- and lowercase, numeric and special character):** This one has been the thorn in the side for many users over the years and has resulted in common substitution techniques (e.g. a 1 for the letter l, or @ for the letter a) which met the requirements but did not increase the security of the password. That said, having special characters and numbers in a password increases the

entropy, and increased entropy makes a password less susceptible to password cracking techniques.

3. **Character sets:** Increasing the allowed character set is good, but it may take some time before it is supported in some technologies.
4. **Password “hints” (e.g. what was your first car?):** Password hints/authentication questions have been used on multiple occasions to gain unauthorized access to user accounts, so getting rid of them is a good move.
5. **Check for “known bad” passwords:** As mentioned previously, this is one of the password requirements that provides “cover” for the minimum password length of eight characters. The concern here is the implementation. Organizations must be able to check for known bad passwords against repositories that are continually being updated.
6. **Throttling:** This is another one of the password requirements that provides “cover” for the minimum length policy. In general, throttling is a good idea, but my concern is in the implementation across the multitude of technologies requiring authentication. More specifically, I would be concerned that the minimum password length is quickly relaxed which is extremely easy to do while waiting some undetermined time for the throttling implementation to be put in place across all the areas where authentication occurs. The time delta between the relaxing of the minimum length (and complexity for that matter) and the implementation of throttling significantly increases an organization’s risk. Again, throttling is a good idea, but in my opinion, it shouldn’t be used as a justification for an 8-character minimum length password.
7. **Password expiration:** This is a big win for users since users often just incremented by one the number at the front or end of their password. This requirement makes the most sense, though, when paired with longer passwords, not one that is just 8 characters.
8. **Using SMS for MFA:** Using MFA with SMS is better than just relying on your password for authentication. Since the primary SMS infrastructure runs on an old infrastructure built without a thought toward security and an SMS-based MFA implementation has been exploited (in conjunction with a weak password), it is a step in the right direction to not use SMS as an MFA solution. In addition, organizational users must use MFA for all access. If MFA is not used on all access points, there is still a risk for compromise due to the very common bad practice of password reuse. Time-bound out of band authenticators that don’t require transmission to the user as SMS does are a better option and easily implemented.

What is a High Strength Password?

My concern about NIST’s password recommendations is primarily the minimum password length and dropping complexity. Regarding passwords, it is the overwhelming tendency for people to just go with what seems the easiest — the minimum 8 character password with no complexity. Yes, complexity has led to substitutions that haven’t added much to security. However, the use of complexity significantly increases the entropy in authenticators and, in my opinion, should still be used.

My recommendation is to use a pass*phrase* in which the use of special characters (e.g. spaces and punctuation) is “normal.” Think of a passphrase over 15 characters (recommend longer for administrators) that is an easy sentence to remember. Then use the normal punctuation to add complexity. Consider the following examples:

- Yes, I like to mountain bike!
- I like 2 MNTN byke w/ J0e!
- I have 1 car, and 3 bikes!

The above passphrase uses complexity (capitalization, special characters, numbers, misspelled words not in a dictionary) in a way that is easy to remember and type. Passphrases such as the above are easy to remember, over 15 characters, and include complexity in a way that is natural. Since you aren’t changing your password every 90 days, you’ll get quite adept at typing it in. Then with the addition of non-SMS based MFA, you’ll add significantly more strength to your authentication process.

Summary

Until passwordless authentication options are prevalent, passwords will still be the weak link in the authentication process. Improving passwords and authentication techniques is, as it has always been, a timely topic of discussion against the backdrop of the NIST password standards outlined in SP 800-63B. The NIST password standards represent significant departures from the federal password requirements of the past decades. To maintain a level of security with the NIST password policy guidelines the recommendations should not be considered a buffet where you only pick the things you like (e.g. minimum password of 8 characters and no complexity). Other elements such as checking for known bad passwords and throttling need to be implemented concurrently, especially with a minimum password policy of only 8 characters.

Overall, organizations should measure how the NIST password guidelines in SP 800-63B fit with their risk appetite and how they may be able to ease at least some of the burden for their users while still providing an acceptable level of protection. MFA should also be enabled for all authentication interfaces based on an organizational risk decision.

Linford & Company has extensive experience with NIST and associated NIST compliance. If you are interested in learning more about NIST requirements and compliance, please contact us.

Ray Dunham (PARTNER | CISA, CISSP, GSEC, GWAPT)

Ray Dunham started his career as an Air Force Officer in 1996 in the field of Communications and Computer Systems. Following his time in the Air Force, Ray worked in the defense industry in areas of system architecture, system engineering, and primarily information security. Ray leads

L&C’s FedRAMP practice but also supports SOC examinations. Ray enjoys working with clients to secure their environments and provide guidance on information security principles and practices.