Comments Submitted Regarding NIST SP 800-63-4 Draft by John M. Willis, Chief Risk Officer, Turnaround Security

Introduction: The proposed updates to NIST SP 800-63-4 are a significant step toward enhancing the security, privacy, and usability of digital identity solutions. These updates address emerging technologies, evolving risks, and the need for scalable, interoperable identity systems. However, there are critical areas that would benefit from further clarification and standardization. Specifically, I would like to address the topics of user-controlled wallets, support for Identity Assurance Levels (IAL) 2 and 3, Federation Assurance Levels (FAL) for authentication methods, and privileged account management.

1. Strengthening Guidance for Privileged Account Password Management and PR-MFA

While OMB M-22-09 and the NIST SP 800-63-4 draft do not explicitly differentiate between regular user accounts and privileged accounts, the elevated risk associated with privileged accounts warrants more detailed guidance. Privileged accounts grant access to critical systems and sensitive data, making them prime targets for attackers. For privileged accounts that permit interactive login, the recommendation is to disable interactive logins wherever possible to reduce risk. The draft also perpetuates a requirement to avoid rotating passwords and not require special characters for accounts in general, but agencies are unlikely to comply with this for privileged accounts due to their heightened security needs. The draft should include specific recommendations for securing these high-risk accounts through Phishing-Resistant Multi-Factor Authentication (PR-MFA) and Privileged Access Management (PAM) tools.

- **Prioritizing PR-MFA at the Application Layer**: As mandated by OMB M-22-09, Phishing-Resistant MFA must be implemented at the application level for all accounts, including privileged accounts. This ensures that privileged users authenticate using robust, phishing-resistant methods such as FIDO2 or PIV (Personal Identity Verification) cards, protecting against credential theft, phishing, and other common attack vectors. Given the critical nature of privileged accounts, this requirement is especially important to prevent unauthorized access.
    - **Reference**: OMB M-22-09 provides the mandate to implement PR-MFA across all accounts, aligning with the principles of Zero Trust Architecture for federal systems.
    - **Recommendation**: The draft should emphasize that PR-MFA is not only required but crucial for privileged accounts due to their elevated access. Agencies must prioritize the integration of PR-MFA into all systems handling privileged accounts, ensuring compliance with OMB M-22-09.
- **Leveraging Privileged Access Management (PAM) Tools**: For systems where PR-MFA cannot be implemented directly at the application layer, PAM tools can serve as a compensatory control. When using a PAM tool, automated password rotation and autologin should be required to eliminate the risks associated with manual password handling and password reuse. PAM tools should enforce PR-MFA before granting access to privileged accounts, ensuring that privileged accounts are accessed only after PR-MFA is verified.

These measures mitigate the risks posed by applications that lack native support for PR-MFA.

- **Recommendation**: The draft should explicitly recommend PAM tools for managing privileged accounts where PR-MFA cannot be directly integrated, with automated password rotation and autologin as required features to enhance security and ensure compliance with the phishing-resistant MFA requirements of OMB M-22-09.

- **Binding Non-Person Entity (NPE) Interactive Login to PR-MFA**: Non-Person Entity (NPE) accounts (such as service accounts) present unique risks due to their lack of human interaction. In cases where NPE accounts require interactive logins, they should be cryptographically tied to a person's PR-MFA session. This ensures accountability and a verifiable chain of trust for any privileged actions initiated by NPE accounts. By linking NPE authentication to a verified user, agencies can minimize the risks associated with these accounts and maintain strict control over privileged actions. Interactive logins should be disabled where possible, as NPE accounts typically do not require this functionality.
  - **Recommendation**: The draft should recommend that interactive logins for NPE accounts be disabled wherever possible. Where interactive logins are required, the draft should recommend that NPE account authentication is cryptographically tied to a human user's PR-MFA session or a verified cryptographic chain of trust to ensure accountability and compliance with the Zero Trust principles outlined in OMB M-22-09.
- **Implementing Group Managed Service Accounts (gMSA)**: For Windows environments, agencies should implement Group Managed Service Accounts (gMSA) where possible for NPE accounts. gMSAs offer automated password management, eliminating the need for manual password rotation while still providing a high level of security. By automating these processes, gMSAs reduce human error and enhance security for NPE accounts in Windows environments.
  - **Recommendation**: The draft should include a recommendation to implement gMSAs for NPE accounts on Windows systems where appropriate, to enhance security through automated password management.
- **Compensating Controls for Non-Conforming Applications**: For legacy applications that cannot support PR-MFA or automated password rotation, agencies must implement aggressive compensating controls to ensure privileged account security. These compensating controls may include:
  - Enhanced logging and auditing of privileged account activity.
  - Frequent manual password rotation.
  - Restricting access to secure environments (e.g., secure enclaves or jump servers).
  - Real-time monitoring and anomaly detection for privileged accounts to identify and mitigate unauthorized access attempts.

While OMB M-22-09 and the NIST SP 800-63-4 draft do not differentiate between regular and privileged accounts, the heightened risks associated with privileged accounts and NPE accounts with interactive logins necessitate specific guidance. The draft should provide clear recommendations for securing privileged accounts through the mandatory use of Phishing-Resistant MFA, as outlined in OMB M-22-09, and leveraging PAM tools for password management and access control. Automated password rotation and autologin should be required when PAM tools are used. Additionally, NPE interactive logins should be disabled where possible, and where interactive logins are required, they must be cryptographically tied to PR-MFA sessions. The use of gMSA for NPE accounts in Windows environments should be recommended to ensure automated password management and improved security. This guidance will better align the draft with the practical security needs of agencies managing privileged accounts and NPE accounts

2. Standardization of Communicating Authentication Methods via Federation Assurance Level (FAL)

While FAL 3 provides strong cryptographic protections and binding of assertions, there is a need for standardization of the claims or attributes used to communicate the authentication method within the assertion. Relying parties must be able to consistently and reliably interpret which authentication method (e.g., PIV, biometric) was used by the Identity Provider (IdP). Standardizing this communication ensures that all parties in a federated system understand and trust the authentication process, ultimately enhancing security, reducing spoofing risks, and promoting interoperability across platforms.

Without a standardized method of communicating the authentication process, relying parties may misinterpret the level of assurance provided, leading to potential vulnerabilities such as credential spoofing or unauthorized access. Standardization ensures a consistent and trustworthy interpretation of credentials across platforms.

3. Support for IAL 2 and IAL 3 in Services Like Login.gov and ID.me

The NIST SP 800-63-4 standards for Identity Assurance Levels (IAL) 2 and 3 provide a clear and robust framework for securing digital identity. Platforms like Login.gov and ID.me are critical to the successful adoption of these standards across federal, state, local, and tribal agencies. However, these platforms must ensure they are fully equipped to implement the necessary identity proofing and authentication mechanisms that meet the defined assurance levels. Specifically, while NIST has established the standards, platforms must adopt technologies and processes that ensure both IAL 2 and IAL 3 are supported for a variety of government services.

While the standards for IAL 2 and IAL 3 are clearly defined by NIST SP 800-63-4, it is imperative that platforms like Login.gov and ID.me are fully equipped to implement these standards. This means they must adopt the necessary identity proofing and authentication technologies to ensure compliance and to secure sensitive services.

This will ensure secure, interoperable, and scalable digital identity solutions, ultimately benefiting agencies and users alike.

4. In Support of User-Controlled Wallets and Federation Assurance Level (FAL) 3

The draft proposal highlights the role of user-controlled wallets in maintaining the integrity of credentials and attributes through cryptographic protections. I fully support the inclusion of FAL 3, as it ensures the highest level of security for credential exchanges in federated environments. Several key points should be considered to reinforce this approach:

- **Cryptographic Protections Ensure Integrity**: The cryptographic binding of credentials ensures they are tamper-proof and traceable to their origin, providing critical security for sensitive credentials like mobile driver's licenses or professional certifications.
- **Trusted Referees and Validators**: Trusted referees provide an additional layer of verification, particularly for high-assurance credentials, ensuring that all attributes entering the wallet are valid and reliable.
- **Continuous Monitoring and Tamper Detection**: The inclusion of continuous monitoring helps to detect unauthorized changes to credentials over time, which is particularly important in high-security environments like banking or government transactions.
- **Balancing Privacy and Security**: FAL 3 also balances privacy by allowing users to control what attributes are shared and when, which enhances both security and user satisfaction.

Conclusion:

The proposed updates in NIST SP 800-63-4 represent a forward-thinking approach to secure digital identity management. However, specific areas can be enhanced through standardization, particularly regarding the communication of authentication methods via FAL 3, the support for IAL 2 and IAL 3 in platforms like Login.gov and ID.me, and the management of privileged accounts using PR-MFA and PAM tools. By addressing these areas, the draft will better align with the security needs of federal, state, local, and tribal agencies while promoting a secure, interoperable, and scalable digital identity framework.

Failure to adequately address these areas could expose agencies to evolving security risks, while comprehensive adoption will position them to safeguard sensitive systems more effectively.

Submitted by:
John M. Willis, Chief Risk Officer, Turnaround Security
[redacted]
TurnaroundSecurity.com