Sandy Kronenberg
[redacted]
Jan 4, 2026, 4:46:44 PM
to 800-171comments@list.nist.gov

Dear Ron Ross and Victoria Pillitteri,
I hope this message finds you well. I am writing to provide feedback on NIST SP 800-172 Revision 3, specifically Section 03.11.03E, in the context of emerging threat vectors that operate at what is often referred to as the “human layer” or “Layer 8” of the OSI model.

First, I would like to acknowledge the continued leadership that you and your colleagues at NIST have shown in advancing cybersecurity guidance to address increasingly sophisticated adversaries. The emphasis in SP 800-172 on deception, misrepresentation, and advanced persistent threats is both timely and necessary.

That said, upon reviewing Section 03.11.03E, I am concerned that the current language does not sufficiently address human-targeted disinformation, AI-enhanced social engineering, and real-time impersonation attacks that occur through modern collaboration and communications platforms (e.g., voice and video conferencing, mobile calls, text messages, etc). These attacks frequently bypass traditional technical controls—such as MFA, encryption, and network monitoring—by exploiting human trust rather than system vulnerabilities.

While SP 800-172 appropriately assumes that users and credentials may be compromised, the control set largely continues to focus on system-centric detection and response mechanisms. In practice, adversaries are increasingly leveraging AI-generated voice, video, and contextual impersonation to convincingly misrepresent trusted individuals (e.g., executives, program managers, government officials) in live interactions. These attacks are difficult or impossible to mitigate through training alone and are not adequately addressed by existing controls that stop at authentication or session establishment.

Importantly, new classes of security tooling are now available that can provide real-time verification of communication authenticity, detect impersonation attempts, and surface indicators of AI-driven deception during live interactions. These capabilities represent a meaningful advancement in defensive posture and align directly with the stated objectives of SP 800-172: namely, resilience against sophisticated, deception-based threats that operate under adversarial conditions.

I respectfully suggest that Section 03.11.03E (or related enhanced requirements) be expanded to explicitly acknowledge and encourage the use of technical controls that address human-layer risk, including but not limited to:

- Detection of impersonation or misrepresentation during live communications
- Verification of speaker or participant authenticity beyond credential-based access
- Technical safeguards that operate independently of user judgment or training

Such clarification would help ensure that the control intent keeps pace with the threat landscape and provides clearer guidance to agencies, assessors, and solution providers evaluating compliance in environments where human deception is the primary attack vector.

Thank you for your continued work on behalf of the cybersecurity community. I appreciate your consideration of this feedback and would welcome any opportunity to discuss these observations further.

Respectfully,
Sandy Kronenberg
CEO - Netarx LLC
[redacted]