NIST Releases Guidelines for Alternate Secure ID Verification

The newly released guidelines aim to uphold government cybersecurity amidst the COVID-19 pandemic.

Adam Patterson
Wed, 08/05/2020 - 14:41

National Institutes of Standards and Technology's new guidelines for granting secure verification to government workers who manage protected information will allow federal employees who work with classified data to be granted access more easily amid the COVID-19 pandemic.
The publication of the NIST SP 800-63B Digital Identity Guidelines follows an ongoing effort across security-focused wings of the government to adapt around social-distancing guidelines while still allowing classified work to safely continue across federal IT networks.

One of the main challenges federal agencies have needed to overcome while allowing secure access to government networks has been the inability to conduct in-person identity verification.

“The challenge across the federal government in onboarding personnel under the FIPS 201 verification or PIV PROGRAM is that they require in-person identity proofing processes. And clearly this is precluded amidst the pandemic,” said David Temosh, senior advisor at NIST, during the Navigating the NIST SP 800-63B Digital Identity Guidelines forum last week.

The current impasse rests on reconciling the need for epidemiological safety with the technical security mandates. As a consequence, NIST and its partner agencies have developed newfound methods for remote verification that do not risk the further spread of COVID-19.

“We’ve needed to move toward credentialing and onboarding personnel using remote processes, but allowing for alternative credentials to the PIV card,” Temosh said. “We don’t want to lower security on the PIV card or reduce any of the binding processes to those cards, but some identity verification cards use biometrics — which means we need to perform in-person biometric collection. Which right now we have to put on hold.”

The newly developed solution has taken the form of a holdover system of remote verification that can allow a certain degree of access throughout the duration of the pandemic.

“So this has enabled agencies to onboard personnel using alternative non-PIV credentials until such time facilities can be opened and we can begin secure sessions to allow the actual intake process we use for onboarding,” Temosh said.
Other secure-focused agencies who work closely with NIST have begun implementing similar measures, using temporary forms of remote ID verification and onboarding before resuming in-person authentication once the pandemic ends.

"At CISA we issued a memo and came up with a series of processes for deriving alternative credentials for onboarding new hires," said Rob Foard, IT specialist at CISA. "We can’t do in-person capabilities, so we do remote capabilities. So they’re issued a card that’s not a PIV card, but has the strength of authentication that the PIV does. And when we end this period we’ll complete the HSPD1 requirements and other requirements more fully and have PIV cards issued to these individuals."

The COVID-19 responsive verification standards developed within NIST and CISA are also being deployed across the federal government as a whole, with CISA currently managing a knowledge-sharing program with partner agencies.

"CISA has been involved in pandemic response beyond identity management. We have a robust team of cybersecurity professionals advising agencies on whatever risks they may be encountering, and there definitely are new risks as we’ve been teleworking. And CISA has been helping agencies attack those risks,” Foard said.

Going forward, NIST also seems focused on creating a long-term response to the upsurge in federal remote work — including ongoing verification processes for employees who work permanently off site.

“Along with the PIV credentials, we’ve been tasked with further broadening the scope and allowing federal credentials and federal authentication processes to be enabled through additional types of authenticators for federal employees. This remote work environment has created acute demand for this kind of expanded capability, which we are building into our guidelines,” Temosh said.