5 Ways to Prioritize Identity Security with the Technology Modernization Fund

By Bill O'Neill

In its first half year, the Biden administration has hit the ground running on not only vaccine distribution and financial relief plans for citizens, but also on cybersecurity policy and information technology funding.

Recognizing the connection between modernized IT systems and cybersecurity, the President included a $1 billion infusion into the Technology Modernization Fund (TMF). The TMF, authorized by the Modernizing Government Technology Act of 2017, had only been given an initial $175 million from Congress to move government IT and security projects forward.

This concern was further amplified by the recent executive order outlining a number of identity and access controls aimed at modernizing the nation's cybersecurity. The ongoing impact of the SolarWinds attack is a constant reminder of the need to significantly improve privileged access rights and prevent attackers from mounting large-scale, deep targeting of federal agencies.

The message is clear: agencies now have no excuse to not address their outdated, insecure networks.

A major contributing factor to this modernization push is that the threat has outgrown the government's approach to privileged access management (PAM). Privileged access abuse is the leading cause of breaches: 80% of all data breaches involve privileged access credentials, according to Forrester.

Modern threats require modern solutions to solve them and mitigate risk, and that means a cloud-ready approach based on Zero Trust principles to protect against access abuse in today's dynamic threat landscape is needed. Organizations that are looking to secure access to infrastructure, DevOps, cloud, containers, big data, and other modern use cases can work to address these issues via the TMF.

To do so, they should consider five key functional priorities:

- Privileged access management (PAM)
- Multi-factor authentication (MFA)
- Privilege elevation and delegation management (PEDM)
- Password vaulting
- Secure remote access for administrators including third-parties

Government organizations should look to the TMF as a catalyst to potentially fast track improvements to their cybersecurity strategies. ThycoticCentrify can help address the root causes of privileged access abuse, and put them in a much stronger position to resist cyberattacks currently challenging the integrity of vital state and federal government infrastructure.