ATARC

WHITE PAPER

Overcoming Identity Challenges to Meet the Federal Government's Zero Trust Memo

Summary of Roundtable, hosted by ATARC in May 2022

The Advanced Technology Academic Research Center (ATARC) recently hosted a roundtable discussion on the Federal Government's efforts to mandate Zero Trust system architecture. President Biden's Executive Order #14028, Improving the Nation's Cybersecurity, directed government agencies to strengthen their security posture against an ever-increasing number of cyber threats, and cited Zero Trust as the solution.

"Never Trust, Always Verify"

Zero Trust Core Concepts:

- No user or device is trusted
- Preventative security measures (MFA, passwordless, etc.)
- Real-time, responsive monitoring

This January, the Office of Management and Budget took things a step further, releasing M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, including guidelines focused on identity. During the discussion, government IT experts shared their reactions to M-22-09 and spoke candidly about the implementation challenges M-22-09 and how to overcome them.

Progress and Challenges

The use of AI in medicine has the potential to improve military service readiness, service member population health, as well as save time and resources. AI has the potential to be a transformative technology in military medicine with numerous applications Participants repeatedly stressed what a significant step forward M-22-09 was throughout the discussion. While some participants said they had been working on Zero Trust initiatives within their agencies for years, not all government agencies are as far along or have started at all. As a result, the level of protection against cyberattacks is uneven across the Federal Government.

PIV and CAC cards are perfect examples. Unlike EO 12048, Federal guidance on PIV and CAC didn't include any mandate that government agencies adopt it by a specific time. Participants added that some small agencies haven't even issued PIV cards to their employees six years later.

There's also the issue of scale. Ironically, smaller agencies that largely bypassed PIV are probably the easiest to transition because fewer cards are issued. But PIV doesn't scale well, and for public-facing agencies, it's not feasible to give a PIV card to every constituent they encounter. Thus, another solution is necessary, one that works both inside and outside the Federal Government and ensures that all agencies have a consistent level of protection.

PIV and CAC: A Government 'Cul-de-sac'?

While the guidance calls PIV "the simplest way to support phishing-resistant multi factor authentication (MFA) requirements," participants spoke frankly about the use of PIV in the Federal Government and its issues. They agreed that the use of PIV and CAC is not the best solution for meeting Zero Trust guidance. While at one time regarded as one of the best ways to provide certainty of identity, adoption never took off outside of larger enterprises. Most PIV usage in the U.S. today is limited to government use.

PIV cards seem dated, even more so given the pace of innovation. Since OMB M-16-11 and M-17-12, the industry has largely moved past hardware-based authentication.

The use of one-time-passcodes and X.509 cryptographic credentials are common. The COVID-19 pandemic accelerated remote work while dramatically increasing the bring your own device (BYOD) approach.

PIV and other hardware-based credentials have low adoption rates and lack mobile compatibility. One participant compared it to a cul-de-sac since the government is the primary adopter of the technology, leaving it isolated. This creates issues when working with external stakeholders. While some agencies are trying to expand PIV card usage beyond their walls (mostly out of necessity), others haven't even issued cards to their own employees. Some agencies can't use PIV cards for various reasons, such as the sensitivity of the networks accessed or other unavoidable roadblocks.

Then there's the issue of familiarity with hardware-based authenticators. Most stakeholders have no experience with PIV or CAC, so training is required. Hardware-based authenticators also create friction during the authentication process, which studies have shown harms overall adoption.

With software-based solutions now as secure as PIV cards (and development underway for government-ready authenticators), most participants agreed there's little reason for the government to continue using PIV cards, even if it is the "simplest way."

Overcoming Identity Challenges

Participants focused on the specific challenges and possible solutions for each of M-22-09's three identity goals for the remainder of the roundtable.

Centralized Identity Management Systems

Employing centralized identity management allows for easier control and visibility of user activities. It is crucial to clearly understand who, what, and where data is being accessed with Zero Trust.

However, participants noted that deploying centralized identity management at scale is challenging. But that's not the only concern. Some government systems are dated, running in some cases outdated software that was built long before PIV cards, one-time passcodes, and MFA. It might not be possible to bring these systems up to par with the guidelines.

The Government's Three Identity Goals in M-22-09

- ❖ Employ centralized identity management systems
- ❖ Implement phishing-resistant MFA
- ❖ Transition from role-based (RBAC) to attribute-based access control (ABAC) using device level signals

Participants recommended that agencies beware of "shiny new object" syndrome and take a cautious approach in adopting centralized identity management instead. One solution isn't going to solve every issue, and careful planning is necessary. Agencies will also need to be sure the solution(s) they choose are interoperable, one participant added.

First, agencies should identify all potential stakeholders, and then proceed to identify any potential challenges in implementation. While some agencies will transition easily, others may have issues due to aging systems, sensitivity, or other unavoidable issues.

Participants also recommended that agencies do a complete "inventory" of their technology. There may be incompatibilities in long-outdated forgotten hardware, which could cause significant issues during the transition.

With these challenges in mind and network infrastructure fully mapped out, agencies should look for software solutions that address those challenges directly. Participants agreed that starting with a solution and then trying to make it work is the wrong way to go about it and will make an already challenging transition that much more difficult.

Phishing-Resistant MFA

Implementing phishing-resistant MFA is a vital part of transitioning to Zero Trust. While MFA is widely used among governmental and non-governmental entities, not all techniques are phishing resistant. PIV cards are, but they aren't well supported outside of the government or on mobile devices – the latter a significant issue in the age of BYOD.

While some participants voiced concerns over losing PIV as the de-facto standard among Government agencies, others pointed out that the industry had caught up to PIV with standards like Fast ID Online (FIDO) which is also better at addressing compatibility and adoption issues.

There was general agreement that agencies should look outside of PIV and CAC to implement phishing-resistant MFA. A host of software-based solutions exist that are far easier to deploy at scale and are Zero Trust-ready and may also help you meet other parts of the Zero Trust directive, including attribute-based access control (ABAC), likely the most challenging directive to complete.

Attribute-Based Access Control

Role-based access control (RBAC) is how organizations have secured their networks for decades. Each user is assigned a "role," which has certain access privileges. While these are extraordinarily easy to set up, they are also very easy to exploit.

An attack could be devastating with the proper credentials and the right role. Therefore, OMB is directing agencies to transition to attribute-based access control (ABAC). ABAC is challenging to plan and deploy, with many participants voicing concerns over whether such a transition makes sense for their agency and the amount of work involved.

Agencies will need to put thought into their policies much more than RBAC. Factors such as login time and location, the security posture of their device, what the user is accessing, and changes to a security posture during the session, are all considered with ABAC, and requires a deep understanding of both the user base and network.

Participants agreed that transitioning to ABAC will be difficult, with some concerned about the complexity. Government agencies can't rip out RBAC from existing applications and networks (although some agencies haven't even implemented RBAC, which like PIV was never mandated).

Participants urged agencies to take the transition to ABAC slowly and in parts to ensure it doesn't create more problems than it solves. Participants generally agreed that moving to ABAC was a good thing: it forces all government agencies to take a hard look at their authentication systems, security policies, and overall security posture.

Zero Trust Isn't One and Done

Adopting Zero Trust across the Federal Government will not be easy and will take all the time allotted by the guidance to implement. Some participants pointed to the eventual need for additional staffing for the day-to-day operations of these new systems. Others noted that it's another thing for agencies to juggle with cloud and IT modernization efforts already underway.

Regardless of the challenges ahead, Zero Trust is an ongoing and permanent change in how agencies handle their data and authentication, and it won't have a finite endpoint like many government efforts. While the deadlines to come into compliance are fast approaching, there is more than enough time for agencies to take the necessary time to both understand, plan, and deploy Zero Trust-compliant solutions.

Most importantly, agencies shouldn't go at it alone. This is a government-wide effort: everyone's working towards the same goal. Participants all agreed that cross-communication between agencies would make the transition easier.

Contact us today to learn more and get involved in ATARC's Cybersecurity and Identity Management Working Groups!