WHITE PAPER

Navigating the Department of Defense Mandate on Zero Trust

AXIOMATICS
a LEONARDO company

Introduction

In a recent article, David McKeown, who serves as the Department of Defense's (DoD) deputy chief information officer and department's senior information security officer said the department is on track to implement its Zero Trust framework by fiscal year 2027 as planned. The framework was originally released last November and it tasked each service to develop its action plan.

He went on to say that: "We've been partnering very heavily with commercial cloud providers, asking them to analyze their offerings, partner with other service provers to try to achieve those 91 capabilities to get us to the target of Zero Trust."

But what does that mean for contractors and agencies looking to implement Zero Trust? And is it possible for the DoD to have a Zero Trust cybersecurity framework implemented by 2027?

What is Zero Trust as the government defines it?

In determining how to proceed and best practices to adhere to a 2027 deadline, the DoD looks to the gold standard for technology planning and implementation - the National Institute of Standards and Technology (NIST). Per their website, NIST views Zero Trust as a framework where "there is no implicit trust granted to assets or user accounts based solely on their physical or network locations (i.e. local area networks versus the internet) or based on asset ownership (enterprise or personally owned)[1].

Because the NIST definition of Zero Trust stretches from individual data through to the network, cybersecurity vendors often add additional color on specific areas, including identity and access management (IAM). As the majority of cybersecurity vendors offer insight on Zero Trust, cutting through the "noise" to identify the right and most pragmatic approach becomes difficult for any enterprise, including federal agencies. This results in agencies being at a variety of different stages in terms of meeting the 2027 deadline.

Where is the government currently at with Zero Trust implementation?

The government has always had a stigma for being a bit behind when it comes to technology. They have been using Federal Public Key Infrastructure (FPKI) and Personal Identity Verification (PIV) credentials as a way of authentication for over 15 years, but some agencies have not adapted or moved along with other technologies as have other highly-regulated industries.

In reality, agencies that are still talking about networks, perimeter security and firewalls are likely already pretty exposed, from a risk standpoint. When looking at the concept of a secure network and the speed that information is available now; it has outpaced the legacy security principles and architecture still in place in many agencies. This is a really bad place to be in terms of security.

1. NIST Zero Trust Architecture
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

For more than a decade, the different federal agencies have been urged to use Zero Trust risk-based principles in their security. Concurrently, these same agencies have also been challenged to update their application development, taking advantage of cloud-native development as a more efficient and cost-effective means of modernizing infrastructure and operations.

Each agency's approach to access control also requires modernization, which includes the need for an efficient, scalable and dynamic approach to authorization. Per the NIST framework, this can be achieved by implementing attribute-based access control, or ABAC. The who, what, where, when and why attributes are essential to ABAC and to Zero Trust.

Through ABAC, a Zero Trust implementation leverages these types of attributes (and others) to ensure the appropriate level of access is given in line with the amount of risk an organization is comfortable with.

Role-based access control (RBAC) and Identity Governance and Administration (IGA)

One of the most common things we hear from clients is how they have invested in role-based access control (RBAC), often through their Identity Governance and Administration (IGA) solutions. Audits and a successful approach to Zero Trust require an agency to look beyond the roles. Roles can be a good start, but you need to consider additional attributes which may include location, security clearance level, and more.

There is a lot of risk when it comes to various clearances in the government. The Director of National Intelligence report on Security Clearance Determinations has estimated that more than 1.25 million people have top-secret clearance. New estimates put that figure closer to 1.3 million people.

John Brennan, who served as the Central Intelligence Agency (CIA) director during the Obama administration, has said that people should only have access to information "they need to do their job." RBAC

is an important first step in achieving this goal, but does not provide a full picture of access and can subject an agency to additional challenges, including role explosion.

As discussed in our article on recertification, if ABAC is utilized it can make sure that the right people are accessing the right information at the correct point of access, each time, based on the attributes collected at that exact point in time, enabling them to do their job and nothing more. This helps mitigate the risk associated with people having more access than they should to complete their job.

How does the cloud come into play?

Zero Trust and the cloud are two separate things.

When you are replacing old hardware servers with cloud-based servers it means that they are no longer static. They have different granular components, but face the same amount of vulnerabilities as their hardware counterparts.

Though all organizations are vulnerable to individual hackers, cyberterrorists, and even state-sanctioned cyber attack, it is a particular pain point for government agencies. Looking back to as recently as February 2023, there were internal US military emails which contained information on special operations that were exposed to anyone with internet access. Even though there was no evidence that these emails were hacked it does highlight the importance of securing critical agency servers no matter where they reside.

How does the cloud come into play?

This is where a Zero Trust framework can come into play as it requires organizations to segment their networks and set up various policies depending on the accessed data to secure it. In the end, this makes it more difficult for unauthorized individuals to slip through the authentication process and reduces pain points that may be associated with the network's security.

There are a lot of pieces that go into both of them, but they aren't always tied together. Once you migrate to the cloud and modernize your system it can be easier to have Zero Trust implemented.

What is the DoD asking for and what do contractors need to do to get to a Zero Trust framework?

There is a lot of confusion around what exactly the DoD is asking for from their contractors when it comes to implementing Zero Trust. Many contractors are already embarking on a Zero Trust implementation journey, but there are no guidelines, timelines or directions with regard to how these efforts must align with the DoD directive when it comes to their work with relevant agencies.

Everyone is trying to figure out the next steps in the process and because of that, agencies and contractors are at different levels of progress.

When it comes to Zero Trust, there is no one standard or solution. It is a framework and a reference architecture on how to apply modern security. That is why people are trying to figure out how to implement it and how much work will be involved in the process especially when it comes to something at this large of a scale.

What role do integrators play?

Integrators including NTT, Deloitte and others play an important role. The DoD understands they don't have the knowledge to implement this infrastructure on their own and that integrators, in their work with vendors across the cybersecurity stack, have a more advanced understanding of how to successfully implement a Zero Trust initiative based on a variety of criteria including (but not limited to) overall organizational maturity, environment, etc.

While some integrators have come up with the concept of "Zero Trust in a box" where they can go in and create the Zero Trust reference architecture using multiple components, other integrators have done this as a best practices recommendation. A variety of approaches enables DoD agencies to determine the right fit for them based on where they are in their Zero Trust journey.

A word from NTT DATA

A statement from Washington Exec and CTO for NTT DATA Federal, Nat Bongiovanni

"NTT DATA Federal is a long time partner of Axiomatics. Together we created an attribute-based access control (ABAC) that can be easily demonstrated to our clients and potential clients. NTT DATA Federal invests in innovation, our research team saw the potential for efficiencies and improvements that fine grain access control could bring to our clients.

By limiting the most restrictive policies and creating policy as code to allow for flexible access control architecture, efficiencies would follow.

We chose Axiomatics as a partner because they had superior technology. Axiomatics compliance with the industry standard extensible access control markup language (XACML) is critical to the success of our joint solution. Axiomatics inclusion of abbreviated language for authorization (ALFA) that was easier to manage and implement solidified our partnership. We can use existing code management tools (Bitbucket, GitHub, etc.) for managing the versions of access control policies. Essentially giving us access control as code.

With Axiomatics, we have enjoyed a partnership in every sense of the word. We work closely with their stellar technical team to develop client-centered solutions and find mutually beneficial opportunities for growth. We are very pleased with our partnership and the opportunities we have gained in the past eight years."

We chose Axiomatics as a partner because they had superior technology. We can use existing code management tools for managing the versions of access control policies. Essentially giving us access control as code.

- Nat Bongiovanni, NTT DATA Federal

Is it realistic to implement Zero Trust by 2027?

There is no such thing as a silver bullet when it comes to Zero Trust.

There is a mass amount of elements that all come into play and it is not easy or always practical to have them tied into Zero Trust. An example of this is the journey that the DoD has to take to adopt or integrate Zero Trust capabilities, technologies, solutions and processes across their architectures and systems. It also means that the DoD must address the Zero Trust requirements within their staff and professional development process.

It's rare for a Zero Trust implementation to be successfully deployed at this level; the DoD rollout will go out to over four million people. This means there is no guide or example of how they can implement the strategy at this scale, but will set an example for the future.

What if your agency does not implement Zero Trust by 2027?

As of June 2023 there are broad guidelines without any consequences that have been outlined by the department on implementing Zero Trust. This gives the sense that they are at the early stages of planning as there is no specific plan or urgency. It also is allowing people to get educated and learn about what Zero Trust infrastructure is.

In addition to the lack of consequences, the DoD takes a long time to agree on and implement different strategies, and things are changing at a rapid pace in the cybersecurity industry. This means that as we advance and introduce new tools and solutions, the government keeps falling further behind.

Setting a standard in Zero Trust

As a part of our advancements we also have to consider the standards that we set. It is important to plan out and actively move forward with implementing something that is correct first as others will then jump onto that idea.

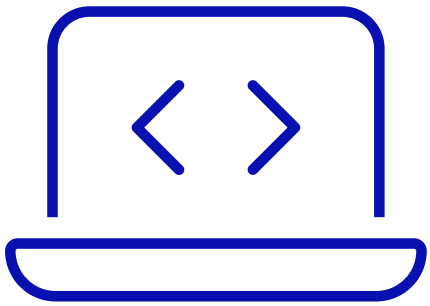
If we are always trying to come up with the next big thing that can slow down the speed that we can advance at because there are no standards that have been agreed upon which makes the solution less implementable. However, a good starting point already exists in NIST's Zero Trust Architecture document, which walks through the areas organizations can focus on when it comes to Zero Trust as well as what technologies should be prioritized for deployment.

It is possible to have a Zero Trust framework by 2027, but it will take a massive amount of work and people coming together to create standards on how to implement Zero Trust at that large of a scale. It can also be important to note that you can have a Zero Trust network, but that still doesn't mean you implemented Zero Trust principles.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240