

Policy Analysis Paper 2: The Political Implications of ZTA

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE425W: Cybersecurity Strategy and Policy

Dr. Hamza Demirel

February 22, 2026

Introduction

Zero Trust Architecture (ZTA) has become one of the most important cybersecurity strategies used by the United States government. Recently, there has been a global push for ZTA as countries in Europe and Asia are adopting it. In my previous policy analysis paper, I explained what ZTA is, its upbringing, and how it can work in today's society. However, ZTA is more than just a technical framework. Implementing it to our current security models comes with major consequences. This paper will explain the political implications of ZTA, how and why policymakers have approached the policy, and the ramifications of their decisions.

Political implications

With the previous perimeter based security model, organizations mainly focused on protecting the outside of their networks. Once someone was inside the system, they were trusted automatically. However, as time progressed, recent cyber threats became more advanced and political leaders began to treat cybersecurity as a national security issue rather than just an IT problem. According to a journal by Tigranovich, "Cybersecurity threats are one of the main national security, public safety, and economic challenges every nation faces in the XXI century" (Tigranovich, 2017) . When cybersecurity is looked at as a national security issue, it allows policymakers to justify the involvement of the government and their spending. To mitigate these issues, ZTA as a strategy has been acknowledged by organizations and governments around the world as a potential solution. Research also supports why zero trust has taken over in settings involving more classified information. In the article "Zero Trust Architecture: A Systematic Literature Review", the authors state that traditional perimeter based security models (PBSM) would no longer work effectively in an environment relying on cloud computing and bring your own device (BYOD) policies. Because federal organizations work with sensitive government

information, policymakers saw zero trust as a stronger, modern approach. (Gambo & Almulhem, 2025).

The approach of policy makers (and why they came to those conclusions)

The political implications of Zero Trust Architecture would suggest why policy makers chose to adopt it at the federal level. With many infamous cyberattacks on the United States government, policy makers and politicians would be faced with strong pressure to respond. For example, the 2010 SolarWinds attack that targeted internal government networks and the Office of Personnel Management data breach could have been mitigated if zero trust were widely implemented. These incidents exposed weaknesses in the country's cybersecurity systems and showed that PBSM would do no good against modern attacks. As a result, a major change in our security strategy was needed.

In 2021, previous President Biden and the executive branch emphasized the need for stronger cybersecurity defenses. To satisfy this objective, they mandated Executive Order 14028. According to the U.S. General Services Administration (GSA), the order suggests a "significant shift in how the US federal government approaches cybersecurity. A key pillar of this initiative is the adoption of a Zero Trust security mode" (GSA, 2021). The GSA explains that this process will be complex and lengthy. That they would rather have a proactive solution rather than a reactive one. This means that instead of waiting for the next cyberattack to occur, they wanted to completely refresh the structure of their security model to conform to upcoming attacks.

Biden set the tone for the future of U.S. cybersecurity standards. The Office of Management and Budget (OMB) was the organization responsible for enforcing Biden's executive order. As a policy maker, OMB issued Memorandum M-22-09 which set forth a Federal ZTA strategy. In the memorandum, they require all agencies to "meet the specific

cybersecurity standards and objectives by the end of the Fiscal Year 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns" (OMB, 2022). Through setting deadlines for agencies to adopt zero trust, OMB strengthened the critical infrastructure of the U.S. by making it a mandatory requirement.

After Biden's term ended, the evolution of the zero trust policy did not stop with the federal strategy. Under the current Trump administration, many cybersecurity leaders came up with what they refer to as "Zero Trust 2.0". While the first version emphasizes on setting standards across federal agencies, the second version focuses on efficiency and rationalization (Doubleday, 2025). Although Trump has not issued an executive order regarding Zero Trust 2.0 yet, he wants to make sure that investments made in future cybersecurity strategies will produce clear security improvements. Nick Polk, the branch directory for federal cybersecurity at the OMB stated, "We want to make sure that when we are making an investment, the investment is rationalized" (Federal News Network, 2025).

The ramifications

With Biden's Executive Order 14028 and OMB's Memorandum M-22-09, the path was paved for the private sector. Although the order was initially meant for federal agencies, it also mentions to "lead by example" (EO14028). As federal agencies push toward improving their security frameworks with ZT principles, private businesses and companies will adapt to the ever changing environment and do the same. As mentioned earlier, the Zero Trust 2.0 model is still in development, however, when it comes to fruition, the Trump administration promises efficiency and lasting results. All these policies indicate that ZT will be a long-term cybersecurity strategy.

References

- Doubleday, J. (2025, July 16). *Trump admin focuses on “zero trust 2.0,” cybersecurity efficiencies*. Federal News Network - Helping Feds Meet Their Mission.; Federal News Network.
<https://federalnewsnetwork.com/cybersecurity/2025/07/trump-admin-focuses-on-zero-trust-2-0-cybersecurity-efficiencies/>
- Executive Office of the President. (2021, May 17). *Improving the Nation’s Cybersecurity*. Federal Register.
<https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nation-s-cybersecurity>
- Gambo, M., & Almulhem, A. (2025). *Zero Trust Architecture: A Systematic Literature Review*.
<https://arxiv.org/pdf/2503.11659>
- Tigranovich, T. (2017, February 17). *The role of cybersecurity in world politics*. Cyberleninka.ru.
<https://cyberleninka.ru/article/n/the-role-of-cybersecurity-in-world-politics/viewer>
- Young, S. (2022). *EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM*.
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
- Zero Trust and Improving the Nation’s Cybersecurity | IT Vendor Management Office*. (2021). Gsa.gov. <https://itvmo.gsa.gov/news/zero-trust/>