SANS

Analyst Program

White Paper

# Looking Ahead to the National Cybersecurity Strategy Implementation Plan

Written by **Matt Bromiley**

November 2023

carahsoft. infoblox. SailPoint. VERITAS

# Introduction

We live in an era of escalating cyber threats and an ever-changing cyber threat landscape. Adversaries continue to hone their capabilities daily while many agencies and organizations struggle to keep up. For many years, public sector cyber defenses have lagged behind adversary capabilities. Fortunately, the executive branch of the US government has taken bold steps to provide guidance and a path forward to increase the resiliency of US cyber networks.

With the issuance of Executive Order 14028[1] (EO 14028) in 2021 and the National Cybersecurity Strategy[2] (NCS) in March 2023, we are approaching a new era of cyber defense. Agencies must challenge traditional cybersecurity models because the new landscape demands adaptive and proactive measures. EO 14028 recognizes that "[i]ncremental improvements will not give us the security we need." These initiatives also safeguard our digital infrastructure, providing a helpful road map for building and maintaining cyber-resilience.

Both EO 14028 and NCS confirm the executive branch recognizes that cyber defense is a top priority. Among the various strategies within each, we identified common principles that contribute to an ideal state. We also identified technology implementations that will be important for adhering to these principles. Three core technologies found within these initiatives are:

- Zero trust
- Identity management
- Attack surface management

In this whitepaper, we will focus on these technologies and analyze how each contributes to a resilient cybersecurity strategy in line with objectives set forth by the executive branch. The zero trust approach challenges the conventional wisdom of "once trusted, always trusted." Trust is not static but rather an ever-evolving state.

Identity management and attack surface management principles work with zero trust principles, ensuring only authorized users can access systems—thereby reducing threats by minimizing the digital footprint. The future of cybersecurity requires a collective, holistic approach—continuously adapting to deter adversaries' best-laid plans. As you work through this paper, we encourage you to consider:

- What requirements or objectives impact your network(s)?
- Where are you in the process of incorporating these principles or strategies?
- What is your timeframe for security posture improvements, and how do you prepare?

Finally, this paper focuses on three key takeaways from recent executive branch initiatives. It is not conclusive in *defining* a robust security posture. We focused on three critical technologies that *enable* robust security postures. You must consider the threats targeting your organization and your current technology stack and use those to guide and hone your security posture in alignment with the required policies and legislation.

[1] "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

[2] "National Cybersecurity Strategy," March 2023, www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

# A New Approach to National Cybersecurity

In this paper, we look to guidance from the executive branch on the future of cybersecurity policies and implementations. Both EO 14028 and the National Cybersecurity Strategy of March 2023 have essential principles and objectives that will collectively shape the nation's cybersecurity posture:

## Unified Vision for Resilience

- Both documents emphasize the adoption of zero trust, highlighting the need for continuous verification and the dynamic nature of trust.
- Government agencies must collaborate with private sector entities and international partners to share threat intelligence and strengthen defenses.
- Commitments to modernize cybersecurity practices and leverage innovative technology are essential.

## Critical Infrastructure Protection

- Both documents recognize the significance of protecting critical infrastructure—such as energy, transportation, and healthcare—against threats.
- Supply chain security is also a shared priority, aiming to secure software and hardware components.

## Workforce Development

- A skilled workforce will be necessary to meet the growing demand within cybersecurity, including currently unmet requirements.
- Technology implementations also require skilled teams to foster and hone them, adding to the need for a skilled cybersecurity workforce.

## Threat Sharing

- Sharing of threat details and indicators will be essential in detecting and responding to active cyber threats.
- The federal government recognizes that partnerships between private and public sectors—as well as sharing between IT and OT service providers—will remove existing barriers and accelerate incident deterrence.

These principles, and many more, reflect a comprehensive and integrated approach for cybersecurity. Fundamental ideals of trust, collaboration, innovation, and resilience set the foundations we analyzed. We settled on three technology implementations or strategies to help organizations get on the right path to enhance their cybersecurity posture and protect their digital assets.

# Zero Trust

Zero trust is a concept that resonates through many organizations, but it is not merely a buzzword. Referenced directly in EO 14028, zero trust is a paradigm shift for many that recognizes the evolving threat landscape and the need for a more proactive security stance. Organizations can no longer rely on the model of perimeter-based defenses. Zero trust puts this challenge to the test, instead insisting on the “Never trust, always verify” mindset.

Fundamental principles of zero trust include but are not limited to:

- **Continuous verification—**In zero trust architecture, trust is never assumed based on a request’s location or source. All interactions with systems, services, applications, and the like are subject to rigorous verification, regardless of the source.
- **Least privilege access—**Access privileges are granted on a strict need-to-know or need-to-have basis. Users and devices are given the minimum access required to perform their task(s).
- **Micro-segmentation—**Networks are segmented into smaller, isolated zones. This proactive containment strategy limits where accounts can move between networks or systems (e.g., lateral movement).
- **Strict identity verification—**Identity verification is a cornerstone of a solid zero trust implementation. Strong identity and access management practices ensure that only authorized devices and individuals access the *right* resources.

> **The “castle-and-moat” approach of *strengthening the perimeter* is no longer sufficient against modern adversaries and evolved threats. Zero trust acknowledges that the perimeter is becoming obsolete, especially in modern networks.**

Zero trust’s fundamental principles and proactive posturing stem directly from threat actors’ techniques and tactics. For years, networks were built using the “castle-and-moat” approach, which relied heavily on perimeter defenses to protect an internal core network. However, cyber threats evolved, and attackers found that once *inside* the perimeter, they had free reign.

For example, consider the principle of micro-segmentation, which breaks networks into highly isolated zones to limit lateral movement. Moving between systems is not inherently malicious. However, when threat actors abuse accounts, it can result in damaging attacks. Thus, micro-segmentation not only protects users but also limits adversaries. Zero trust acknowledges that the perimeter is no longer a reliable defense.

Zero trust is a strategy, not a set of tools. It can be a significant shift for some organizations, overhauling legacy processes for long-term prevention and mitigation. We encourage you to utilize public guides[3] and zero trust models to help determine the best path for implementation. One of the most valuable resources is the Zero Trust Maturity Model (ZTMM), designed by the Cybersecurity and Infrastructure Agency (CISA).[4]

[3] “SANS 2022 Report: Moving to a State of Zero Trust,” August 17, 2022, www.sans.org/white-papers/sans-2022-report-moving-to-a-state-of-zero-trust

[4] “Zero Trust Maturity Model,” April 2023, www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

The ZTMM, currently in version 2.0, provides a structured framework for organizations to evaluate their current level of zero trust maturity and develop a road map for future implementations. The ZTMM breaks down implementation concepts into five pillars, " in which minor advancements can be made over time toward optimization." Figure 1 provides a graphic of the ZTMM.

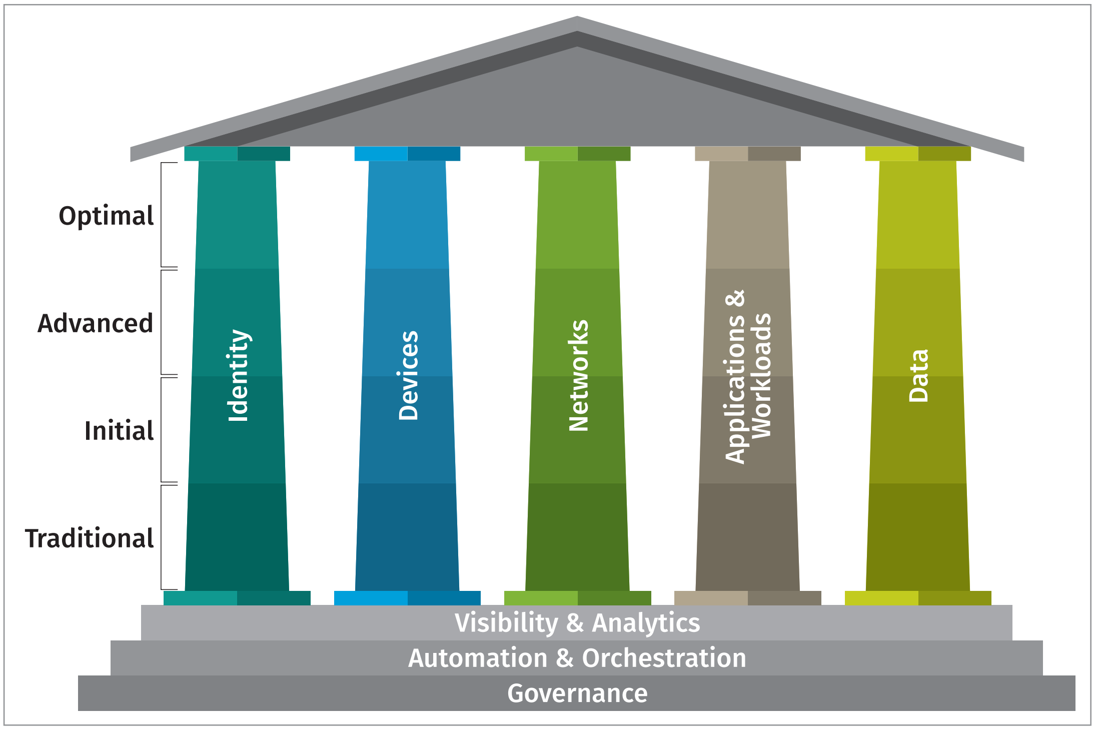

*Figure 1. The Five Pillars of Zero Trust Implementations and Evolutions, per ZTMM v2*

In its release of the ZTMM, CISA also recognizes that three capabilities are applicable to each pillar:

- Visibility and analytics
- Automation and orchestration
- Governance

This capability of "cross-cutting" recognizes that agencies will be relying on automated technologies that dynamically enforce policies. The ZTMM also realizes that each pillar will progress at its own speed, according to the agency's road map and implementation plan.

## Best Practices: Using the ZTMM for Zero Trust Assessment

Putting the ZTMM to work is worthwhile for any department seeking guidance on a zero trust implementation. Let's look at a step-by-step process of utilizing the ZTMM to map out a zero trust implementation:

### Step 1: Assessment

Perform a comprehensive assessment of your existing cybersecurity controls, network architecture, and access privileges. This also can include identifying all network assets, user identities, and access permissions.

### Step 2: Planning

Develop a zero trust road map, outlining clear objectives, milestones, and key performance indicators (KPIs) for measuring implementation progress. This also may be the phase where various tools and technologies are tested.

### Step 3: Implementation

With a chosen technology(ies) and process(es), implement zero trust principles across your network infrastructure. This includes strict enforcement of least privilege access, robust authentication, and network segmentation.

### Step 4: Monitoring

In addition to controls implemented by zero trust, we should also look to real-time monitoring and threat detection systems to continuously assess network activity.

### Step 5: Automation and Orchestration

Finally, to enhance response capabilities, look for opportunities to automate processes or workflows. With playbooks, integrated systems, and automated response actions, a security team can find efficiencies that maintain zero trust principles without requiring a long-term time sink.

By following the ZTMM framework, an agency can successfully implement a zero trust model in accordance with the wishes of the executive branch. This can reduce cyberattack risks and help protect national security information.

## Identity Management

A key element in any zero trust strategy is identity management. This is also a capability that took center stage in both EO 14028 and NCS as a fundamental component of modern cybersecurity strategies. Both documents recognize that establishing trust hinges on robust identity verification and continuous monitoring—directly in line with a zero trust approach.

EO 14028 calls on agencies and organizations to prioritize identity management by implementing strong authentication mechanisms such as multifactor authentication (MFA). Similarly, the NCS advocates for the adoption of rigorous identity management practices across the public and private sectors. By securing digital identities through continuous authentication and authorization processes, the strategy aims to increase cyber resiliency (a recurring theme through both documents).

The NCS takes things a step further, establishing "Development of a Digital Identity Ecosystem" as a strategic objective, highlighting the need for robust identity management. This objective goes beyond the "simple" requirements of cybersecurity and focuses on digital identity as a holistic approach for building a "more innovative, equitable, safe, and efficient digital economy." The NCS does recognize that identity theft and data breaches are on the rise, with nearly 300 million victims in 2021 and billions of dollars lost during the COVID-19 pandemic.

This objective highlights the need for robust and integrated identity management. Although this initiative moves beyond the needs of cybersecurity, it underlines the effort and resources the federal government is putting into building out these ecosystems. This gives agencies and organizations a chance to consider a holistic approach that *includes* cybersecurity risks, and it structures identity and access around them.

## Best Practices: Preventing a Data Breach with Identity Management

Consider a government agency responsible for handling sensitive citizen data, including Social Security numbers and financial records. This agency is trusted with safeguarding the data, and any data breach could have severe consequences. With a vast network of systems and databases, adversaries could use a large attack surface to exploit vulnerabilities. To help mitigate cyber threats, the agency implements an identity management solution.

### Key Steps of an Identity Management Implementation

- **User authentication—**Implementing MFA for all personnel and contractors, limiting access to sensitive systems. Government agencies typically also may require smart card or biometric authentication.
- **Role based access control (RBAC)—**Also sometimes referred to as identity governance, establishing RBAC policies limits user access to only information and systems necessary for their roles. This is in line with a zero trust implementation, as discussed earlier.
- **Continuous monitoring—**Tracking user activities and detecting anomalies in real time. Any suspicious behavior, such as an unusual access request or repeated failed login attempts, should trigger an alert for an investigation.
- **Privileged access management (PAM)—**PAM solutions can be integral for privileged users, such as administrators, who should be tightly controlled and monitored.
- **Audit trails—**Maintain detailed audit logs of all user activities and access attempts, providing a forensic trail for post-incident analysis.

> **We're still talking about MFA? It seems like MFA has been a suggestion or solution for years, despite still being vulnerable to various phishing and SMS spoofing attacks. However, we'll stand by the recommendation, because it can raise your adversarial "barrier to entry" and make it difficult for automated operations or other low-skilled adversaries who might rely on single-factor authentication.**

By implementing a comprehensive solution, like the one above, an agency can significantly reduce the risk(s) associated with a data breach. This includes:

- Unauthorized access is disrupted through MFA and RBAC controls.
- Continuous monitoring and real-time alerts allow for rapid detection before access abuse can get out of control.
- Privileged access is tightly controlled, limiting what internal users can get access to.
- In the event of a breach, audit logs provide necessary insight to determine the root cause and impacted data.

The aforementioned steps are not a conclusive security posture, but they help move the progress bar in the right direction for many organizations. Simple identity solutions, tools, and processes can go a long way to stop even skilled adversaries in their tracks.

# Software Supply Chain

In today's world, software plays such an integral role in operations but also provides a myriad of entry vectors for adversaries. As such, another core similarity between both EO 14028 and NCS is the highlighting of the importance of *securing the software supply chain*. Software applications and components are essential to the operation of critical systems across all levels of government, only underscoring the need for software supply chain security. Both documents focus specifically on securing the software supply chain, recognizing it as a necessary security function, a key component of critical infrastructure, and yet a simultaneous attack vector for adversaries.

At the time of its creation, Executive Order 14028 placed a distinct emphasis on securing the software supply chain. The EO highlights the potential risks associated with software components from various sources, identifying the risks they pose as vectors for malicious code execution and compromise. The executive order calls for a thorough assessment of the software supply chain, identifying and mitigating vulnerabilities swiftly.

The NCS builds upon this emphasis by recognizing that secure software supply chains are vital for ensuring the security of critical infrastructure and government agencies. It cannot be overstated that software supply chain risks have become a method of choice for many adversaries, and unknowing security teams are the last to know once they have been exploited. We'll look at a few key topics that both documents identify as critical needs for government agencies.

## An Avenue for Cyber Threats

Across both documents, there is a position that the software supply chain presents enormous opportunities for agencies and applications while simultaneously being a dangerous avenue for cyber threats. The software supply chain serves as a prominent vector for adversaries looking to exploit vulnerabilities. Threat actors have become well-versed in discovering and exploiting vulnerable software components, particular those from third parties. This can present a potential weak link in even the best-laid security plans.

EO 14028 specifically calls on vulnerabilities from third-party software and libraries, asking agencies to assess and secure their supply chains. Of course, this is often easier said than done. NCS continues the theme, focusing on the need to understand the role of software supply chains in critical infrastructure and federal agencies.

### SBOM

Within the concept of securing the software supply chain, the concept of a Software Bill of Materials (SBOM) is a cornerstone that is addressed in both EO 14028 and NCS. This approach seeks to promote transparency and accountability within the software supply chain, helping security teams identify vulnerabilities before they can be exploited. EO 14028 acknowledges the significance of SBOMs and even calls for the establishment of a baseline SBOM format and tools to enhance software products.

NCS continues this theme, amplifying that SBOMs are a means of ensuring the integrity of software components. The document further encourages collaboration between private and public sectors to develop and standardize SBOMs, again furthering the omnipresent “work together” theme.

### Secure Software Development

Another critical component with respect to software supply chain security is an emphasis on secure software development practices. Both documents advocate for better and secure development methodologies, capturing best practices as essential components of software supply chain security. This may include, but isn’t limited to:

- Integration of security considerations into the development process
- Adoption of coding standards
- The use of secure development tools to minimize vulnerability and assist in the forming of SBOMs (see above) to track software used across an agency
- Continuously testing software for threats and vulnerabilities, in addition to private sector reporting
- Minimizing of vulnerable code reuse or reliance on old, legacy libraries

Albeit brief, secure software development gets a reference from both documents as a technique to further strengthen the software supply chain.

## Best Practices: Securing Your Software Supply Chain

In response to the two documents our paper has centered on, an agency that is responsible for critical government functions must recognize the importance of securing its software supply chain. As always, the issue is how to deal with the broad spectrum of software components and dependencies supporting all of its various operations. Challenges include:

- **Software diversity—**Over the years, software has been procured from various sources, resulting in a complex, and often outdated, software supply chain.
- **Vulnerability risks—**Without a proper assessment, the agency doesn’t know what it doesn’t know. Are we currently vulnerable, and what is protecting us from compromise?
- **Data protection—**Given the sensitivity of agency data, a high level of protection against supply chain attacks and safeguarding data is a must, not a wish.

What practices can be implemented to mitigate risks and enhance the resiliency of the software supply chain?

- **SBOM—**Adopt an SBOM to gain transparency into software components, dependencies, and origins. This may require an extensive lift, but will pay off in dividends for years to come.
- **Vendor assessment—**Conduct rigorous assessments of third-party software vendors, evaluating security practices and ensuring that they are not introducing additional risks into your environment.
- **Patch management—**The security adage of "patch, patch, patch" can go a long way in preventing software supply chain attacks. It should be a priority, when possible, for any and every security team.
- **Secure development processes—**Integrate secure development practices, including secure coding, double or triple code review, and threat modeling, into the software development lifecycle.

The agency's goal is to gain increased transparency into what it *has*, to prepare for what it *will have* in the future. By focusing on simple steps and working towards a more secure software pipeline and lifecycle, the agency can move towards a much more resilient software supply chain.

## Closing Thoughts

Executive Order 14028 and the National Cybersecurity Strategy of March 2023 emphasize modernizing cybersecurity policies in response to the evolving threat landscape. Recognizing that the United States is responsible for protecting the data and infrastructure of its citizens, both directives realize that an equally comprehensive approach is required. Both initiatives call for the adoption of zero trust policies, where trust is never assumed and is continuously verified. This approach establishes that all interactions are subject to rigorous scrutiny, mitigating the risk of unauthorized access and lateral movement.

Similarly, we found advocacy for robust identity management as a cornerstone of a robust security posture. Not only an integral part of zero trust, identity management can also help mitigate key risks associated with user account theft and unauthorized access—one of the leading side effects of cyberattacks. Finally, attack surface management calls for the systemic profiling and reduction of an organization's attack surface. Organizations are better prepared to defend against modern cyber threats by identifying and mitigating vulnerabilities and securing supply chains.

These directives and their implied security improvements pave the way for organizations to navigate and combat modern cyber threats today and tomorrow. The fact that the executive branch recognizes that cyber threats aren't going away—setting the tone for improvement and using modern defenses—is a step in the right direction.

## Sponsors

**SANS would like to thank this paper's sponsors:**

carahsoft®

infoblox®

SailPoint®

VERITAS™