Forum for American Leadership

EINSTEIN Reauthorization: A Chance to Leap Ahead in Federal Network Security

July 7, 2022

There is broad recognition that federal network security is more than just a government IT issue, but rather something foundational to the personal privacy of Americans' sensitive information and national security. The federal government has learned this truism the hard way far too often—from the China-backed OPM breach that exposed sensitive information on over 20 million Americans to the Russia-backed SolarWinds cyber espionage campaign that resulted in exposure of incalculable amounts of non-public government data across nine agencies.

Federal civilian networks, which encompass those outside of the Department of Defense (DoD) and the Intelligence Community, represent a sprawling conglomeration of over 100 agencies' digital enterprises. While the Cybersecurity and Infrastructure Security Agency (CISA), the civilian operational lead for cybersecurity and OMB (interagency "referee") nominally sit at the middle of the so-called ".gov" space, centralized, real-time visibility has been a persistent challenge.

When discussing CISA's current offerings to support .gov security, two programs are frequently mentioned in tandem—Continuous Diagnostics and Mitigation (CDM) and EINSTEIN. The congressional authorization for EINSTEIN expires in December 2022, which presents a compelling opportunity to rethink holistically the overarching .gov security posture. These strategic conversations should build on recent policy improvements from cyber-focused executive orders, security improvements from related legislative activity, and maturation in CISA's capabilities governance policies (such as TIC 3.0).

The sunset of the current EINSTEIN authorization provides a unique opportunity to force necessary evolutions of the program at a moment where there is bipartisan interest in better fortifying federal networks.

EINSTEIN Explained

EINSTEIN is the dominant tool in CISA's manifestation of the 2015 legislative intent—formally called the National Cybersecurity Protection System (NCPS). In practice, EINSTEIN and NCPS are often used synonymously.

In simplest terms, EINSTEIN provides perimeter defense for Federal Civilian Executive Branch Agencies. In totality, it represents the evolution of three iterations—E1 that provided net flow

data (collecting and monitoring network traffic flow), E2 to provide signature-based intrusion detection, and E3A to leverage capability of commercial internet service providers (ISPs) to more nimbly detect potential cyber incidents and prevent compromise.

The EINSTEIN Program was launched in 2003 with an estimated lifecycle cost of well over $5 billion to date. It was formally authorized through the *Cybersecurity Act of 2015*, which required civilian agencies to begin utilizing the program, a significant milestone in ensuring full intrusion prevention coverage across the government.

Specifically, that legislation authorized a "Federal Intrusion Detection and Prevention System" that has the "capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk."

The law also acknowledges concerns around the inherent shortcomings of EINSTEIN's underpinning technology by requiring DHS to "regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities… as appropriate to improve the intrusion detection and prevention capabilities."

While EINSTEIN can continue operating after its seven-year authorization expires in December 2022, reauthorization presents an opportunity to strategically reorient a defense in depth posture for federal cybersecurity.

"Necessary but Not Sufficient"

There is growing recognition that EINSTEIN represents, at best, the most basic and elementary blocking and tackling for network defense—a reality reinforced by a slew of GAO reports and congressional oversight.

- During a June 2015 congressional hearing in the wake of the OPM breach, Andy Ozement, DHS Assistant Secretary for the Office of Cybersecurity and Communications, said that "EINSTEIN 3A is a signature-based system. It can only block attacks that it knows about. This is necessary, but not sufficient, for protecting the civilian government."

- CISA Executive Assistant Director for Cybersecurity Eric Goldstein testified during a 2021 House Appropriations Committee hearing that EINSTEIN "[h]as grown somewhat stale over time, and now does not provide the visibility that CISA needs." He went on to highlight, rightfully, the need to move detection capabilities from the perimeter layer deeper into agency networks.

Post SolarWinds Scrutiny—Diagnosing the Wrong Problem

In the wake of SolarWinds, EINSTEIN came under significant public scrutiny for having "missed" the Russian-backed campaign. This narrative spread beyond cybersecurity and national security trade press. While EINSTEIN's limitations have become abundantly clear, the appropriate question post SolarWinds should not have been "why did EINSTEIN not detect SolarWinds," but rather "what happened to the complementary suite of tools that theoretically *could* have detected SolarWinds?"

This reality was further highlighted in a letter from the leadership of the Senate Homeland Security and Government Affairs Committee to CISA in the spring of 2021 that recognized the "inherent limitation of perimeter-based intrusion detection systems" as they are "ineffective at identifying or blocking sophisticated and novel attacks."

To increase the security of federal civilian networks, Congress should implement the following recommendations during the EINSTEIN reauthorization process:

- Go beyond simply reauthorizing "better" signature-based intrusion detection. That represents the most minimalist foundation of effective network defense for complicated enterprises. That approach would fail to appropriately compartmentalize the misguided nature of the post SolarWinds EINSTEIN criticism.

- Codify and build upon many of the principles contained in the Executive Order on Improving the Nation's Cybersecurity. While not a silver bullet, this EO represents a well-crafted collection of policies that, in total, move the federal civilian space closer towards having centralized visibility of network threats. Specifically, the focus on secure cloud, Zero Trust, advanced endpoint detection, secure software supply chains, and holistic attack surface management posture presents a compelling model for the future of .gov security.

- Ensure the EINSTEIN reauthorization fits together with other related legislative efforts. These include proposals to codify CDM, ongoing Federal Information System Management Act (FISMA) reform conversations, and Federal Risk and Authorization Management Program (FedRAMP) codification. These should be complementary authorities acting in concert, not a grab-bag of laws haphazardly layered on top of one another.

- Pay specific attention to cloud visibility. CISA's Cloud Security Technical Reference Architecture is a solid piece of policy that should continue to account for comprehensive cloud security controls across all program areas, including asset inventories and automated governance for consistent visibility and enforcement. Its historical focus was geared towards documentation accounts for cloud applications solely via its data protection requirements—that is, requirements to control where specific data types can reside, whether or not data is publicly exposed, and who may access it.

- Focus on data integration. With a growing array of enterprise security tools in its toolbox—integration of data layers and security automation become paramount. Network, cloud, and endpoint data should be seamlessly integrated to maximize centralized, actionable visibility. This should be fused with enhanced capability to automate defensive operations, leveraging advanced data lakes and AI.

- Consider anticipated evolutions of CISA's shared services model. CISA's Cybersecurity Quality Service Management Office has tighter organizational synergy to the CDM program than EINSTEIN. The optimal long-term arrangement between EINSTEIN capability and CISA's growing shared services model should be considered during reauthorization.

- Optimize the capability of the EINSTEIN technology stack. We should encourage advanced techniques to monitor networks that ISPs can bring to bear and marry those with threat intelligence, vulnerability information, and other telemetry from leading cybersecurity companies. This would result in a more dynamic fusion of capability than current E3A solutions. CISA should increase transparency around current capabilities embedded within EINSTEIN, identified gaps, and opportunities for commercial solutions to fill those gaps.

This paper is a product of the Forum for American Leadership's Technology and National Security Innovation Working Group.

The Forum for American Leadership (FAL) is a non-profit organization that presents expert analysis and national security recommendations to policymakers in Congress and the Executive Branch.

Want to learn more about this subject, arrange an interview, or set up a briefing with FAL experts? Contact us here.