BYOS, the National Cybersecurity Implementation Plan, and its Implications for the FY25 Budget

Whitepaper - August 2024

In May 2024, the White House released Version 2 of the National Cybersecurity Implementation Plan[1]. This plan is a roadmap that aligns federal funding to the nation's top cybersecurity priorities. Pillar one of this plan, reflecting the highest priority for our national security; Defend Critical Infrastructure.

This whitepaper will discuss the priorities of the Government for critical infrastructure protection, a brief cross-reference to relevant threat data, and explain how the BYOS solution contributes to threat surface reduction and security for critical infrastructure at scale.

Initiative 1.2.1

Under Initiative 1.2.1, *Scale public-private partnerships to drive development and adoption of secure by-design and secure-by-default technology*, the Government seeks to partner with technology manufacturers and others to drive the development and adoption of software and hardware that is secure-by-design and secure-by-default. BYOS meets this initiative by providing an endpoint microsegmentation capability that is secure by design. The patented BYOS Secure Edge is a hardened, embedded security stack that isolates assets onto their own unique network *micro-segment of one*, protecting it from compromised networks and other compromised endpoints on the network. BYOS has two products:

1. Secure Endpoint Edge™: a small, portable, plug-and-play USB device for devices like Laptops, tablets, and phones, which allows employees, and contractors to safely and securely connect to any network, regardless of their location or network environment.
2. Secure Gateway Edge™: a small IoT Gateway for micro segmenting industrial and unmanaged devices like PLCs, Controllers, Switches, and Workstations.

Microsegmentation is a technique that divides networks into small, distinct, protected zones in order to strengthen an organization's security posture. This approach decreases risk by reducing the available attack surface within a network and makes it easier to contain and remediate security incidents if and when they occur by preventing lateral movement and privilege escalations.

Endpoint microsegmentation differs from network segmentation in the way a network is protected. In network segmentation, each segment is protected as its own mini-network, and administrators create policies to define how traffic can flow from one segment to another. Users, endpoints, and network traffic already within an organization's perimeter are automatically trusted, so protecting the enterprise's system from the world beyond it becomes the priority. This approach has become less secure over time, and is currently being routinely exploited, per data obtained from a recent report of the Director of National Intelligence: Recent Cyber Attacks on

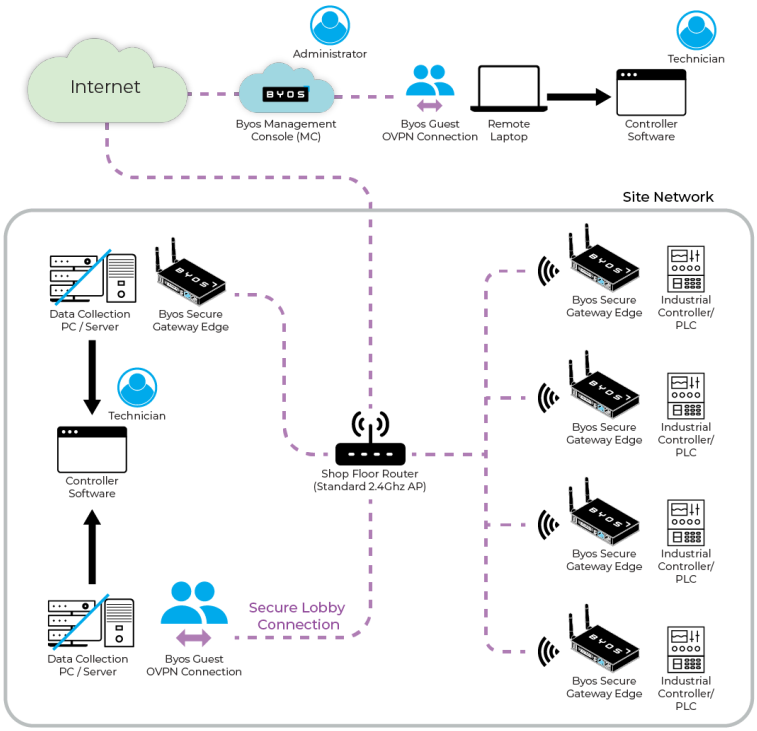
[1] https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024 (June 2024)[2].

- During the 6-month period observed in the report, there were 36 successful attacks against US Critical Infrastructure.
- Food and agriculture, healthcare, and water and wastewater sectors were impacted by these attacks.
- Human Machine Interfaces (HMI), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), and Industrial Equipment were targeted.

Top recommendations offered by DNI for immediate triage include; change default passwords, Inventory ICS assets to find vulnerable devices and associated Common Vulnerabilities and Exposures (CVEs), and Enforce User Access Controls and Multifactor Authentication for Remote Access. These are logical recommendations that can immediately reduce risk, **but what happens when 35% of critical ICS vulnerabilities identified in CISA CVE's have no patch or remediation available from the vendor?**[3]

One solution is to "front end" ICS, SCADA, and PLC's that cannot be patched with BYOS Secure Gateway Edge™ devices, enabling these critically vulnerable devices to be protected from direct access by adversaries, and obfuscated from discovery tools, techniques, and practices (TTPs) such as network mapping and port scans. In a 1:1 deployment of BYOS for these critically vulnerable assets, critical infrastructure can reduce its corresponding threat surface by 35% today, without requiring patches that are likely to never come.



Initiatives 1.5.1 and 1.5.2

Moving on to Initiatives 1.5.1 and 1.5.2, *Secure unclassified Federal Civilian Executive Branch (FCEB) systems and Modernize Federal Civilian Executive Branch (FCEB) technology*,

[2]https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
[3]https://www.csoonline.com/article/574409/many-ics-flaws-remain-unpatched-as-attacks-against-critical-infrastructure-rise.html

respectively, BYOS offers a low-cost path to enterprise-level security of all network endpoints, including brownfield investments that are harder to protect as they approach end of life.

Network modernization investments can then be spread over FY's, affording the opportunity for agencies to selectively upgrade investments based on mission priority rather than "rip and replace" at scale. This approach aligns favorably with a recent White House Memorandum outlining Administration Priorities for FY 2025 Budget[4], helping agencies address *how* they intend to meet the cross-agency cybersecurity investment priorities in their budget submissions:

> "*Consistent with the five pillars of the National Cybersecurity Strategy (NCS), departments and agencies should prioritize five cybersecurity effort areas: 1) Defend Critical Infrastructure; 2) Disrupt and Dismantle Threat Actors; 3) Shape Market Forces to Drive Security and Resilience; 4) Invest in a Resilient Future; and 5) Forge International Partnerships to Pursue Shared Goals. These priorities should be addressed within the FY 2025 Budget guidance levels provided by OMB.*"

Furthermore:

> *"Agency investments should lead to durable, long-term solutions that are secure by design. Budget submissions should demonstrate how they:*
>
> - *achieve progress in zero trust deployments as outlined in OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, and explain efforts to close any gaps in those requirements;*
> - *meet the goals set forth in the Federal Zero Trust Strategy and make clear how agency investments support people, processes, and technology that advance agency capabilities along the Zero Trust Maturity Model;*
> - *prioritize technology modernization where agency systems are reaching end of life or end of service and where Federal Information Security Modernization Act High and High Value Asset systems that are unable to meet zero trust requirements, ensuring that these systems meet standards for security and customer experience requirements;*
> - *secure National Security Systems, including those that are owned or operated by Federal civilian Executive Branch agencies"*

BYOS endpoint microsegmentation extends zero trust to any connection, including remote Wi-Fi connections, and supports a number of target level and advanced ZTA requirements, including:

- BYOS enables rapid identification of User and System Inventory
- Establishes a basic set of user attributes for authentication and authorization as well as adding / updating attributes within the solution
- Enables conditional user access / just-in-time access / just enough administration methods
- Enables dynamic access decision making down to the specific endpoint / microsegment
- Enables enclave / DDIL identity, credential, and access management
- Provides multi-factor authentication for users and machines in a single application
- Ensures privileged access management down to the endpoint / microsegment

[4] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf

- Meets interoperability standards for data rights management and protection down to the endpoint / microsegment

BYOS delivers these ZTA benefits at a low cost per endpoint with the flexibility to scale to an entire enterprise with no disruption to continuing operations. Protect end of life systems until budgets allow their replacement, protect high value asset systems utilizing 1:1 microsegments, and secure any network, OT, critical infrastructure asset where vulnerabilities might remain "forever days" due to products that are no longer supported / vendors not planning future releases / fixes.

Disrupt and Dismantle Threat Actors

Pillar 2 of the White House Budget Memorandum aligns to Pillar 2 of the NCS. Both call for mounting disruption campaigns and other efforts to make ransomware operations unprofitable. Analysis by popular website Cybercrime Magazine projects the global cost of ransomware attacks to exceed $265B annually by 2031[5]. BYOS Secure Edge is a force multiplier for the disruption of ransomware threats. The first three steps of any successful ransomware attack require surveillance, initial compromise, and persistence on a targeted system. A BYOS-enabled endpoint is obfuscated from surveillance TTPs, which in turn rapidly reduces the likelihood of an initial compromise. If an adversary has compromised an endpoint prior to the installation of BYOS, activating a BYOS Secure Edge breaks adversary persistence. When an attacker attempts to reconnect to the previously "known compromised" device, it is no longer discoverable on the network due to BYOS network obfuscation.

Should ransomware be deployed on a network post-installation of BYOS (dead-man PLC, time bomb, zombie, etc.) the "blast radius" of the ransomware attack becomes *that single endpoint*. Privilege escalation and lateral movement in a 1:1 deployment of BYOS Secure Edge is also constrained to a single endpoint. If an agency wishes to put an entire department on a single BYOS microsegment, the "blast radius" of a ransomware attack is contained that specific microsegment, not the entire network. This combination of features will help you defend your networks against devastating ransomware attacks, which are projected to cost hundreds of billions of dollars annually by 2031, and also erode the public trust. In a whole of government deployment, it is plausible to consider that BYOS Secure Edge would drastically reduce the likelihood of a successful "fire sale" type attack as dramatized in the recent film "Leave The World Behind".

In conclusion, BYOS endpoint microsegmentation provides one of the most powerful, cost-effective solutions for ICS/SCADA/IT/OT protection available today. User-definable endpoint microsegmentation delivers the greatest flexibility for protecting high-value network assets and brownfield systems on any network of any size, enabling any organization to achieve a phased-approach to security and modernization that accommodates a variety of budgetary planning / execution objectives for FY25 and beyond.

For additional information or to schedule a demonstration today, please contact David Stephens: david.stephens@byos.io, 571-437-1111 or John Kerr: John.kerr@fcnit.com, 571-612-0144. Special thanks to our contributors Bobby Westerman & Floyd Marshall.

[5] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion