ZERO TRUST FOR FEDERAL ENTERPRISE

FEDERAL CYBERSECURITY AND PRIVACY PROFESSIONALS FORUM
May 21, 2024

Branko S. Bokan –
Architecture and Engineering Center of Excellence, CISA
Federal Civilian Zero Trust Landscape

The Principles
NIST SP 800-207
Zero Trust Architecture

The Imperative
EO 14028
Improving the Nation’s Cybersecurity

The Strategy
OMB M-22-09
Zero Trust Strategy

The Operational Guidance

CISA Zero Trust Maturity Model

TIC Catalog

Federal Cloud Security TRA

NSTAC Report

Branko Bokan
May 21, 2024
This **Zero Trust Maturity Model (ZTMM)** is one of many paths to support agencies

Version 2.0 was released in April 2023 based on feedback from agencies, vendors, consulting services, academia, trade associations, individuals, and foreign organizations.

**Intent:** Help agencies as they develop plans to implement Zero Trust Architectures (ZTA) in response to EO14028 Sec 3,b,ii (May 2021)

**OMB’s M-22-09** (January 2022) requires agencies to achieve specific zero trust security goals that are organized using the ZTMM
Zero Trust Maturity Model Overview

- The ZTMM represents a gradient of implementation across five distinct pillars and three cross-cutting capabilities

- **Four stages**: Traditional, Initial, Advanced & Optimal

- Heavily influenced by OMB, NIST, DOD, and NSA’s Zero Trust publications
Zero Trust Maturity Journey

- Each stage on the Zero Trust Maturity Journey requires greater levels of protection, detail, and complexity for adoption, with exponential growth in efforts and benefits.

  - **Traditional**: Manual configuration, response, and mitigation; static and siloed policies and solutions
  
  - **Initial**: Starting automation; initial cross-pillar solutions; some responsive changes to least privilege; aggregated visibility for internal systems
  
  - **Advanced**: Automated controls where applicable; cross-pillar policy enforcement; least-privilege changes based on risk/posture; response to pre-defined mitigations
  
  - **Optimal**: Fully automated, just-in-time, self-reporting; dynamic least privilege access; cross-pillar interoperability with continuous monitoring, centralized visibility

*New with ZTMM V2
TIC 3.0
Journey from TIC 2.0 to Zero Trust Architecture (ZTA)

TIC 2.0 - Traditional TIC/Managed Trusted Internet Protocol Service (MTIPS)
- Acceptable architecture to meet TIC 3.0 requirements
- Defined by the Traditional TIC Use Case
- Provides perimeter security by funneling all incoming and outgoing data through TIC Access Points

TIC 3.0 – Secure Access Service Edge (SASE)/Security Service Edge (SSE)
- Acceptable architecture to meet TIC 3.0 requirements with greater flexibility than traditional TIC2/MTIPS model to account for multiple and diverse architectures rather than single perimeter approach
- Zero Trust Network Access (ZTNA) provided through policy enforcement parity with TIC Access Point
ZT Capabilities Observatory
ZT Capabilities Observatory

- Visual representation of relationships between CISA’s cybersecurity capabilities and the ZT concepts
- A comprehensive database maps cybersecurity CISA provides to FCEB to CISA’s ZTMM 2.0.
- Helps the practitioners answer questions like:
  - How can CISA-provided capabilities support agency Zero Trust efforts?
  - How do my organization’s existing cybersecurity capabilities align with Zero Trust principles?
  - Where are my organizational gaps (Zero Trust pillars or functions without or with light capability coverage)?
  - What capabilities should my organization invest in to improve my Zero Trust maturity?
  - What CISA capabilities are available to my organization that I can use to improve my Zero Trust maturity?
Protective Domain Name System (DNS)
**EINSTEIN Statutory Requirements**

- 6 USC § 663 requires:
  - CISA is to operate a capability to detect and prevent cybersecurity risks associated with agency network traffic travelling between agency information systems.
  - The "head of each agency shall apply and continue to utilize the intrusion detection and prevention capabilities and any improvements to such capabilities made available by CISA."
  - This means each FCEB agencies are required to utilize CISA's detection and prevention services including EINSTEIN sensors, Protective DNS, and future capability improvements.
E3A DNS Sinkholing

- In September 2022, CISA replaced the DNS Sinkholing capability with Protective DNS and FCEB agencies were required to migrate by April 2023.

- CISA evaluated the performance, benefits, and cost of E3A when deciding to sunset both Email Filtering and DNS Sinkholing capabilities on December 22nd.

- This change did not affect EINSTEIN 1 (E1) and EINSTEIN 2 (E2) capabilities, which will remain operational, per agencies requirement to use.
DNS Defense – Evolved: CISA Protective DNS

- Protects on-premises networks, cloud instances, roaming, nomadic, and mobile devices
- Supports emerging encrypted DNS protocols
- Aligns with the Federal ZT Strategy by supporting modern encrypted DNS protocols and being device-centric
- Logs ALL DNS traffic and provides enhanced visibility
- Fully integrated with four SASE/SSE vendor solutions.
- Distributed to 300+ data centers across 90+ countries for maximum availability and resilience
Protective DNS and SASE/SSE

- OMB Memorandum M-22-09 requires FCEB agencies to encrypt DNS traffic where technically feasible.
- Several SASE/SSE vendor platforms are fully integrated with Protective DNS.
- SASE/SSE solutions allow encrypted DNS protocols and Protective DNS integration on mobile, roaming, and nomadic devices.
Protective DNS

- Nomadic Windows/ MacOS/*nix
- Roaming Windows/ MacOS/*nix
- Mobile iOS
- Mobile Android

CISA Protective DNS

- DNS over HTTPS DoH:443 (via Cloudflare Warp client)
- Authorized sources allow listed by IP
- Perimeter firewall (blocks any:any:S3:853)
- "Traditional teleworker"
- DoH enabled Browser/app
- Public DNS Resolver (DNS:S3, DoH, DoT)
- Agency cloud instances
- SASE enabled roaming users

- Data lake
- Threat feeds
- Management application Web interface
- DNS:S3
- Root DNS Server
- Authoritative DNS
- DNS over HTTPS:443
- SASE Provider
- Intercepted DNS:S3 forwarded over HTTPS:443
Background

- Provides implementation guidance for federal agencies to meet federal requirements related to encryption of DNS traffic designed to guide agency network practitioners and assist with implementation of currently feasible technical capabilities.
- OMB Memorandum M-22-09 specifically calls for agencies to use encrypted DNS traffic where technically feasible.
- Agencies are also required to use CISA’s Protective DNS capability for all egress DNS resolution, per both M-22-09 and 6 U.S.C. § 663.
- Result of CISA’s work with both federal DNS experts across FCEB and vendors.
- The guidance does not prescribe nor endorse any particular vendor or solution.
Encrypted DNS protocols

DNS over HTTPS (DOH)
DNS over TLS (DOT)
DNS over QUIC (DOQ)

Not DNS over IPSec!

At the time of issuance, only a few technologies (Firefox and Chromium based browsers) used in the enterprise supported these protocols.

CISA has been working closely with major vendors and as of today, Protective DNS, major DNS servers (Infoblox and Bind), operating system native stacks (Windows 11), and major SASE/SSE products support encrypted DNS protocols.
Checklist and phased approach

- Implement and enforce Protective DNS
- Block unauthorized DNS traffic
  - We are still observing egress DNS queries to E3A and many foreign countries!
  - Disable or configure web browsers.
- Encrypted DNS traffic between agency DNS infrastructure (DNS servers) and Protective DNS
- Encrypt DNS for roaming and nomadic devices
- Encrypt DNS in cloud deployments
- Encrypt DNS traffic for on-premises endpoints
Integration with Protective DNS

- All egress on-premises DNS traffic must be routed to Protective DNS
  - Agencies must work to minimize bypass

- Roaming/nomadic/mobile devices:
  - access via agency DNS infrastructure, or
  - via Agency SASE/SSE

- Cloud instances (primarily IaaS and PaaS):
  - direct access, or
  - via agency DNS infrastructure
Guest networks and security appliances

- New guidance under development
- Separate networks, NAT sources, authorized sources, and Protective DNS destinations (for DoT and DoH).
- Clearly label sources in Protective DNS
- On guest networks:
  - Block any:any over :53 and :853 on guest network perimeter
  - Assign (dedicated) internal DNS server or Protective DNS as default via DHCP
  - Display legal banner
Vendor Specific Implementation Guidance

- DNS Servers
- SASE Platforms
- Web browsers
- Operating system native stacks
Secure Cloud Business Applications (SCuBA)
SCuBA Overview

WHAT IS SCUBA

- Secure Cloud Business Applications (SCuBA) project provides guidance and capabilities securing cloud business application environments. The project was developed with comprehensive threat-informed methodology to identify cloud visibility coverage gaps and requirements.

SCUBA BENEFITS

- SCuBA will enhance the security of cloud business application environments through added configurations, settings, and security products.
- This comprehensive approach ensures robust and reliable resources that can rapidly adopt to the constant changes, updates and threats common in SaaS offerings.

WHO IS SCUBA FOR

- SCuBA is open source and no cost, for Federal Civilian Executive Branch (FCEB) agencies, critical infrastructure, small businesses and those who want enhanced security.
SCuBA Workstreams

Cloud Solutions Guidance
- SCuBA develops operational guidance for cloud solutions to help organizations make informed security decisions within their cloud environments.
- The Technical Reference Architecture, Hybrid Identity Solutions Guidance and the Secure Web Gateway Solutions Guidance are in various stages of development.

Engagements
- Agency pilots exercise SCuBA’s guidance and tools in an agency’s tenant to address issues with security and functionality.
- Workshops build the capacity for an organization’s use of SCuBA’s tools and guidance by collaboratively engaging stakeholders with technical expertise.
- Technical Exchange Meetings bring together key stakeholders to identify areas for continuous product improvement and future service offerings.

Secure Configuration Baselines
- Detailed, product-specific guidance on configuring agency cloud environments to meet the minimum-security recommendations. Cloud Security Provider suites are open to vulnerabilities if misconfigured. Current baselines efforts are centered around M365 and GWS products.
- Automated assessment tools provide an easily digestible, visual report to quickly identify areas of security posture improvement.

Visibility
- eVRF enables organizations to identify visibility data that can be used to mitigate threats, analyze it from a threat-informed perspective, understand the extent to which specific products and services provide useful visibility data in their telemetry and identify potential visibility gaps.
- WeVRF will provide entities the ability to build visibility coverage maps through an app to help easily identify areas in their architecture where security needs to be bolstered.
CISA's Zero Trust Initiative
CISA's Zero Trust Initiative

- Education and training:
  - Expand Zero Trust training opportunities
  - Identify the skills/knowledge needed for successful ZT implementations
- Playbooks and guidance:
  - Build on existing CISA resources like ZTMM and TIC 3
- Community building and collaboration:
  - Established two ZT forums open to agencies - Practitioners COP & NetMod WG
  - Expand relations w/ inter-agency partners and the greater IT community
- Gauging an organization’s ZT Maturity:
  - Collaboratively develop metrics and benchmarks to track progress towards ZT maturity
Questions?
zerotrust@cisa.dhs.gov

Zero Trust Maturity Model Webpage:
https://www.cisa.gov/zero-trust-maturity-model