CISA, FEDERAL CIVILIAN ENTERPRISE, AND ZERO TRUST

Branko S. Bokan, CISSP-ISSAP, ISSEP, ISSMP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

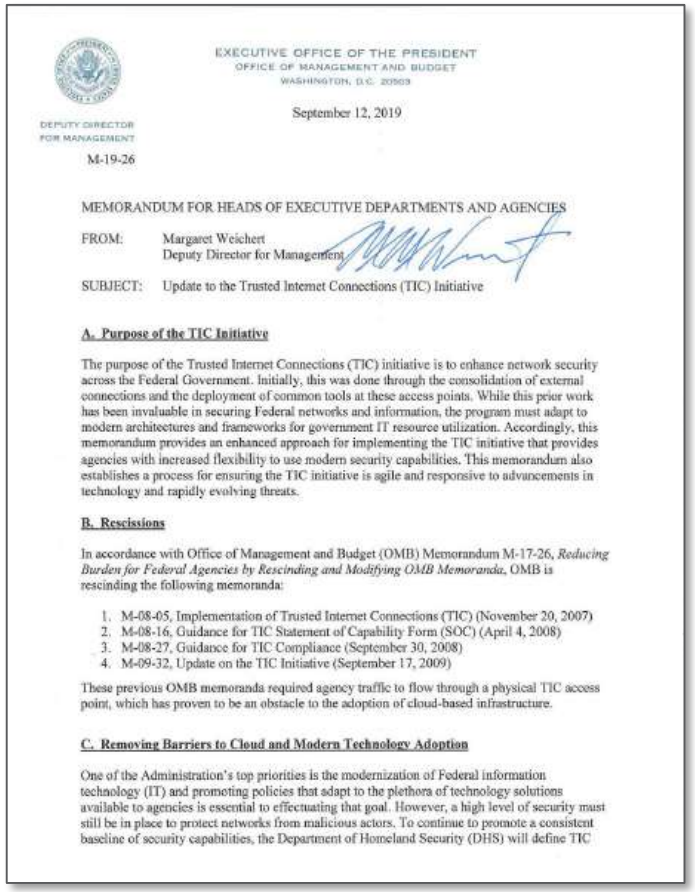
months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

Trusted Internet Connection Memo & Core Guidance



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 12, 2019

DEPUTY DIRECTOR FOR MANAGEMENT

M-19-26

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret Weichert
Deputy Director for Management

SUBJECT: Update to the Trusted Internet Connections (TIC) Initiative

A. Purpose of the TIC Initiative

The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modern architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

B. Rescissions

In accordance with Office of Management and Budget (OMB) Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, OMB is rescinding the following memoranda:

1. M-08-05, Implementation of Trusted Internet Connections (TIC) (November 20, 2007)
2. M-08-16, Guidance for TIC Statement of Capability Form (SOC) (April 4, 2008)
3. M-08-27, Guidance for TIC Compliance (September 30, 2008)
4. M-09-32, Update on the TIC Initiative (September 17, 2009)

These previous OMB memoranda required agency traffic to flow through a physical TIC access point, which has proven to be an obstacle to the adoption of cloud-based infrastructure.

C. Removing Barriers to Cloud and Modern Technology Adoption

One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect networks from malicious actors. To continue to promote a consistent baseline of security capabilities, the Department of Homeland Security (DHS) will define TIC

1| Program Guidebook

2| Reference Architecture

3| Security Capabilities Catalog

4| TIC Use Case Handbook & Use Cases

5| Overlay Handbook

- Intended to guide secure implementations and help agencies satisfy program requirements within discrete networking environments
- Updated Capability Catalog with 118 Capabilities, including:
  - Identity (8 capabilities)
  - Map new capabilities
  - Email (11 new TIC capabilities to ZT Maturity Model)

Traditional TIC Use Case

Branch Office Use Case

Remote User Use Case

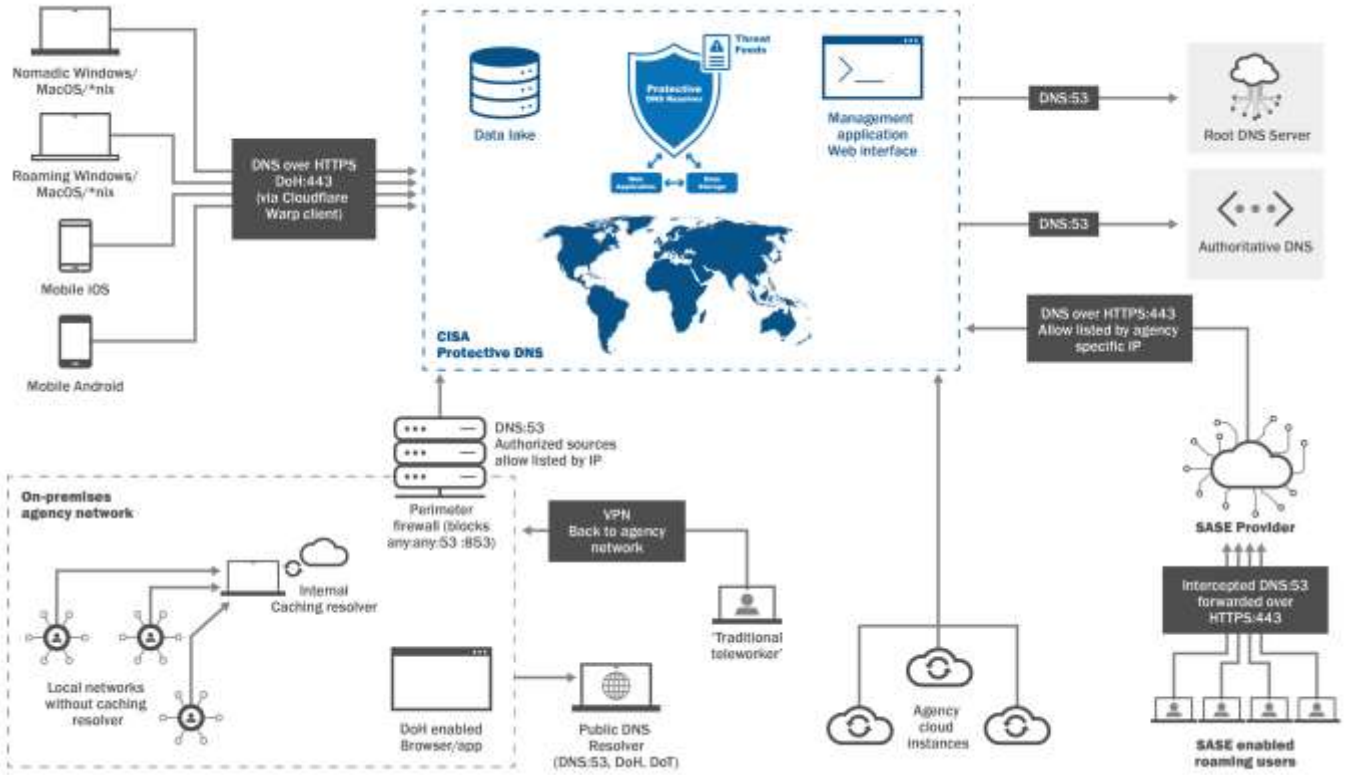
Cloud Use Case

- Represents IaaS, PaaS, SaaS, and EaaS
- Largest Use Case released
- Aligns with the CSTRA and ZTMM
- Request for Comments (RFC) added a Cloud-to-Cloud security pattern

Federal Civilian Executive Branch (FCEB) Team Building

- Zero Trust Community Building & Surveying
  - Initiating Managers' Community of Practice (CoP)
  - Cohort training – 10 agencies in the first cohort
- 10+ CyberStat Workshops that support OMB's M-22-09 & ZTMM Pillars
  - Well attended, over 600 participants on some webinars
- Meeting with CIOs and CISOs on understanding agencies' ZT challenges and priorities
- Together with OMB co-hosting multiple Communities of Action (CoAs)

Protective Domain Name System (DNS)



Protects the enterprise by preventing government Internet traffic from reaching malicious destinations by using state-of-the-art DNS technologies

- Replacing NCPS/E3A DNS service
- Aligns with the Federal ZT Strategy by supporting modern encrypted DNS protocols and being device-centric
- Provides enhanced visibility

Continuous Diagnostics and Mitigation (CDM)

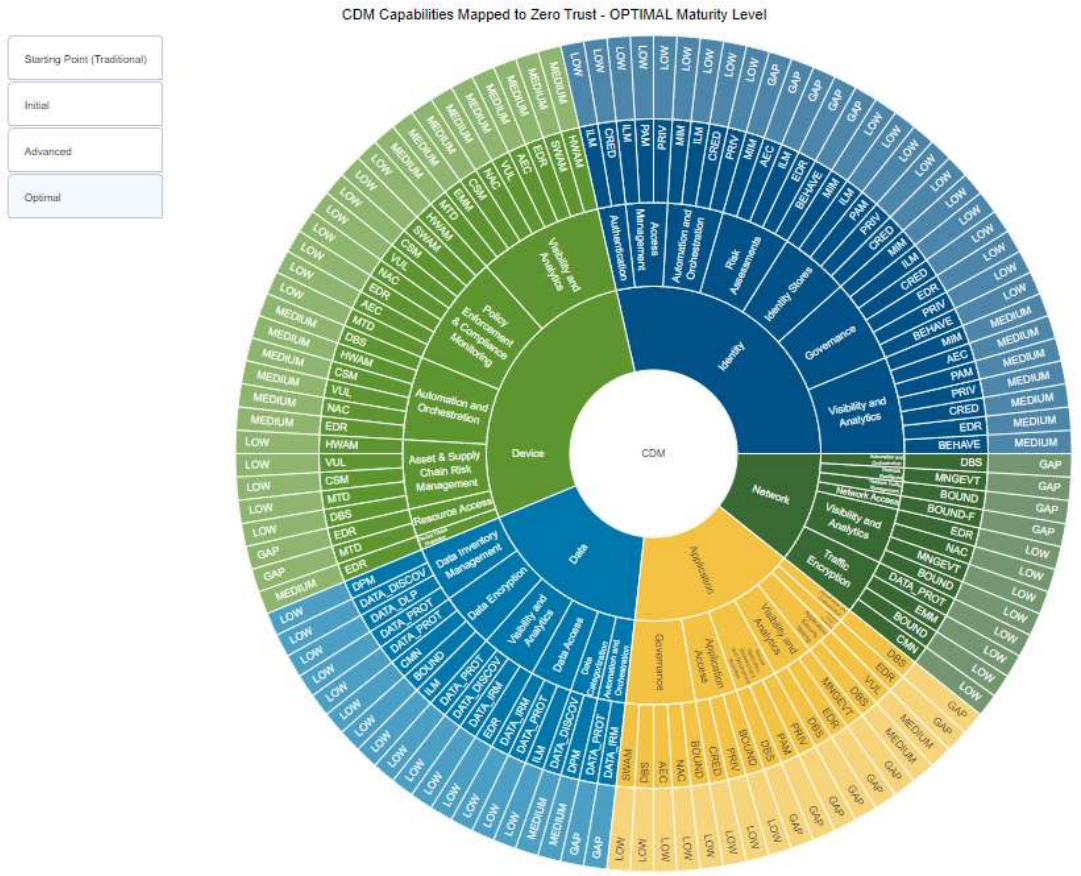
- Working to realign ongoing Continuous Diagnostics and Mitigation (CDM) efforts to support broader CISA and agency ZT initiatives
  - Exploring how to prioritize backlogged capabilities to address underserved ZT pillars (e.g., data, application)
- Devices
  - Completing Asset Management Baselining (AMB) efforts to close remaining gaps
  - Mobile endpoint and threat detection progressing
  - Continuing Endpoint Detect and Response (EDR) deployments
  - 45 agencies participating in CDM's deployment
- Identity
  - Continuing efforts on Identity Lifecycle Management (ILM) and Privileged Access Management (PAM)
- Network
  - Expect to operationalize CISA's Persistent Access Capability (PAC) in FY23 in support of CDM-Enabled Threat Hunting Use Case

Zero Trust Capabilities Observatory

- Allows cybersecurity practitioners to visualize the relationships between CISA's cybersecurity capabilities and ZT concepts.
- A representation of a comprehensive database of mappings between CISA offerings and ZTMM 2.0
- Aimed at FCEB agencies but can be used by other industries – from practitioners to leadership.

Zero Trust Capabilities Observatory

- Zero Trust assumes no implicit trust in any part of the environment.
- Zero Trust does not require ‘rip and replace’
- Instead, embarking on a Zero Trust journey is about using and expanding existing cybersecurity capabilities to better protect organizational assets.



Zero Trust Capabilities Observatory

- Helps organizations to better understand how their existing capabilities align with Zero Trust Concepts
- Helps 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?

Questions?

For CISA Media inquiries:
Contact CISA Media at CISAMedia@cisa.dhs.gov
or 703-235-2010

TIC Webpage:
https://www.cisa.gov/tic

TIC Frequently Asked Questions:
https://www.cisa.gov/tic-faq

TIC Mailbox:
tic@cisa.dhs.gov

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

Zero Trust Mailbox:
zerotrust@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA