TRUSTED INTERNET CONNECTIONS

MAKING THE RIGHT CONNECTIONS: AN OVERVIEW OF TRUSTED INTERNET CONNECTIONS (TIC) 3.0

CISA
CYBER+INFRASTRUCTURE

Sean Connelly
February 6, 2020

AGENDA

- TIC History
- TIC Present
- TIC Future
- Next Steps

TIC HISTORY

Pre-TIC Federal Horizon

- In the mid 2000s, OMB held a data call asking agencies to inventory their connections to the internet
- Agencies reported ~4,000 external connections
- OMB and the Agency CIOs and CISOs:
  - Were not aware of the total number of connections until the data call
  - Did not have parity of security across all connections
  - Challenged at managing growth
- DHS was beginning to mature its authorities to monitor and secure the federal .gov horizon

OMB Data Call Reaction

Explicit Goals (it was recognized there was a need for):

- Network consolidation across agencies
- Standardization of security perimeter
- Provides a platform for DHS/CISA to deploy sensors (EINSTEIN)

Implicit Goals (new authorities required):

- Empower enterprise CIOs and CISOs
- Motivate all agencies towards a stronger cyber posture
- CISA to weaken exfiltration activities across .gov

Program History

TIC 1.0 - Consolidate

- Reduced internet connections points
- Stand-up TICs for agencies and MTIPS Vendors

TIC 2.0 - 2.2 – Standardize

- Standardized the security of network connections in use by the federal enterprise, improving security posture, awareness, and incident response capability

TIC 3.0 – Modernize

- Environment-agnostic to drive security standards
- Leverage advances in technology as agencies move into the cloud
- Establishes agency and CISA visibility into modern cloud-based computing platforms

Focusing TIC Capabilities

As the goals of TIC evolve, the capabilities also evolve

- TIC 3.0 concentrates cybersecurity strategy, architecture and visibility
- Capabilities in TIC 2.2, which are not embedded in TIC 3.0, may exist elsewhere
- High-level changes in capabilities are categorized into three criteria

Some TIC 2.2 requirements are better captured in other CISA/OMB initiatives	Some TIC 2.2 requirements are no longer applicable	CAP Scoring and TCVs were retired

TIC Program Evolution Overview

	TIC 1 & 2 (PRE-2012)	SINCE TIC 2 RELEASE IN 2012	TIC 3.0 Future Approach
Circuit Consolidation Goal	▪ 4,300 down to ~50 TICs	▪ Declared complete in 2016	▪ Controlled expansion of multi-boundaries
NCPS Compliance	▪ HSPD-54 & TIC Requirement	▪ Federal Cybersecurity Enhancement Act of 2015	▪ Stronger delineation between NCPS and TIC ▪ NCPS Cloud Reference Architecture
Incident Response/NCCIC	▪ ~8 TIC Requirements	▪ M-15-01	▪ CISA's Federal Incident Response Requirements (FIRR) ▪ OMB's M-20-04
SCIF, Secure People & Communications	▪ ~5 TIC Requirements ▪ SCIF requirements were prepositioned for E3	▪ TIC 2.2 relaxed requirements in 2016	▪ M-20-04 includes clearance requirements
External Penetration Testing	▪ NCATS began in TIC PMO	▪ NCATS moved out of FNR in 2013	▪ High-level 3rd party testing requirement as applicable
Validation	▪ ~17 TICAPS: TCV Teams ▪ MTIPS: TCV Teams ▪ Smalls: Self-attestation	▪ TCVs disbanded in 2016 ▪ Currently no validation of TICAPs ▪ MTIPS: No Validation ▪ Smalls: No validation	▪ Policy promotes CDM and NCPS visibility ▪ FISMA 2014 ▪ TCV teams and framework integrated into HVA assessments
Compliance	▪ 2 OMB CAP Goals ▪ POA&M in Cyberscope	▪ Discontinued as CAP Goals ▪ POA&Ms discontinued ▪ CSP inventory moved to FISMA	▪ FISMA 2014 ▪ CDM visibility ▪ NCPS telemetry

TIC 2 Strategic Challenges

TIC 2 Environment

- Consolidation of networks
- One solution that offered a binary choice:
  - Networks are either External or Internal
- One security model to meet all data types

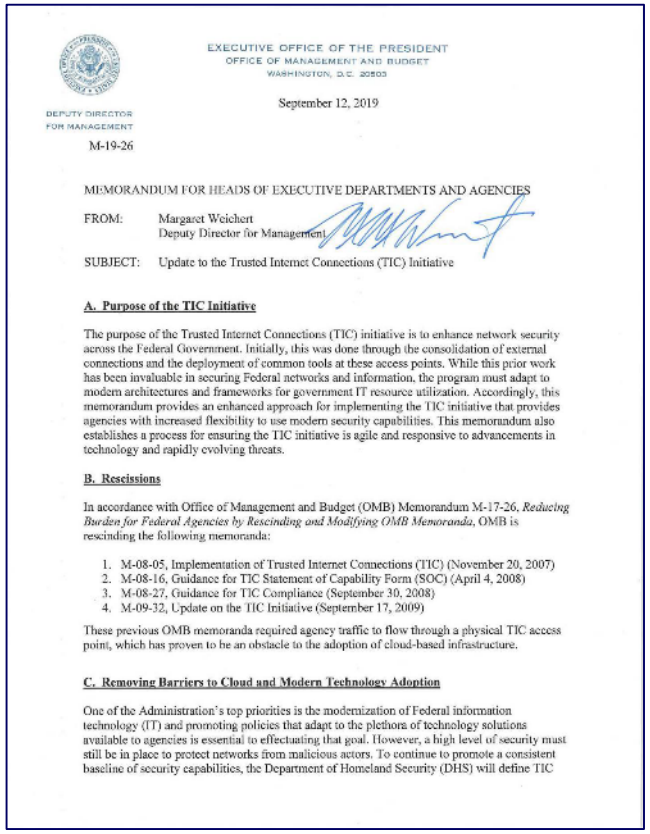
Challenges to Traditional TIC

- The Perimeter is dissolving
  - Mobile, cloud environments, partner networks, collaboration tools
- The risk tolerance of agencies varies
  - Agency embracement of the same cloud can vary per agency
- Traditional security assets (FW, IDS, WAF, AV) are not as easily transferrable to new environments

TIC PRESENT

OMB Memorandum M-19-26

- Released September 2019
- Tasks DHS CISA with modernizing the TIC initiative
- Calls for updated program guidance, use cases, and pilots
- Focus is towards:
  - Strategy
  - Architecture
  - Visibility



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

DEPUTY DIRECTOR
FOR MANAGEMENT

September 12, 2019

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

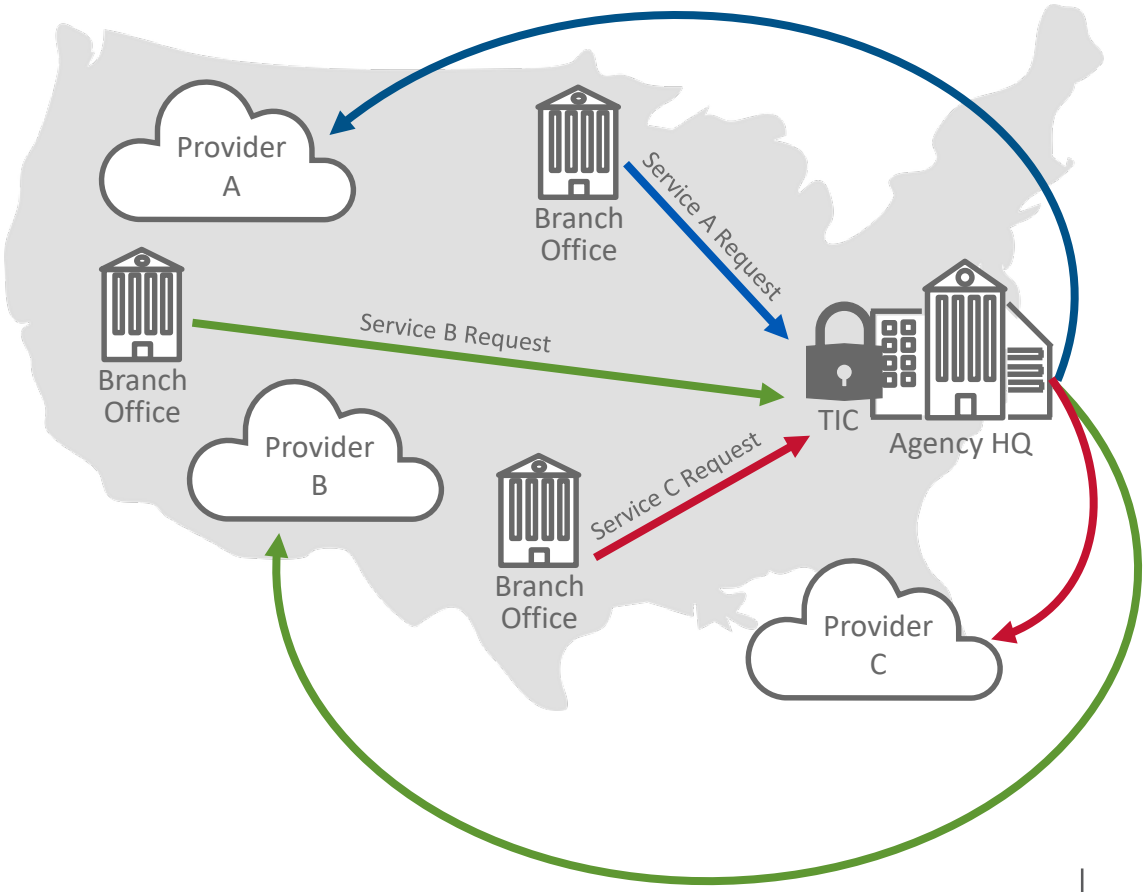
One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect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

CISA
CYBER+INFRASTRUCTURE

TIC 3.0 Accelerates Cloud Adoption

Eliminates the "TIC Tax":

- Reduces transport costs
- Reduces latency
- Improves user experience

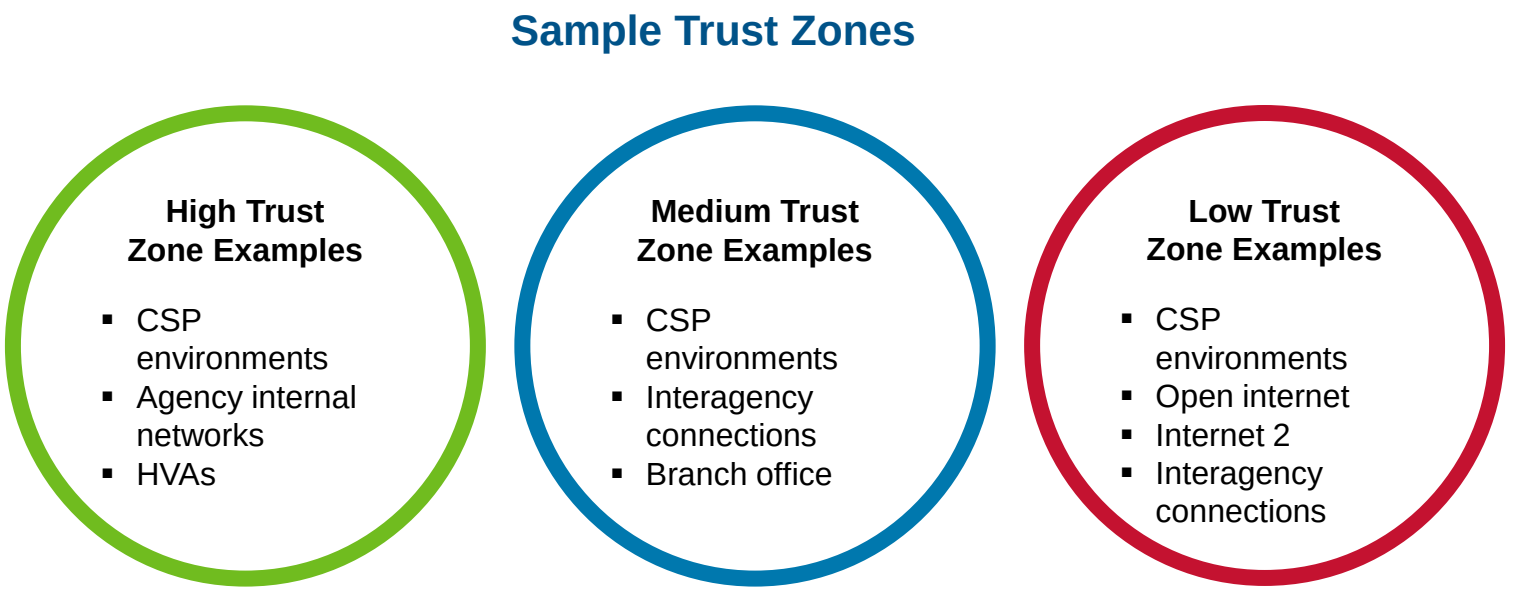


Multi-Boundary Approach Benefits

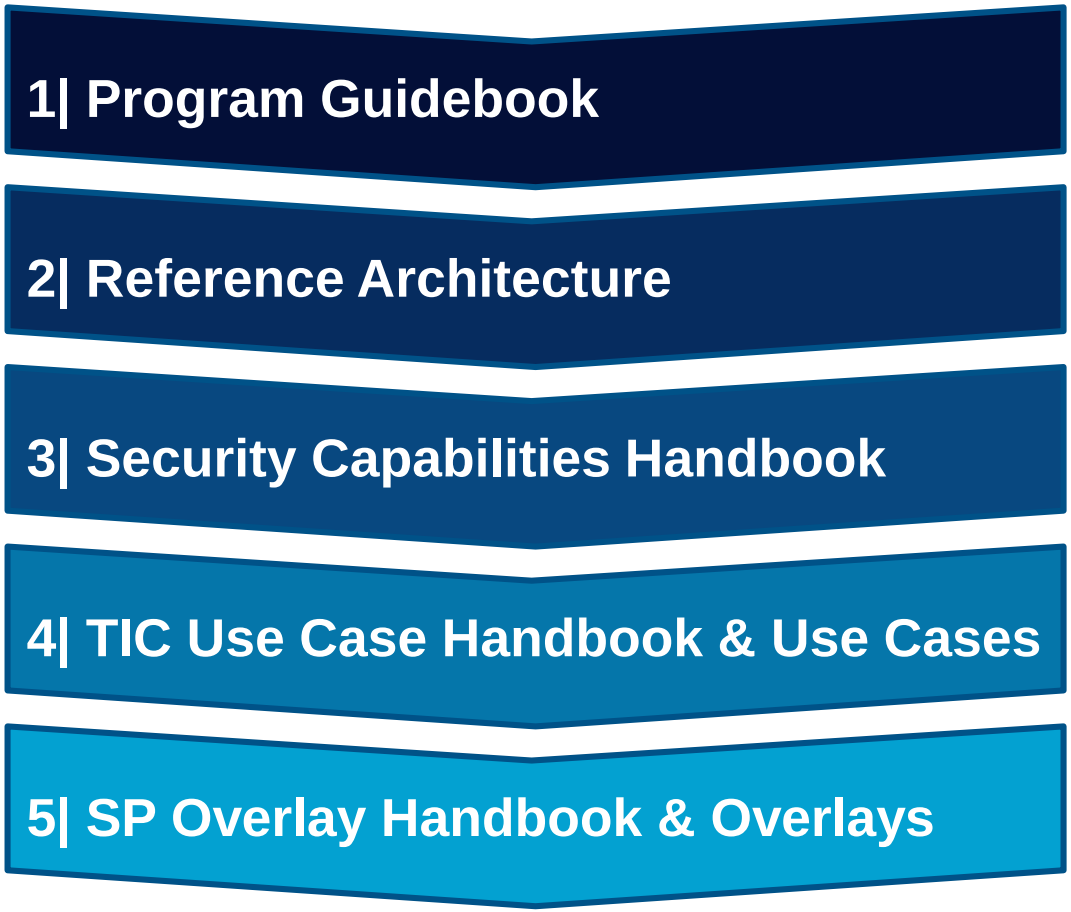
- TIC 3.0 supports the creation of trust zones to address agencies' distributed networks
- These zones create additional network boundaries and require the placement of security capabilities throughout the environment
- The additional security capabilities will give agencies greater visibility into their network, leading to operational and fiscal efficiencies

Multi-Boundary Approach Guidance

Agencies should designate trust zones based on their control, transparency, sensitivity, and verification of the data



Key Program Documents



- CISA released updated **draft** guidance December 2019
- Key **draft** program documents are high-level and conceptual in nature
- **Request for Comments (RFC) period closes February 7, 2020**

CISA
CYBER+INFRASTRUCTURE

1| Program Guidebook

- The **draft** TIC Program Guidebook outlines the modernized TIC program, expectations, and historical context
- Introduces the TIC Strategic Program Goals

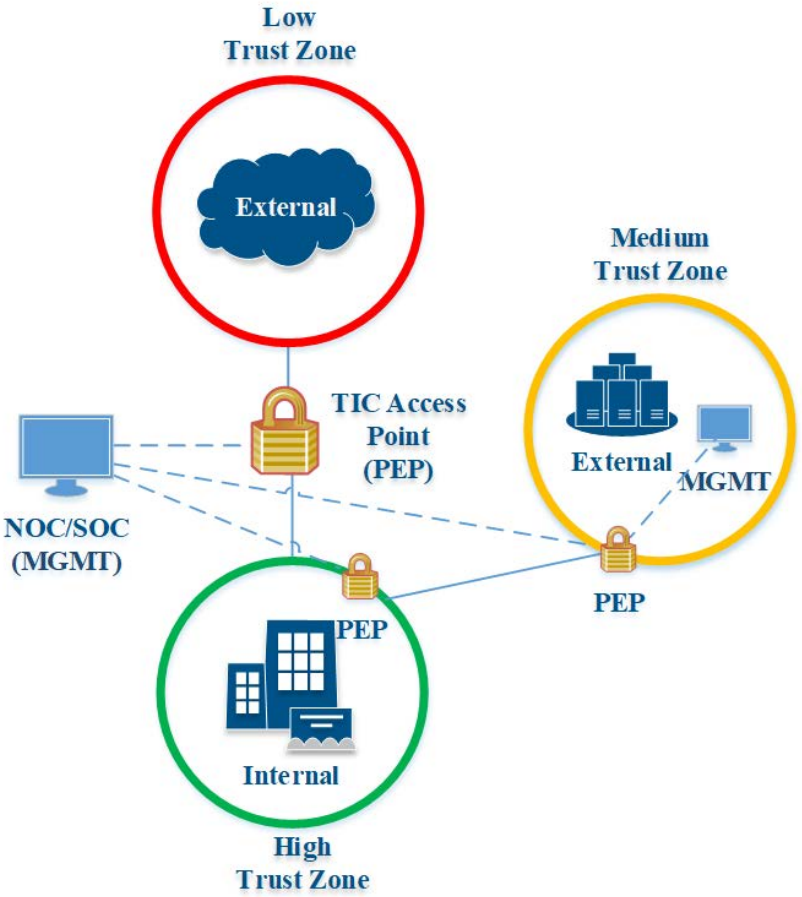
TIC Strategic Program Goals

1. Boundary-Focused
2. Descriptive, Not Prescriptive
3. Risk-Based
4. Environment-Agnostic
5. Dynamic and Adaptable
6. Automated and Streamlined Verification
7. Delineate TIC and NCPS

2| Reference Architecture

- The **draft** Reference Architecture defines the concepts of the program (Trust Zones, PEPs, MGMT) to guide and constrain the diverse implementations of the security capabilities
- Introduces a solid technical foundation that provides a baseline for TIC Use Cases

TIC 3.0 Example Trust Zone Diagram



3| Security Capabilities Handbook

- The **draft** Security Capabilities Handbook provides a list of security objectives, controls, capabilities, and best practices
- Intended to keep pace with the evolution of policy and technology
- Capabilities will be continuously evaluated and expanded upon

TIC 3.0 Security Objectives

- Manage Traffic
- Protect Traffic Confidentiality
- Protect Traffic Integrity
- Ensure Service Resiliency
- Ensure Effective Response

Security Capabilities Application

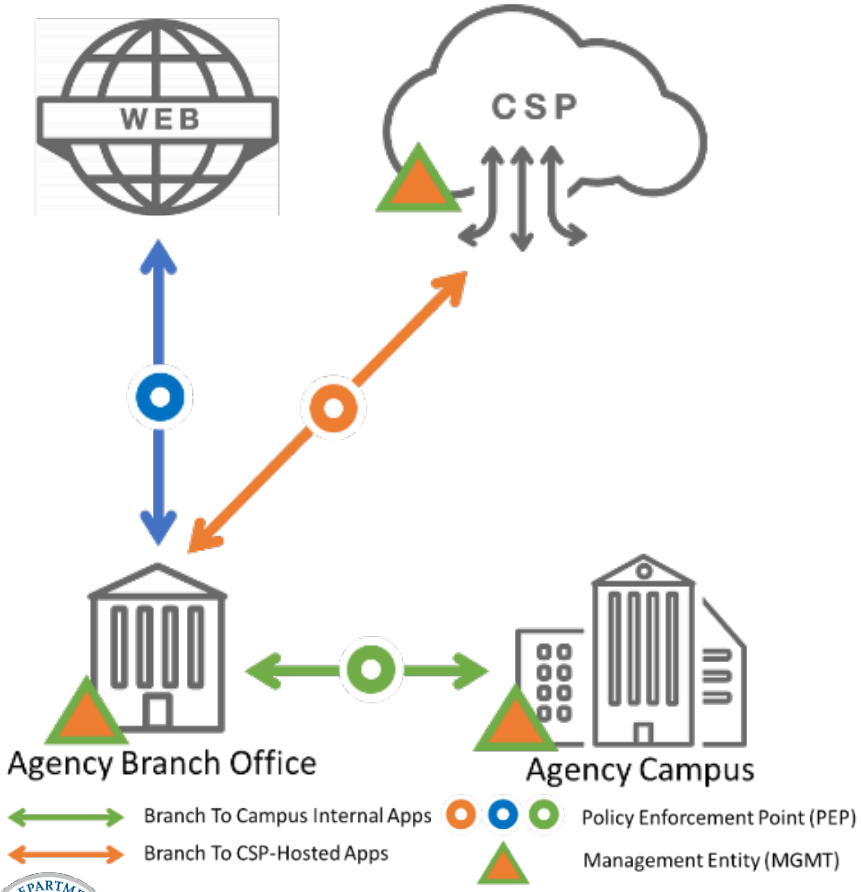
- There are two types of security capabilities:
  - **Universal** (enterprise-level and apply across use cases)
  - **Policy Enforcement Point** (network-level and apply to specific use cases)
- Agencies should determine the level of rigor required for each security capability with the following considerations:
  - Trust criteria (presented in the Reference Architecture)
  - Federal guidelines
  - Risk tolerance
- Agencies have discretion to position capabilities:
  - In the communication path
  - At endpoints
  - At trust zone boundaries
  - Through service providers

4| Use Case Handbook & Use Cases

- The **draft** TIC Use Case Handbook introduces use cases, which describe an implementation of TIC for each identified use
- Published use cases (branch office and traditional TIC) reflect current architectures
- CISA and Federal CISO Council TIC Subcommittee will continue to develop additional use cases (partner networks, zero trust, etc.) over time

Branch Office Use Case Example

Branch Office Conceptual Architecture



The branch office use case defines how network and multi-boundary security should be applied when an agency has personnel in more than one physical location

Use case contains:

- Conceptual architecture
- Security capabilities
- Security patterns
- Telemetry requirements

CISA
CYBER+INFRASTRUCTURE

Branch Office Security Capabilities

Universal Security Capabilities

Capability	Use Case Guidance*
Secure Administration	Branch office system components may not permit the same out-of-band administration as…
Strong Authentication	Agencies must ensure branch office functions with the same authentication protections as…
Time Synchronization	Agencies should consider whether the branch office component time synchronization occurs against…
Vulnerability Assessment	The assessment should explicitly consider the case where communication between the…
Resilience	The Branch Office Use Case presents the agency with the option to depend upon centralized…
Policy Enforcement Parity	When branch office locations are configured to permit connections to CSP and Web services directly…

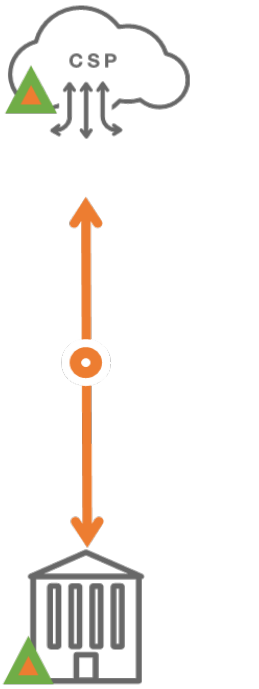
PEP Security Capabilities

PEP Capability Group	Inclusion Justification and Implementation Guidance*
Files	Branch office users will perform information exchanges utilizing file transfers. The…
Web	Branch locations may have specialized roles that permit a more granular approach to…
Networking	Connectivity from the branch location to all other resources must be done utilizing all feasible security mechanisms. Traffic…
DNS	While it is unlikely an agency will be hosting authoritative name services from a branch location, the agency should ensure…
Intrusion Detection	Branch locations may have specialized roles that permit a more fine/granular approach to enforcement of IDS protections. Agencies…
Enterprise	VPN services provide bulk data encryption between network devices for given source/destination locations.

*Use case guidance provided for illustrative purposes only. Refer to Branch Office Use Case for complete information.

Branch Office to CSP Security Pattern

Direct From Branch Office
Direct connect, Express route, TLS, VPN, etc.



Option 1

Hairpin Back Through Campus
Shared path with Security Pattern 3,
but with new final destination

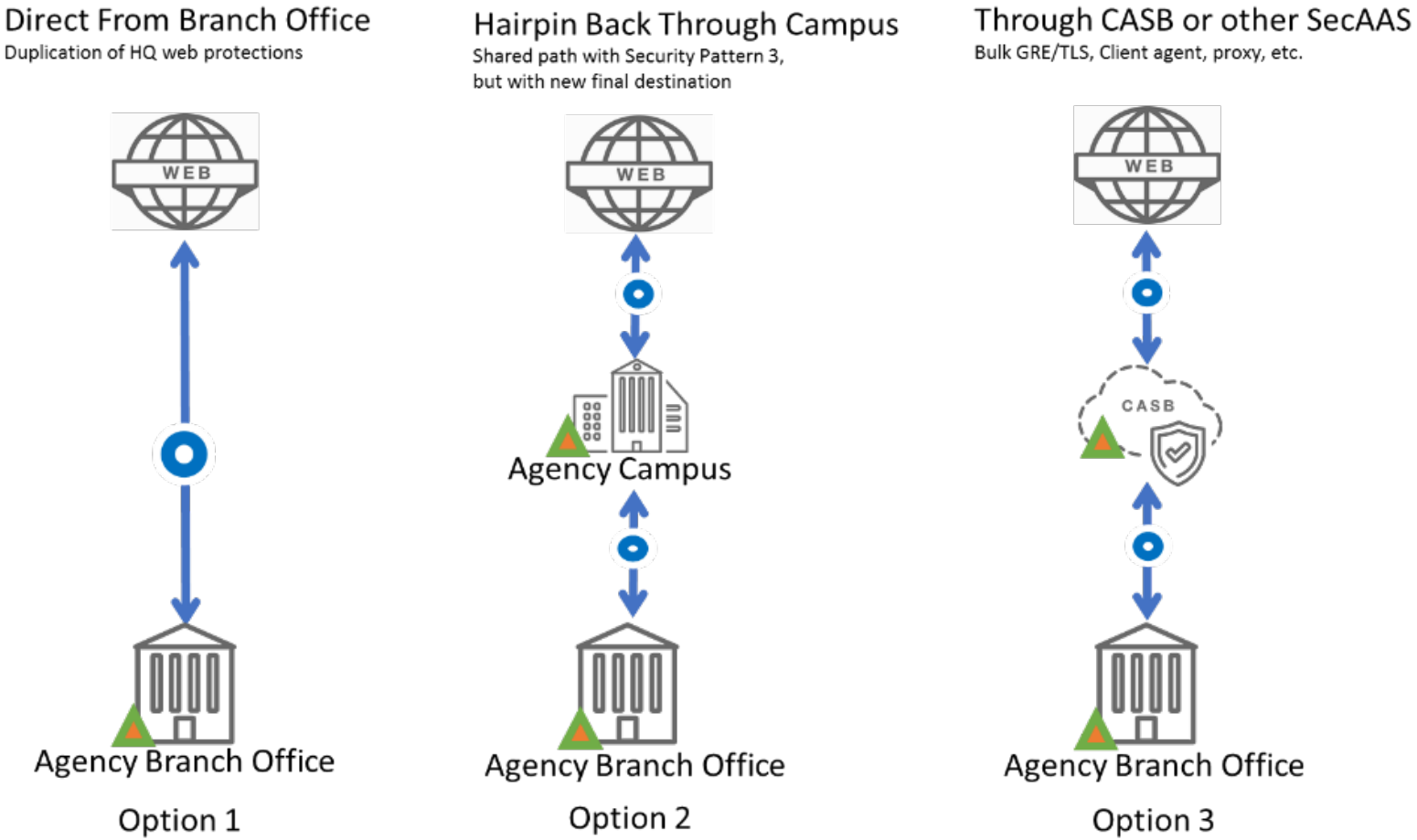
Option 2

Through CASB or other SecAAS
Bulk GRE/TLS, Client agent, proxy, etc.

Option 3

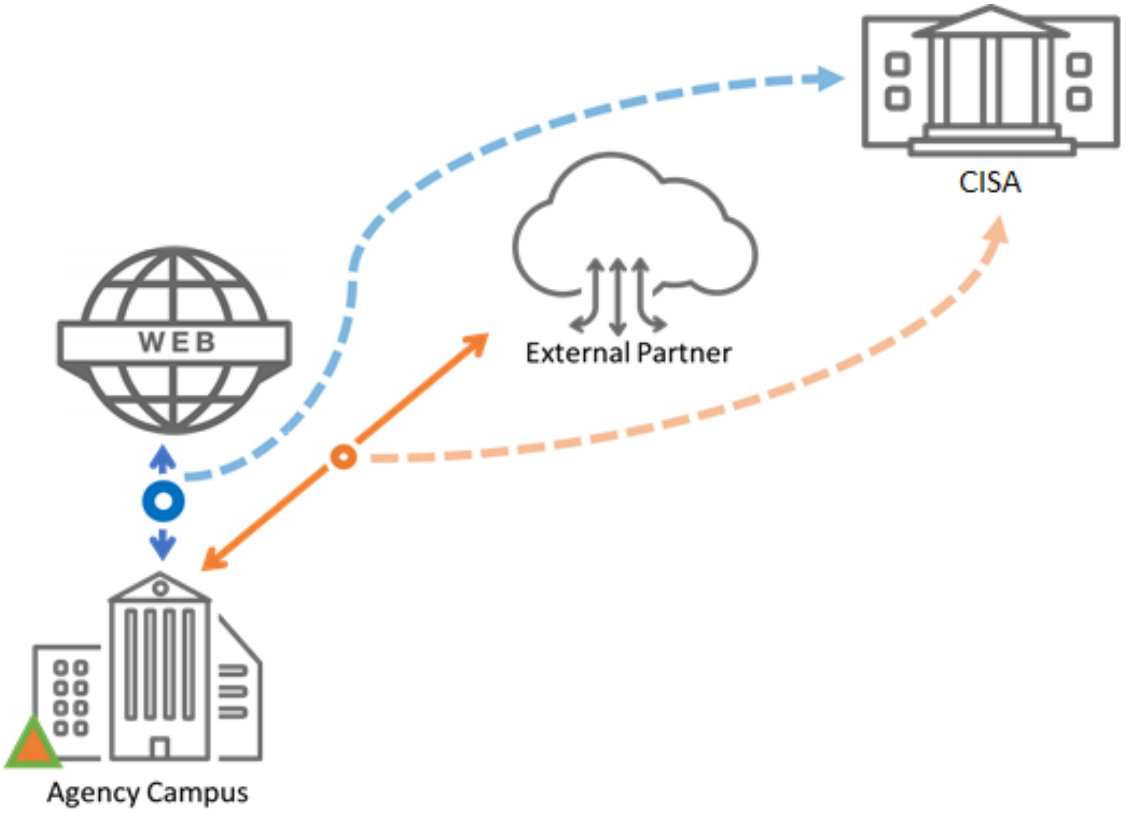
Applicable capabilities are articulated for each security pattern

Branch Office to Web Security Pattern



Capabilities are positioned according to agency discretion

Branch Office Telemetry Sharing



Telemetry diagram provided for illustrative purposes only. Refer to NCPS Cloud Interface RA for complete information.

5| Service Provider Overlay Handbook

- The **draft** Service Provider (SP) Handbook introduces overlays, which are high-level mappings of a vendor's security functions to the TIC capabilities
- Overlays were developed to address use case limitations, but they are independent of the use cases and do not map to any specific use case
- Mappings may be imprecise since a vendor's security solution may not map exactly to a TIC security capability
- CISA will adjudicate overlays and post to GitHub as they become available

Service Provider Overlay Examples

TIC Overlay for Azure*

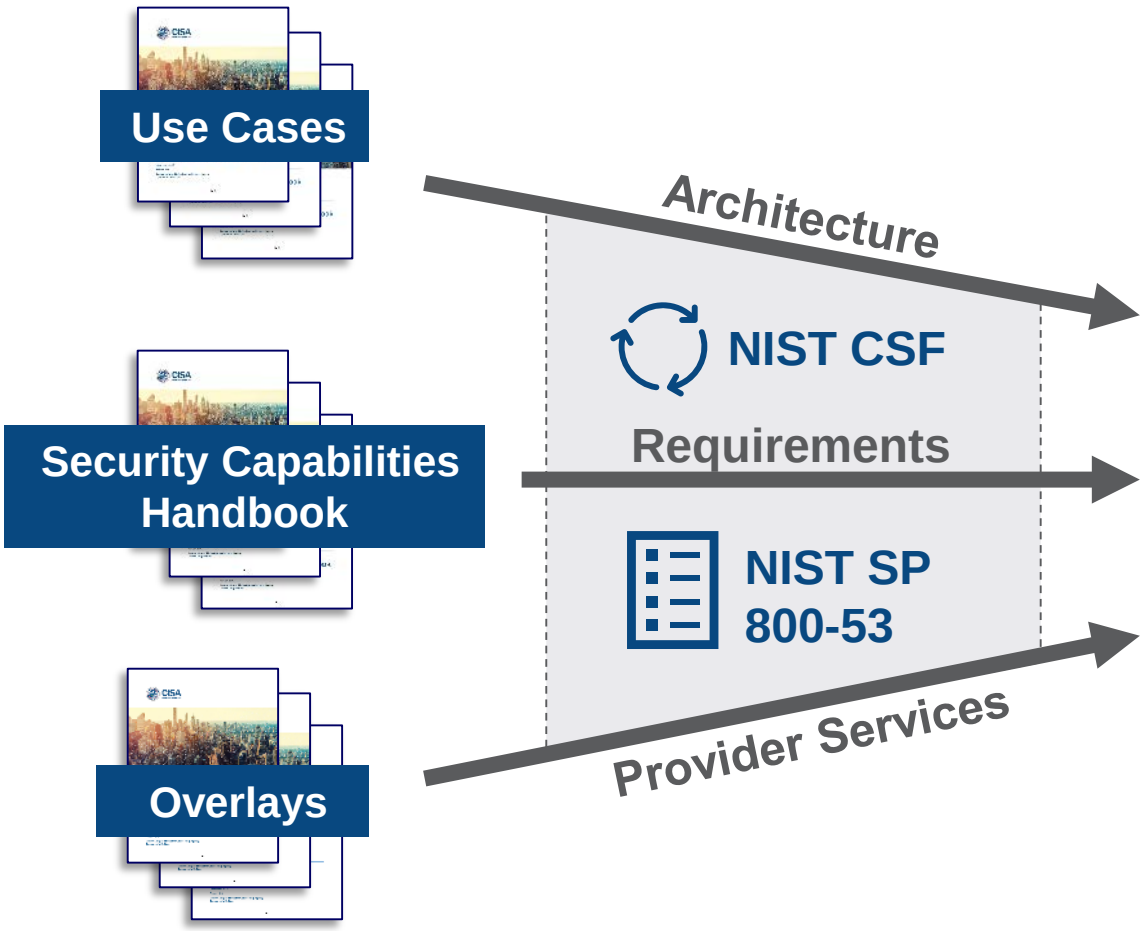
TIC Capabilities	Traditional On-Prem TIC Access Point	Azure Services
Restrict	Firewall & ACLs	Network Security Groups (NSG)
Detect	IPS/IDS	***3rd Party Only***
Restrict	Web Application Firewall (WAF)	Application Gateway
Monitor	SIEM Log Analytics	Advanced Log Analytics Azure Monitor
Identity	Privileged Access Management (PAM)	Azure AD Privileged Identity Management
Detect	Data Loss Prevention (DLP)	Information Protection (AIP)

TIC Overlay for AWS*

TIC Capabilities	Traditional On-Prem TIC Access Point	AWS Services
Restrict	Firewall & ACLs	Security Groups AWS Network ACLs
Detect	IPS/IDS	***3rd Party Only***
Restrict	Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager
Monitor	SIEM Log Analytics	AWS Security Hub Amazon GuardDuty
Identity	Privileged Access Management (PAM)	***3rd Party Only***
Detect	Data Loss Prevention (DLP)	Amazon Macie

*Overlays provided for illustrative purposes only. Refer to vendor overlays for complete information.

Implementing TIC 3.0 Guidance



Agency Risk Management

- Architectural Documents
- System Design Documents
- Security Documents
- Acquisition Documents
- Key Artifacts (A&A)

CISA CYBER+INFRASTRUCTURE

TIC Future

Updated Document Release

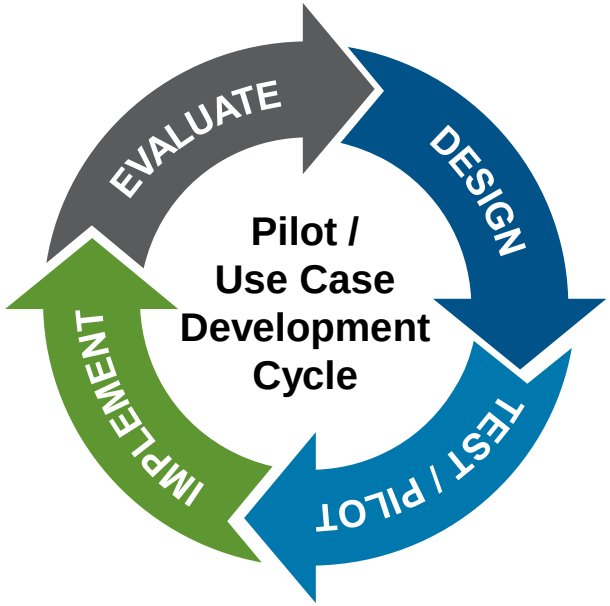
Finalized documents will be released Spring 2020

Agency Interpretation

- Agencies are expected to incorporate guidance into their risk management strategy
- Guidance is intentionally abstract, high-level, and theoretical to provide agencies with flexibility to interpret guidance to suit their needs
- Agencies should determine if protections are commensurate with the level of risk pertaining to their computing scenarios
- TIC PMO is collaborating with Continuous Diagnostics & Mitigation (CDM) program to develop a validation process

Next-Gen Tech Adoption Prioritization

- Pilots will enable agencies to prioritize the adoption of next-generation technologies
- Perpetual pipeline of pilots will ensure continuous learning and updating of guidance
- DevOps approach (build, test, release) will facilitate faster production of options
- Central repository will be available to stakeholders



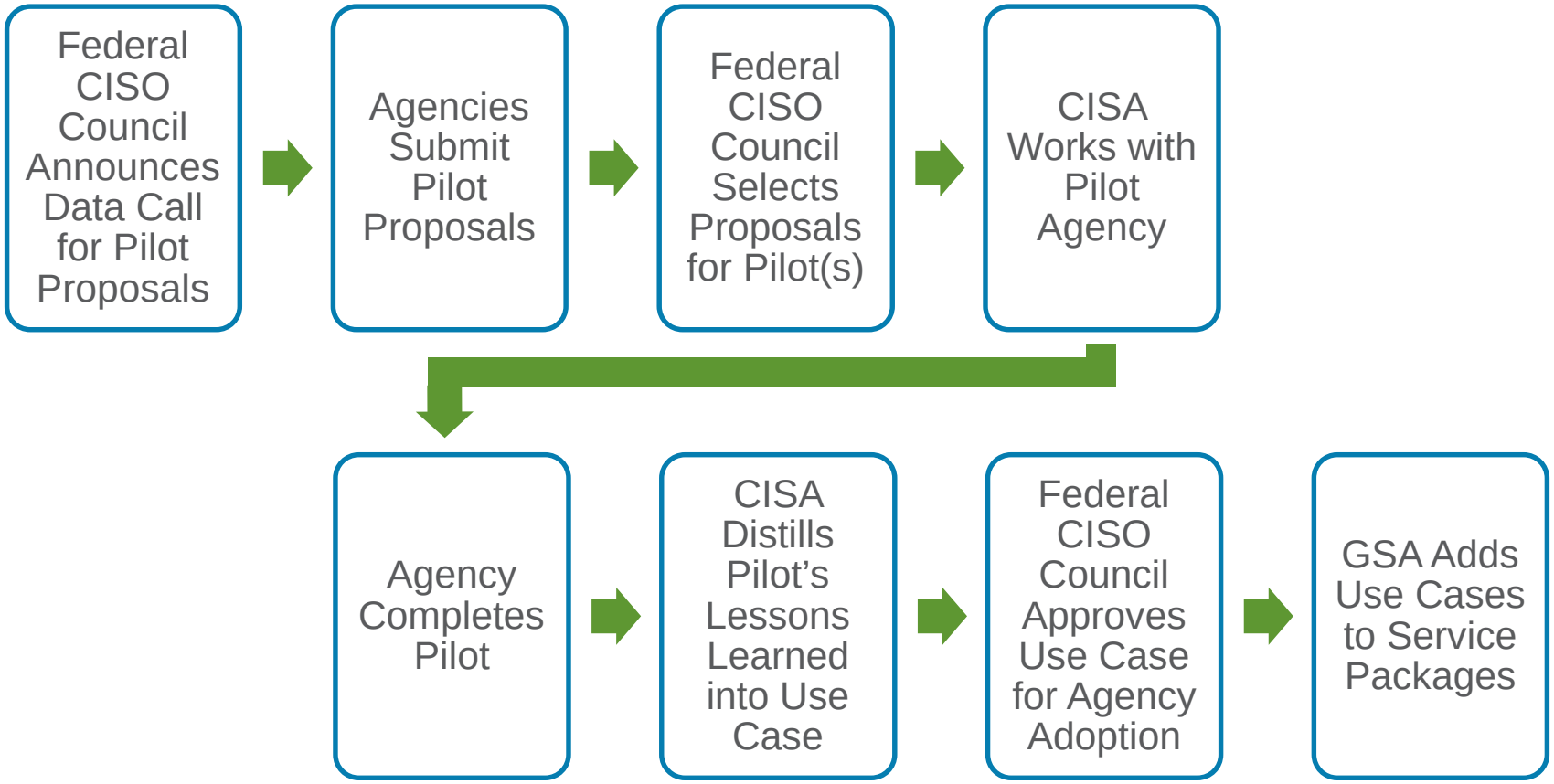
TIC Pilots – Overview

Pilot Stakeholders

- Sponsoring Agency
- OMB
- Federal CISO Council
- GSA
- CISA

TIC pilots will use real world implementation test cases to identify solutions for securing new types of environments

TIC Pilots – Process



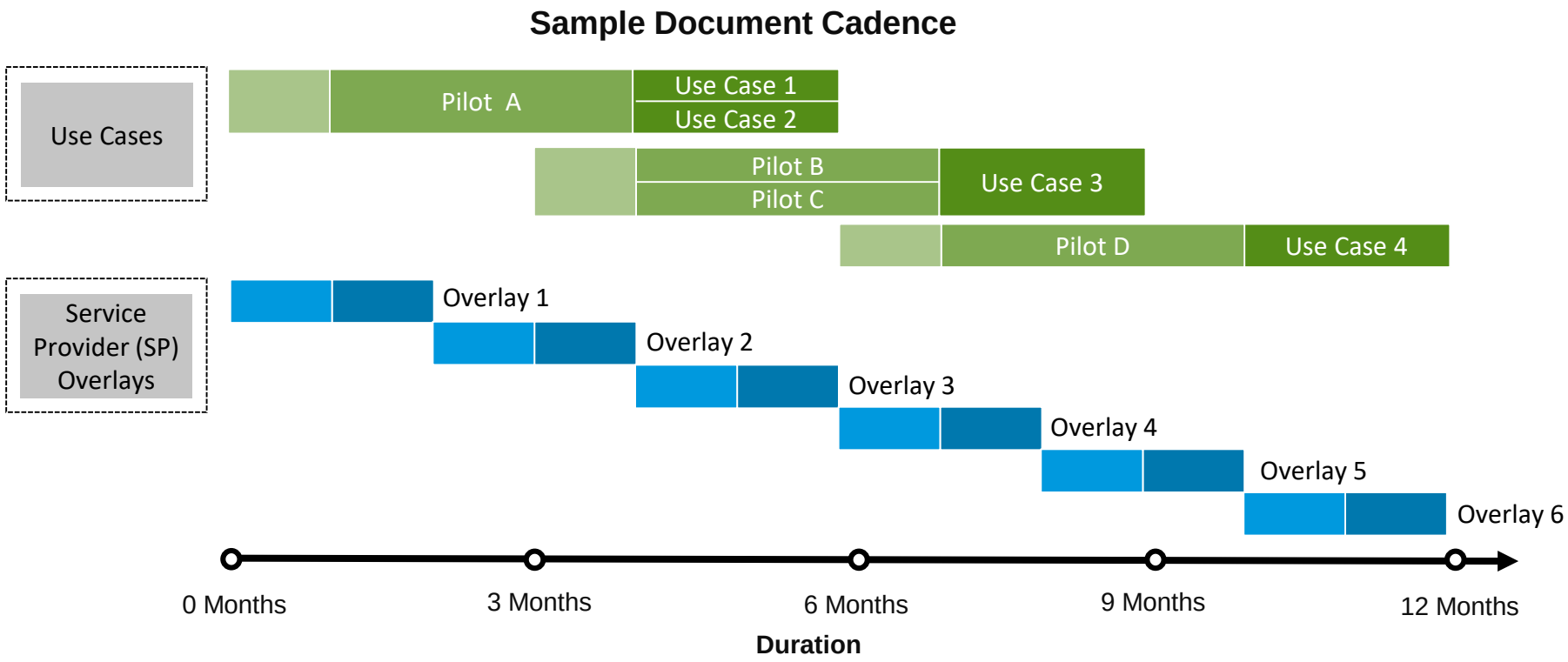
Process provided for illustrative purposes only. Refer to Pilot Process Handbook for complete information.

TIC Pilots – Agency Participation

- CISA is seeking agencies to actively participate in pilots
- Agencies should submit Pilot Proposals to the Federal CISO Council
- A TIC 3.0 pilot should test the configuration and security capabilities of a technology in an agency's environment
- Upon completion of a pilot, CISA will collect and analyze lessons learned from the sponsoring agency

TIC 3.0 Use Case & Overlay Cadence

Use cases and overlays can be developed at different paces



CISA CYBER+INFRASTRUCTURE

Anticipated Use Cases

OMB M-19-26 Use Cases

- Traditional TIC
- Cloud:
  - Infrastructure as a Service
  - Software as a Service
  - Email as a Service
  - Platform as a Service
- Branch Office
- Remote Users

Potential Use Cases

- Zero Trust
- Internet of Things (IoT)
- Zero Trust
- Partner Networks
- Zero Trust
- GSA Enterprise Infrastructure Solutions (EIS)
- Zero Trust
- Unified Communications

TIC 2.0 vs Zero Trust

TIC 2.0

- Perimeter-based strategy
- Network focused
- Host-agnostic
- Consolidation/control of networks
- Relies on tools/sensors on the network

Zero Trust

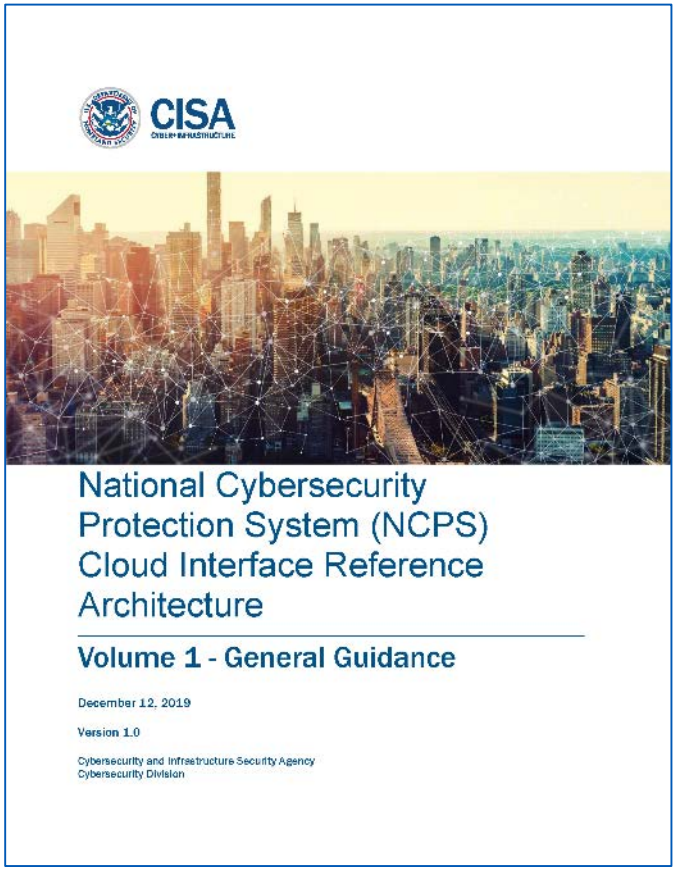
- Data protection strategy
- Endpoint focused
- Network-agnostic
- Networks are suspect
- Relies on APIs/agents on the endpoints

TIC 3.0 & Zero Trust

- Independent Zero Trust Architecture (ZTA) efforts going on for over a year
- TIC 3.0 aligns with ZTA goals & objectives
- OMB, NIST, GSA, and CISA have been meeting with agencies and vendors for the last year
- There is enough critical mass to begin and formalize ZTA towards TIC 3.0
- Zero Trust is not a complete enterprise solution for federal enterprises (yet)

TIC & NCPS

- NCPS released **draft** Cloud Interface Reference Architecture
- Agencies should refer to document for telemetry requirements
- Contact NCPS for additional information



GSA EIS Support for Modernization

- The *Report to the President on Federal IT Modernization* identified EIS as a primary acquisition vehicle for government IT modernization
- EIS encourages SD-WAN, Zero Trust, 5G/IoT and cloud-based security solutions
- Security “building blocks” are already in the contract to create new solutions
- GSA and CISA will work with Industry to establish baseline solution sets once new services reach a maturity level

GSA EIS Support for TIC Policy Update

Managed Network Services

- SD-WAN
- Secure connections to cloud services

Managed Security Services

- Managed Prevention Service (MPS)
- Vulnerability Scanning Service (VSS)
- Incident Response Service (INRS)

TIC 2.2/MTIPS

- MTIPS remains available as a baseline package

SaaS-based tools

Flexibility to update existing and add new cybersecurity services as needed in response to evolving threats

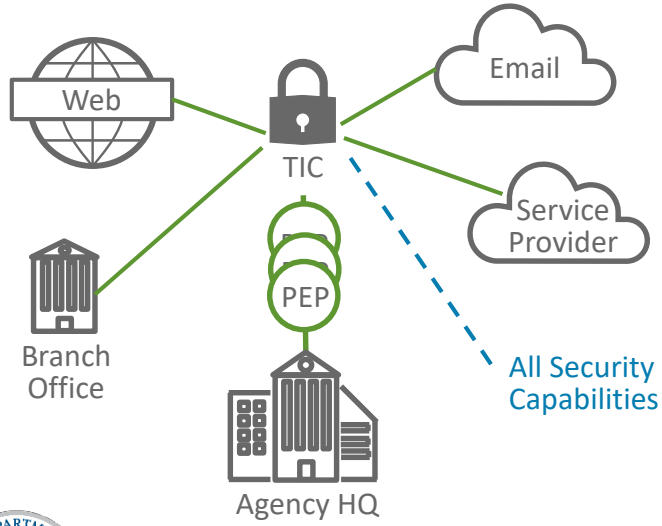
Future of the Federal Enterprise

- Data centers are no longer the center of the enterprise
- The federal enterprise of tomorrow will support:
  - More work performed off of the enterprise network than on it
  - More workloads running in the cloud than at data centers
  - More traffic destined to the cloud than to data centers
  - More traffic from branch offices going directly to the cloud than to the enterprise

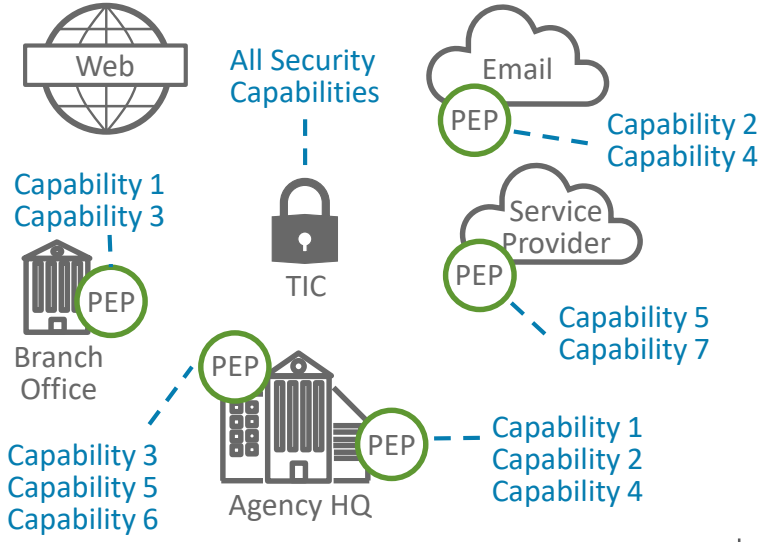
TIC & Future Federal Enterprise

- The flexibility provided by TIC 3.0 can be used to shape the federal enterprise of the future
- TIC 3.0 allows agencies to place security capabilities closer to the data, and not force the rerouting of data to the inspection sensors

TIC 2.2 (Consolidated Architecture)



TIC 3.0 (Distributed Architecture)



CISA CYBER+INFRASTRUCTURE

TIC Future Goals

The TIC initiative will continue to evolve to support its core goals:

- Empower enterprise CIOs and CISOs
- Motivate all agencies towards a stronger cyber-posture
- CISA to weaken exfiltration activities across .gov

By remaining committed to these goals, TIC will ensure it continues to provide visibility into network traffic while enabling agencies to secure their ever fluctuating boundaries and perimeters

NEXT STEPS

Request for Comments

Agencies are encouraged to answer RFC questions:

1. How does your agency expect to utilize the updated TIC guidance to modernize and secure its environments?
2. How does your agency expect to adopt the TIC Use Cases?
3. Does your agency have any suggestions for other use cases?
4. Are there additional documents or artifacts that would be helpful to agencies when implementing the TIC guidance?

Comments addressing these questions should be submitted via the issue submission form on GitHub (https://github.com/cisagov/tic3.0/issues/new) or via email at tic@cisa.dhs.gov. **All comments should be submitted by February 7, 2020**.

CISA
CYBER+INFRASTRUCTURE

Questions?

Contact TIC PMO at
tic@cisa.dhs.gov