# TRUSTED INTERNET CONNECTIONS

## NIST INFOSEC & PRIVACY ADVISORY BOARD TIC 3.0 WEBINAR

Sean Connelly
June 24, 2020

# Agenda

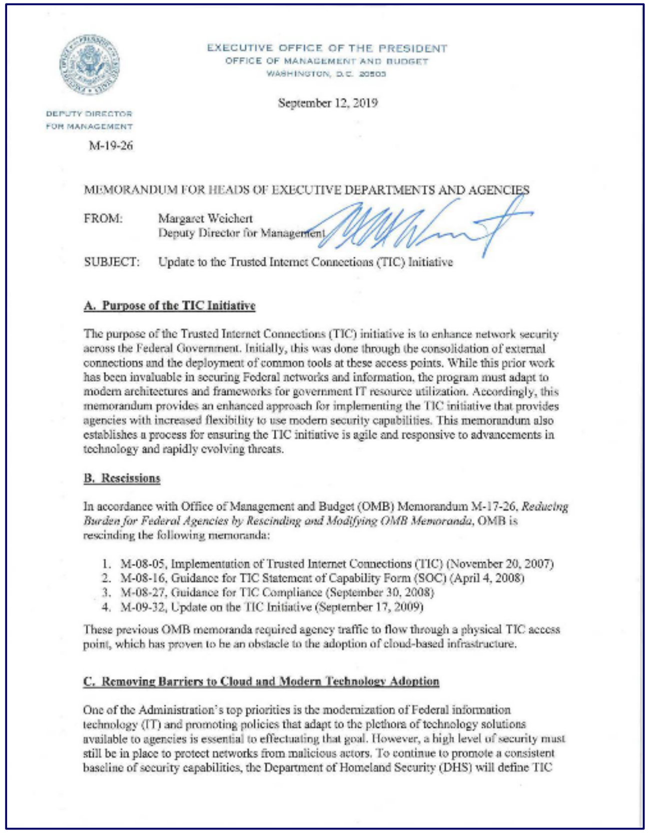
- Background
- Telework Security Challenges
- TIC 3.0 Interim Telework Guidance Overview
- Service Provider Engagement
- Next Steps

# Background

# OMB Update to the TIC Program

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.
- Requires program to be agile and responsive.
- Focus is towards strategy, architecture, and visibility.



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**

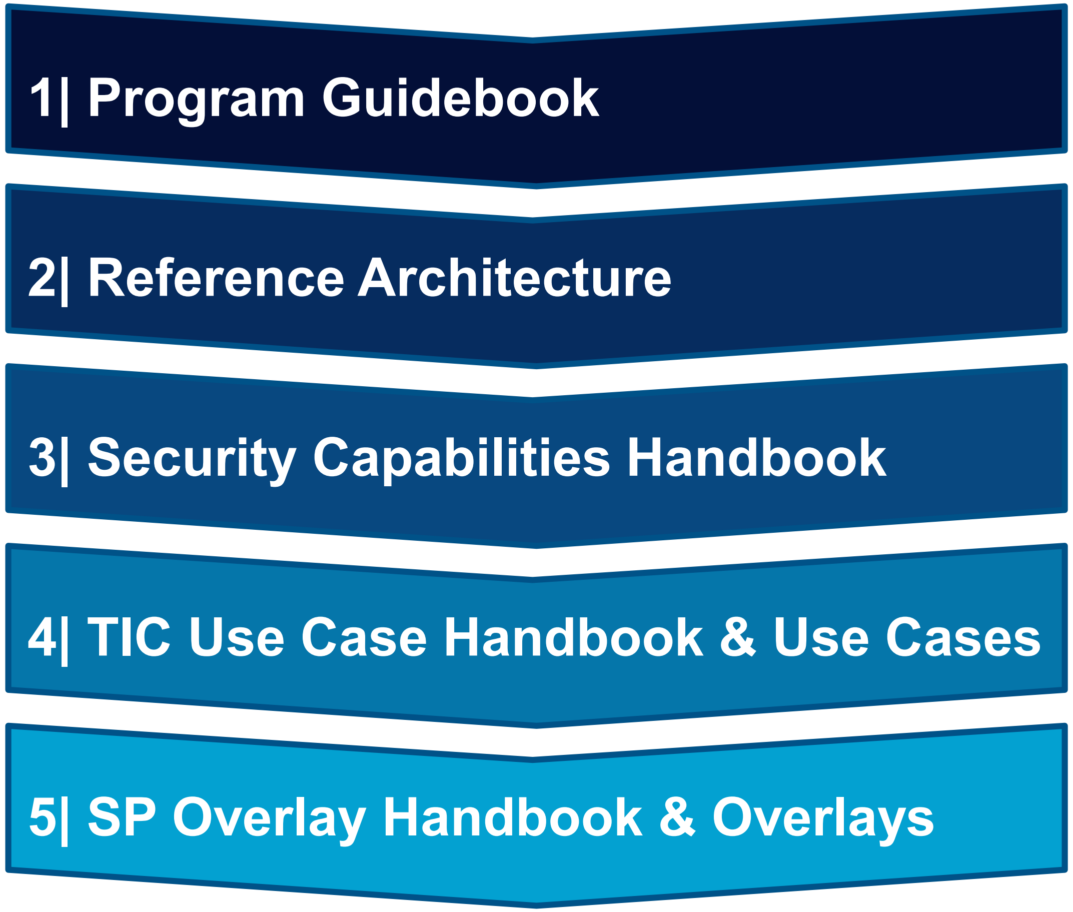
One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect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

# Updates to IT Mod Initiatives

Advancements in related IT Modernization programs and initiatives:

- **NIST SP 800-207 – Zero Trust Architecture**
  - Provides guidance for zero trust and zero trust architectures.
- **GSA Enterprise Infrastructure Solutions (EIS) Acquisition Vehicle**
  - Encourages SD-WAN, zero trust, 5G/Internet of Things (IoT) and cloud-based security solutions.
- **CISA**
  - **National Cybersecurity Protection Service (NCPS)**
    - Piloting Cloud Log Aggregation Warehouse (CLAW) for cloud telemetry.
  - **Continuous Diagnostics and Mitigation (CDM)**
    - Piloting the monitoring of agency cloud environments.

# Key TIC 3.0 Program Documents



1| Program Guidebook

2| Reference Architecture

3| Security Capabilities Handbook

4| TIC Use Case Handbook & Use Cases

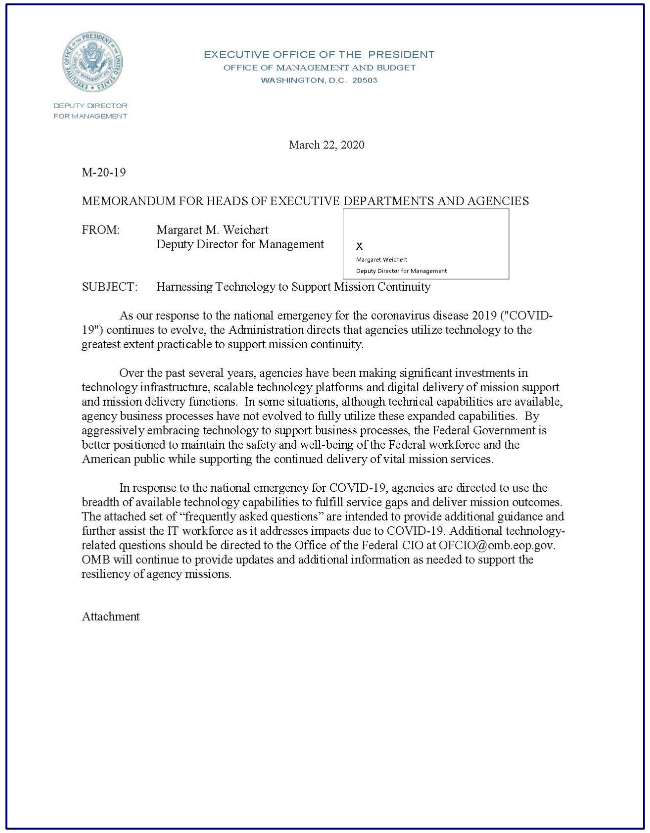
5| SP Overlay Handbook & Overlays

- Key program documents constitute core TIC 3.0 program guidance.
- Draft documents released December 2019.

# OMB Memorandum M-20-19

OMB Memorandum M-20-19 released March 2020.

- *Harness Technology to Support Mission Continuity*
- Encourages agencies to leverage approved collaboration tools and capabilities.
- Advises agencies to make risk-based security decisions.



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

DEPUTY DIRECTOR
FOR MANAGEMENT

March 22, 2020

M-20-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret M. Weichert
Deputy Director for Management

X
Margaret Weichert
Deputy Director for Management

SUBJECT: Harnessing Technology to Support Mission Continuity

As our response to the national emergency for the coronavirus disease 2019 ("COVID-19") continues to evolve, the Administration directs that agencies utilize technology to the greatest extent practicable to support mission continuity.

Over the past several years, agencies have been making significant investments in technology infrastructure, scalable technology platforms and digital delivery of mission support and mission delivery functions. In some situations, although technical capabilities are available, agency business processes have not evolved to fully utilize these expanded capabilities. By aggressively embracing technology to support business processes, the Federal Government is better positioned to maintain the safety and well-being of the Federal workforce and the American public while supporting the continued delivery of vital mission services.

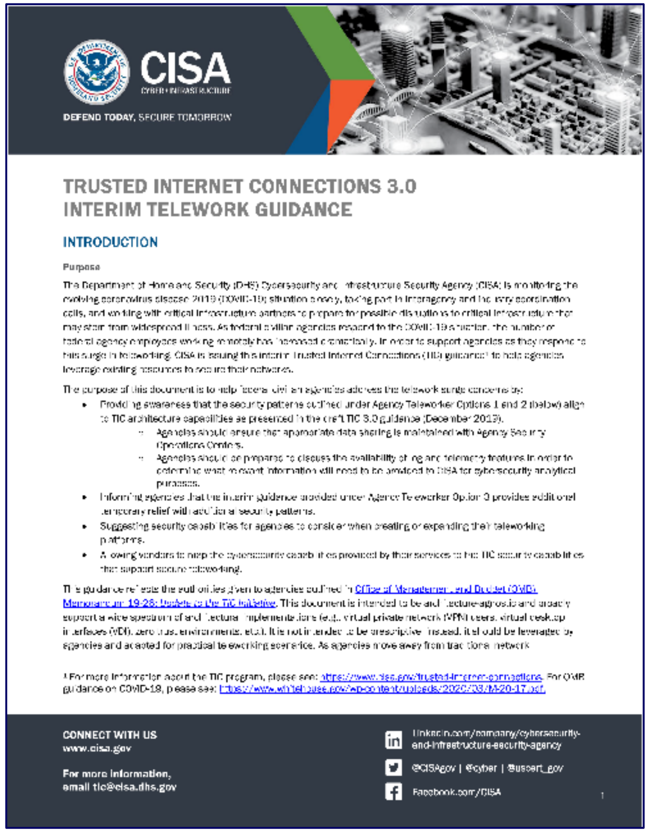
In response to the national emergency for COVID-19, agencies are directed to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes. The attached set of "frequently asked questions" are intended to provide additional guidance and further assist the IT workforce as it addresses impacts due to COVID-19. Additional technology-related questions should be directed to the Office of the Federal CIO at OFCIO@omb.eop.gov. OMB will continue to provide updates and additional information as needed to support the resiliency of agency missions.

Attachment

# TIC 3.0 Interim Telework Guidance

TIC 3.0 Interim Telework Guidance released April 2020.

- Developed to support OMB M-20-19 and current telework surge.
- Addresses telework security challenges.
- Discretionary and not part of core TIC program guidance.
- Valid for Calendar Year (CY) 2020 only and deprecated by Remote User Use Case by year end.



CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW

## TRUSTED INTERNET CONNECTIONS 3.0 INTERIM TELEWORK GUIDANCE

### INTRODUCTION

**Purpose**

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is monitoring the evolving coronavirus disease 2019 (COVID-19) situation closely, taking part in interagency and industry coordination calls, and working with critical infrastructure partners to prepare for possible disruptions to critical infrastructure that may stem from widespread illness. As federal civilian agencies respond to the COVID-19 situation, the number of federal agency employees working remotely has increased dramatically. In order to support agencies as they respond to this surge in teleworking, CISA is issuing this interim Trusted Internet Connections (TIC) guidance[1] to help agencies leverage existing resources to secure their networks.

The purpose of this document is to help federal civilian agencies address the telework surge concerns by:

- Providing awareness that the security patterns outlined under Agency Teleworker Options 1 and 2 (below) align to TIC architecture capabilities as presented in the draft TIC 3.0 guidance (December 2019).
  - Agencies should ensure that appropriate data sharing is maintained with Agency Security Operations Centers.
  - Agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant information will need to be provided to CISA for cybersecurity analytical purposes.
- Informing agencies that the interim guidance provided under Agency Teleworker Option 3 provides additional temporary relief with additional security patterns.
- Suggesting security capabilities for agencies to consider when creating or expanding their teleworking platforms.
- Allowing vendors to map the cybersecurity capabilities provided by their services to the TIC security capabilities that support secure teleworking.

This guidance reflects the authorities given to agencies outlined in Office of Management and Budget (OMB) Memorandum 19-26: Update to the TIC Initiative. This document is intended to be architecture-agnostic and broadly support a wide spectrum of architectural implementations (e.g., virtual private network (VPN) users, virtual desktop interfaces (VDI), zero trust environments, etc.). It is not intended to be prescriptive. Instead, it should be leveraged by agencies and adapted for practical teleworking scenarios. As agencies move away from traditional network

[1] For more information about the TIC program, please see: https://www.cisa.gov/trusted-internet-connections. For OMB guidance on COVID-19, please see: https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-17.pdf.

CONNECT WITH US
www.cisa.gov

For more information,
email tic@cisa.dhs.gov

linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

1

# Telework Security Challenges

# Telework Surge Impacts

- Workers are geographically dispersed and more reliant on mobile devices.
- Distributed workforce has caused agencies to implement more cloud-based, remote user, and teleconference solutions.
- Agencies are exploring modern architectures to secure their increasingly distributed networks.

# Telework Surge Security Challenges

Traditional perimeter security model is less applicable.

From: Boss
To: Employee
Subject: Urgent Survey !

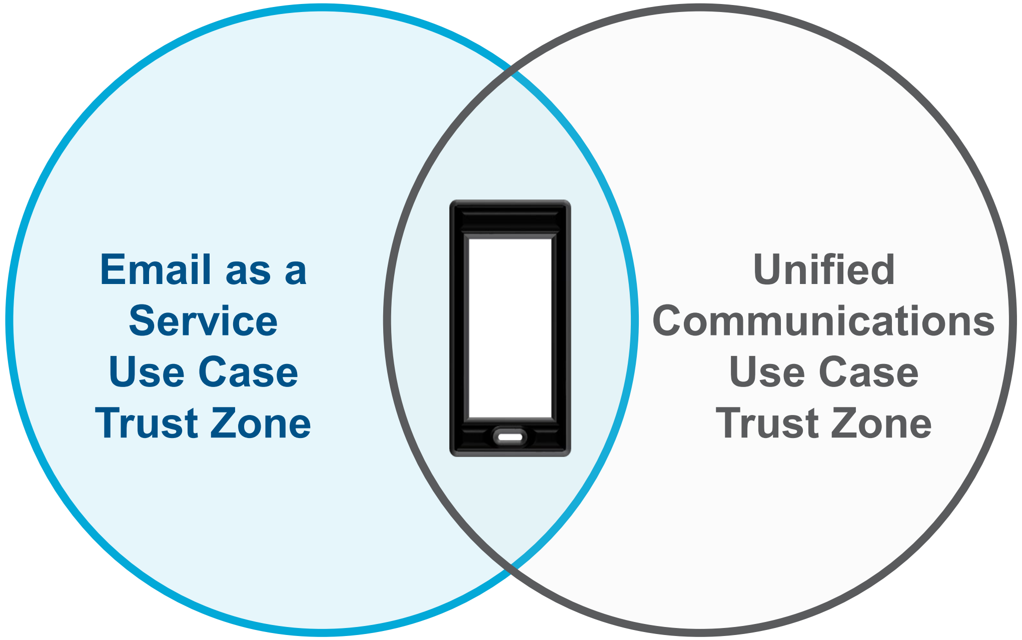
Click Here NOW!

Attacks are increasingly focused on end users.

Trust cannot be assumed.

# Telework Security and Trust Zones

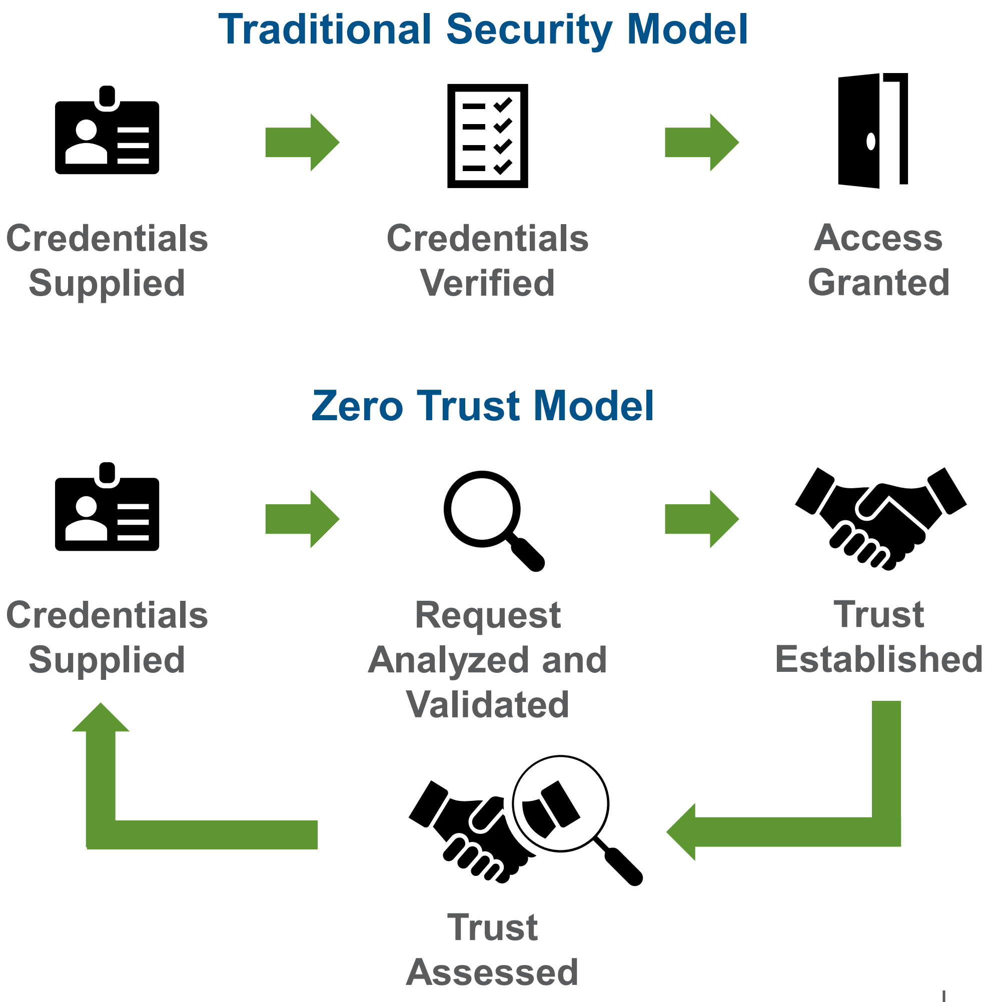
- Trust zones are used to secure network components with similar protection requirements.
- Segmenting networks into trust zones and enforcing traffic between zones helps prevent lateral network movement.
- A single network component, like a mobile device, can be included in different trust zones for different use cases.


Email as a Service Use Case Trust Zone
Unified Communications Use Case Trust Zone

Notional use cases provided for illustrative purposes only.

# Telework Security & Zero Trust

- Zero Trust assumes all users and access requests are suspect.
- Trust has a half-life.
- Trust is established and reestablished by:
  - Robust Identity, Credential, and Access Management (ICAM);
  - Access Controls;
  - Network Analysis;
  - Telemetry; and
  - Threat Intelligence.



Traditional Security Model

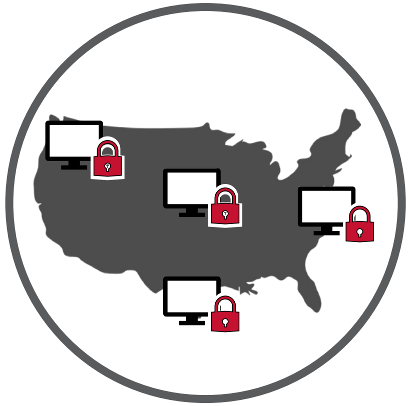
Zero Trust Model

# Telework Guidance & Architectures

- Implementing zero trust or highly segmented architectures may involve extensive planning, designing, and procurement efforts.
- Interim Telework Guidance accommodates traditional, micro-segmented, and zero trust architectures by providing agencies with the flexibility to place Policy Enforcement Points (PEPs) anywhere in their existing network architecture.

Traditional “Castle” Security Perimeter

Micro-segmented “City” Security Perimeters



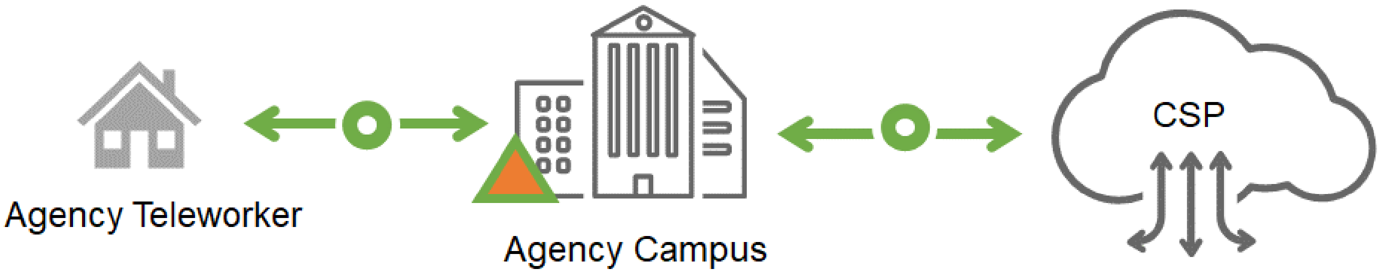
No “Zero Trust” Security Perimeter

# TIC 3.0 Interim Telework Guidance Overview

# Interim Telework Guidance Overview

- Applicable to scenarios in which teleworkers access sanctioned cloud services.
- Broadly supportive of a wide spectrum of architectural implementations including:
  - Virtual Private Network (VPN) users,
  - Virtual Desktop Interfaces (VDI), and
  - Zero Trust environments.
- Provides security patterns and capabilities to support secure teleworking.

# Traditional Telework Security Pattern

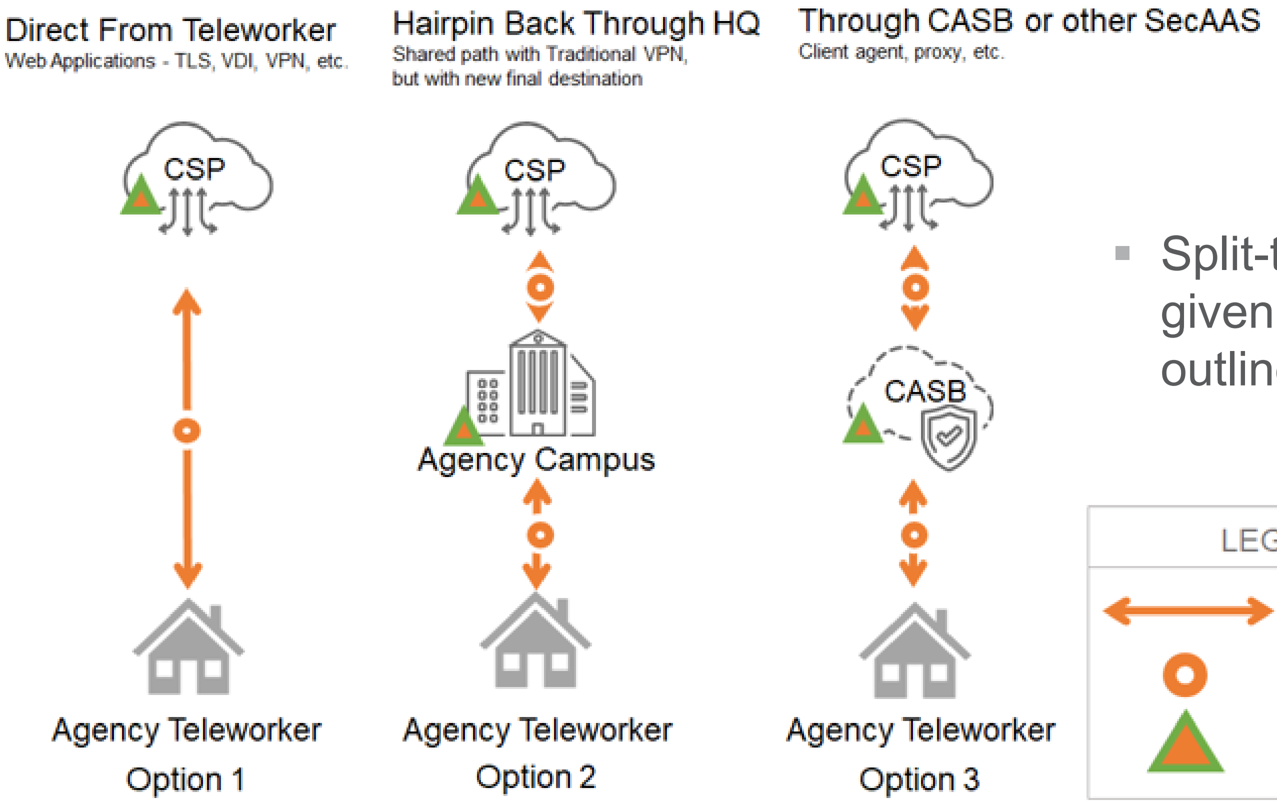


LEGEND

| | |
|---|---|
| ↔ | Teleworker To HQ Internal Apps and CSP-hosted Apps |
| ○ | Policy Enforcement Point (PEP) |
| ▲ | Management Entity (MGMT) |

Capabilities are positioned in centralized location.

# Alternative Telework Security Patterns



Direct From Teleworker
Web Applications - TLS, VDI, VPN, etc.

Hairpin Back Through HQ
Shared path with Traditional VPN,
but with new final destination

Through CASB or other SecAAS
Client agent, proxy, etc.

CSP
CSP
CSP
Agency Campus
CASB
Agency Teleworker Option 1
Agency Teleworker Option 2
Agency Teleworker Option 3

- Split-tunneling acceptable given considerations outlined in guidance.

LEGEND

⟷ Teleworker To CSP-hosted Apps

○ Policy Enforcement Point (PEP)

▲ Management Entity (MGMT)

Capabilities are positioned according to agency discretion.

# Telework Security Capabilities Overview

## Policy Enforcement Point (PEP) Capabilities

- PEP capabilities apply to specific use cases. Telework PEP capabilities are network-level but may evolve in future guidance.
- As architectures move towards a zero-trust solution, there may be a greater reliance on authentication mechanisms to validate remote users and protect data.
- Telework surge-specific capabilities are included for Data Protection and Unified Communications and Collaboration.

## Universal Capabilities

- Universal capabilities are enterprise-level and apply across use cases.
- Agencies should review each capability, and corresponding implementation guidance, to consider how a surge in telework affects changes to their enterprise.

# PEP Telework Security Capabilities

## PEP Telework Security Capabilities

### Files

- Anti-malware

### Email

- Anti-phishing Protections
- Data Loss Prevention
- Encryption for Email Transmission
- Malicious URL Protections
- URL Click-Through Protection
- NCPS E$^3$A Email Protections

### Networking

- Network Segmentation
- Micro-segmentation

### DNS

- DNS Blackholing
- DNSSEC for Agency Clients
- DNSSEC for Agency Domains
- NCPS E$^3$A DNS Protections

### Intrusion Detection

- Adaptive Access Control
- Endpoint Detection and Response

### Enterprise Capabilities

- Virtual Private Network
- Application Container
- Remote Desktop Access

### Unified Communications and Collaboration (UCC)

- UCC Identity Verification
- UCC Encrypted Communication
- UCC Connection Termination
- UCC Data Loss Prevention

### Data Protection

- Access Control
- Protections for Data at Rest
- Protections for Data in Transit
- Data Loss Prevention
- Data Access and Use Telemetry

Capabilities should be implemented in accordance with agency risk tolerances.

# Universal Telework Security Capabilities

## Universal Security Capabilities

- Backup and Recovery
- Central Log Management with Analysis
- Configuration Management
- Incident Response Plan and Incident Handling
- Inventory
- Least Privilege
- Secure Administration
- Strong Authentication
- Time Synchronization
- Vulnerability Assessment
- Auditing and Accounting
- Resilience
- Enterprise Threat Intelligence
- Situational Awareness
- Dynamic Threat Discovery
- Policy Enforcement Parity
- Effective Use of Shared Services
- Integrated Desktop, Mobile, and Remote Policies

Capabilities should be implemented in accordance with agency risk tolerances.

# Interim Telework Guidance Caveats

- Guidance is not part of the current core TIC 3.0 document set and does not support an existing TIC 3.0 use case.
- Traffic to public internet should still be routed through TIC access points, including the EINSTEIN sensors.
- Agencies interested in adopting guidance may work with service providers to implement capabilities and discuss telemetry options.

# Service Provider Engagement

# Service Provider Overlays Overview

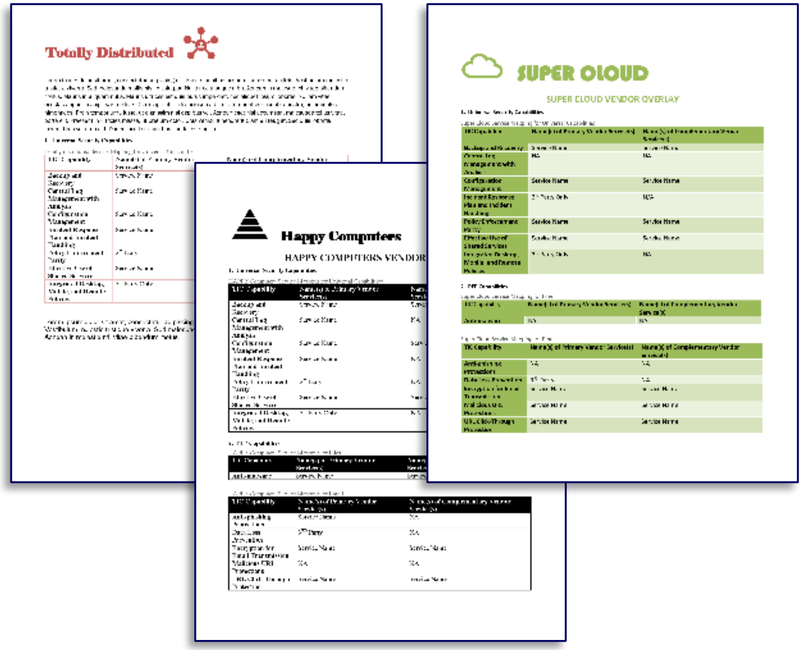
- Interim guidance supplies service providers with sample template for mapping services to TIC telework capabilities.

## Service Provider Overlay Template

Trusted Internet Connections 3.0 Interim Telework Guidance

APPENDIX A: SERVICE PROVIDER OVERLAY

## Notional Service Provider Overlays



Totally Distributed

Happy Computers

HAPPY COMPUTERS VENDOR

SUPER CLOUD

SUPER CLOUD VENDOR OVERLAY

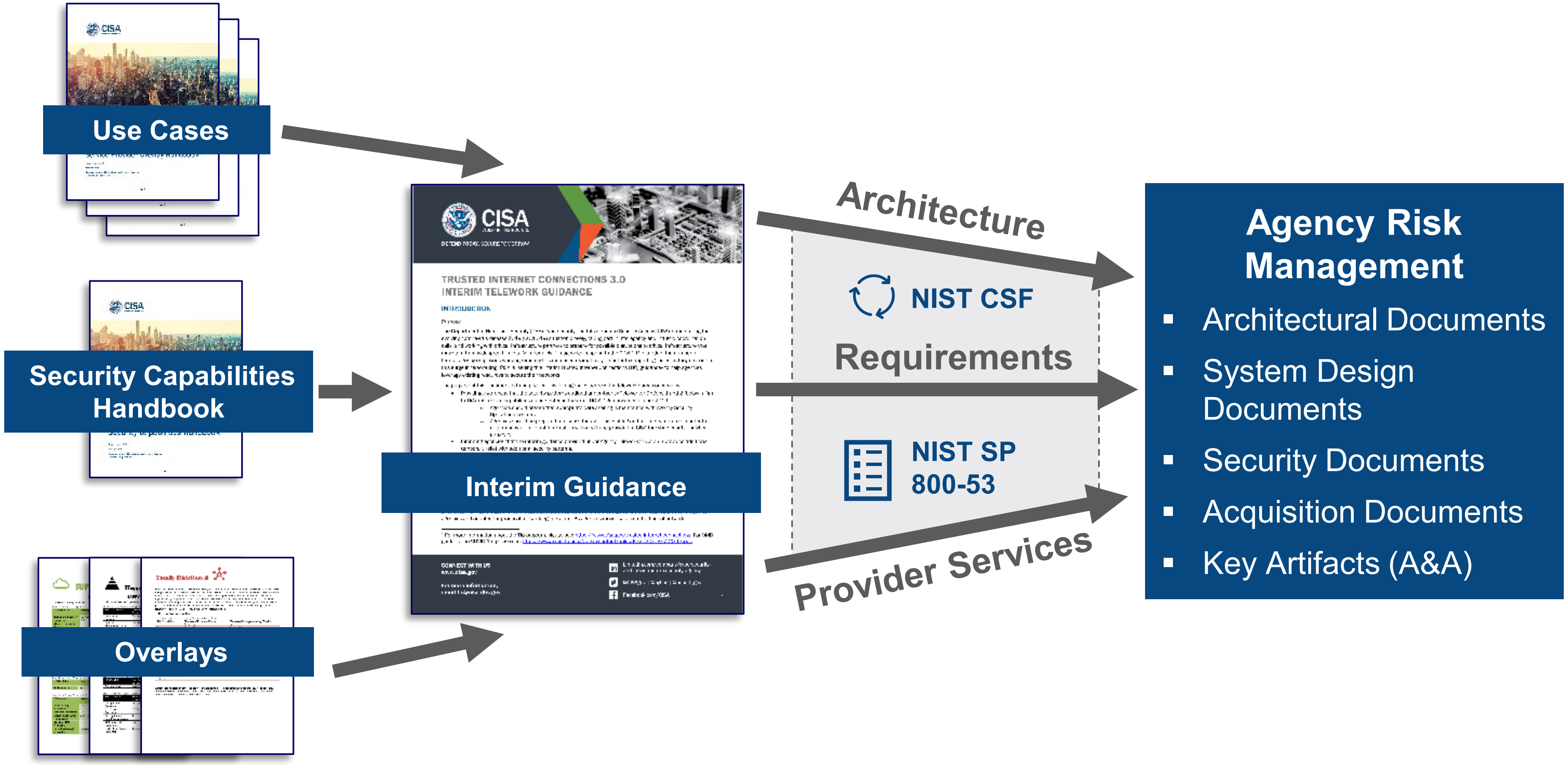
Notional overlays provided for illustrative purposes only.

# Service Provider Overlays Guidance

- Agencies should utilize overlays to understand the coverage, and gaps, offered by a service provider’s products and services.
- Service providers are responsible for producing and distributing overlays.
- Overlays will vary in content and appearance as service providers are expected to customize the CISA template to suit their needs.
- CISA will not adjudicate or endorse overlays, attest to the strength of the mappings, or validate implementations.

# Next Steps

# Implementing Interim Guidance



Use Cases

Security Capabilities Handbook

Overlays

Interim Guidance

Architecture

NIST CSF

Requirements

NIST SP 800-53

Provider Services

**Agency Risk Management**

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

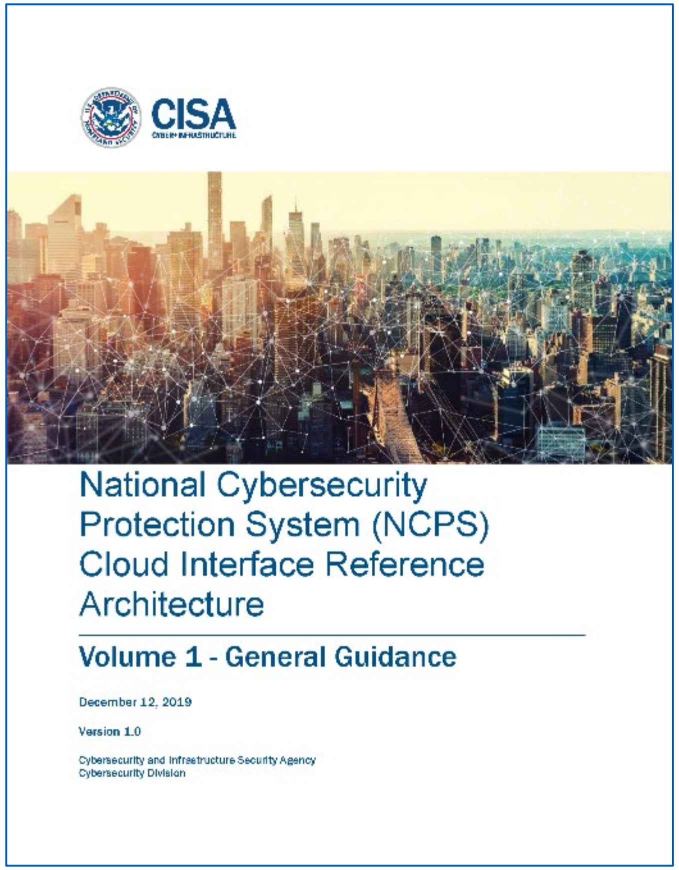
# Final TIC 3.0 Guidance Documents Release

Finalized program documents will be released Summer 2020.

- Current draft documents are available on CISA's TIC web page: www.cisa.gov/trusted-internet-connections.
- Remote User Use Case will not be included in this release.

# TIC & NCPS

- NCPS is evolving to ensure that security information about cloud-based traffic can be captured and analyzed.
- NCPS released **draft** Volume 1 of the Cloud Interface Reference Architecture (CIRA).
- NCPS is actively working to develop Volume 2 of the CIRA.
- Agencies should refer to document for telemetry requirements.
- Contact NCPS for additional information.



CISA
CYBER+INFRASTRUCTURE

National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture

Volume 1 - General Guidance

December 12, 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

# Document Release Phases

## Core Guidance

- Program Guidebook
- Reference Architecture
- Security Capabilities Handbook
- Use Case Handbook
- Service Provider Overlay Handbook

## Use Cases

- Traditional TIC
- Branch Office

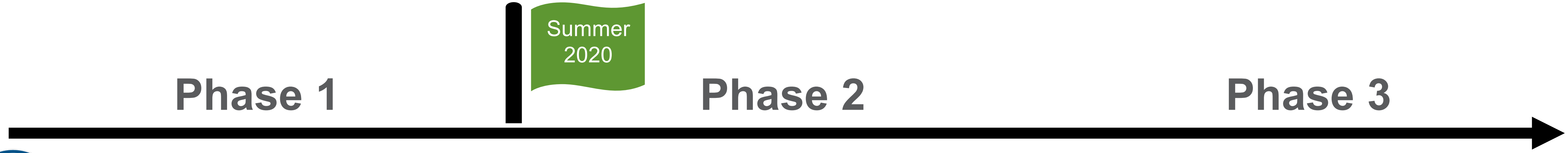
## OMB M-19-26 Use Cases

- Remote User
- Infrastructure as a Service
- Software as a Service
- Platform as a Service
- Email as a Service

TIC Working Groups

## Potential Use Cases

- Zero Trust
- Internet of Things
- Partner Networks
- GSA Enterprise Infrastructure Solutions (EIS)
- Unified Communications
- Additional Use Cases to be determined



# TIC Resources

- CISA TIC website: https://www.cisa.gov/trusted-internet-connections.
- CISA TIC FAQ: https://www.cisa.gov/tic-faq.
- TIC Webinar Recording on GSA YouTube: https://youtu.be/sQHde_YQPnI.

## TIC FAQ Examples

- **How does TIC 3.0 differ from earlier versions of the program?**

TIC 2.0 focused exclusively on securing an agency's perimeter by funneling all incoming and outgoing agency data through a TIC access point. Through Office of Management and Budget (OMB) M-19-26, OMB focuses on strategy, architecture, and visibility in TIC 3.0, recognizing the need to account for multiple and diverse architectures rather than single perimeter approach like TIC 2.0…

- **How do agencies implement TIC 3.0?**

Due to the wide variety of modern IT environments and requirements based upon varying missions, needs, and resources of agencies across the .gov, the updated policy allows for broader interpretation authorities to be assumed by federal civilian agencies. As modern architectures become both more complex and diverse, TIC 3.0 accommodates a wide variety of scenarios, focusing on cloud, mobility, and encryption…

# Questions?

**For program inquiries:**
Contact TIC PMO at
tic@cisa.dhs.gov.

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