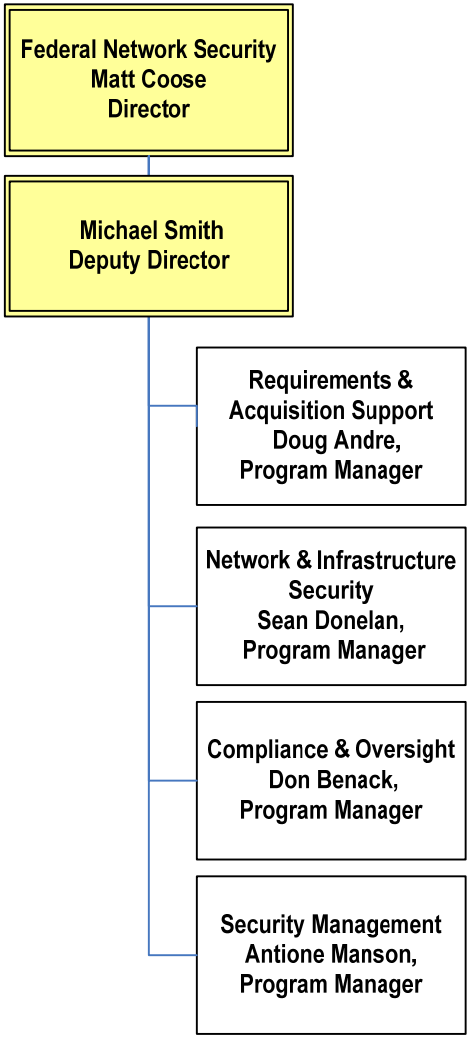
Department of Homeland Security
Federal Network Security

Trusted Internet Connections (TIC) Update
for the
Information Security and Privacy Advisory Board

July 29, 2009

Federal Network Security Branch



Branch Vision: To be the recognized leader for driving change that enhances the cyber security posture of the federal government

- Holistic approach to government network security
- Work across all federal agencies
- Address common challenges faced by all agencies
- Design, implement, and maintain solutions that address the aggregate need

- DHS – NPPD – CS&C – NCSD

- Started in 2008 to coordinate the Information
- System's Security Line of Business (ISS LoB)

- Identified in OMB M-08-05 to oversee CNCI #1, also known as the Trusted Internet Connection (TIC) Initiative

- Recently grew into 4 distinct programs

Federal Network Security Objectives

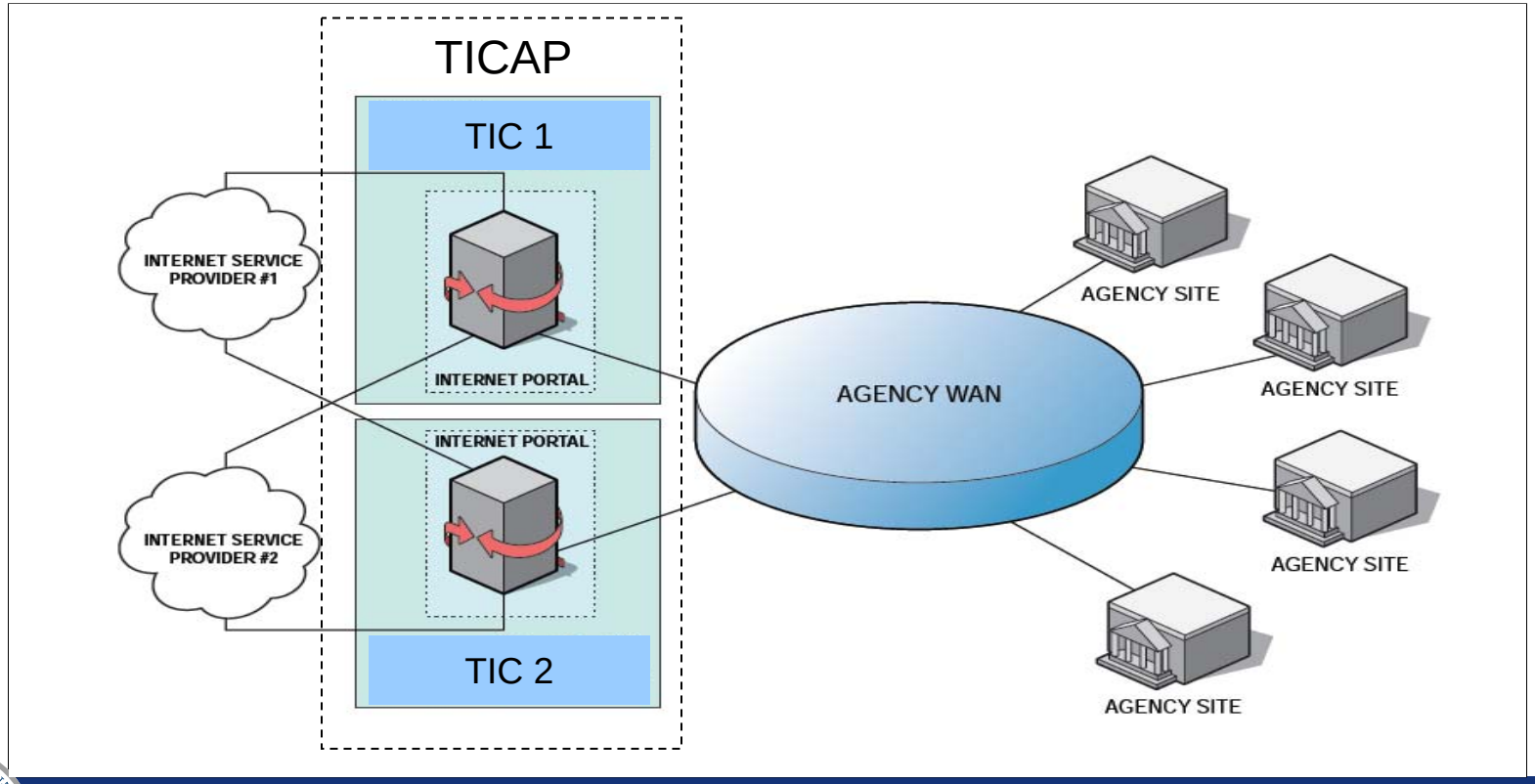
- Assess and prioritize common cyber security needs and solutions across the federal civilian government
- Promote actionable cyber security policies, initiatives, standards, and guidelines for implementation across the federal civilian government
- Enable and drive the effective implementation of cyber security risk mitigation strategies across the federal civilian government
- Measure and monitor agency implementation strategies and compliance with published cyber security policies, initiatives, standards, and guidelines
- Build a cohesive organization and associated programs that aggressively reduce cyber security risks in partnership with public and private stakeholders



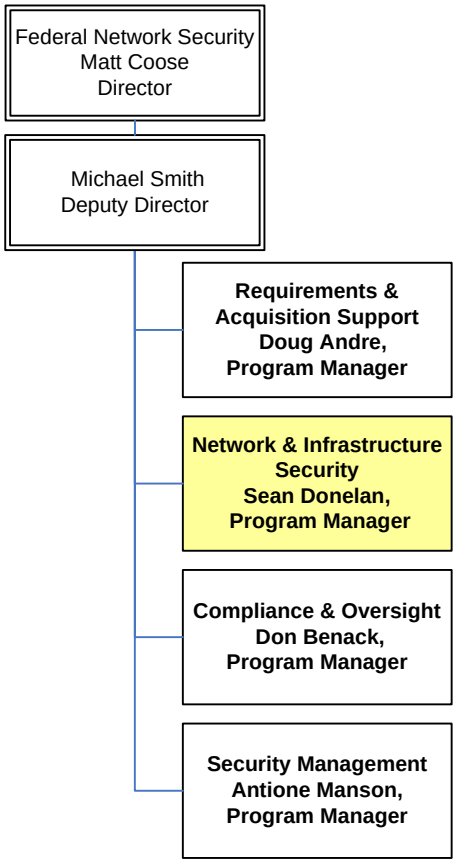


TIC Glossary

- **TIC**: Facility. Physical location containing security hardware & software
- **TICAP**: Access provider that manages the operation of TICs in support of customer requirements and policies; includes two or more TICs, two or more connections as well as the supporting NOC/SOC functions
- **MTIPS**: Service sold by a Networx vendor, also a TICAP



Network & Infrastructure Security



- **Mission**: Optimize Individual agency network services into a common solution for the federal government
- **TIC Initiative**: Responsible for implementation and oversight of CNCI #1:
  - Reduce & consolidate external access points, including connections to the internet across the federal government
  - Define and maintain baseline security capabilities for TICs and TIC Access Providers (currently 51 capabilities such as a state full firewall, email virus/spyware/spam blocking, etc)
  - Agencies can implement additional security capabilities on top of the baseline TIC security capabilities
  - 20 Agencies have been designated TIC Access Providers (TICAP) by OMB
- **Networx**: Managed Trusted IP Services (MTIPS) is the sole vehicle for other federal civilian agencies in the US to acquire TIC-Compliant services
  - Four MTIPS awards (AT&T, Qwest, Sprint and Verizon)
  - Bundles Internet access, managed security services (24x7 NOC/SOC) and baseline TIC security capabilities
  - Agencies can buy additional security capabilities on top of MTIPS
  - State Department TICAP will support a few agencies in the foreign affairs community outside the US
- **Architecture and Standards**: Assist in the clarification and implementation of NIST standards.
  - Lead efforts to clarify ambiguous terms aka (“external connection”)
  - Maintain Federal Network Security Architecture Document
  - Share implementation experiences and best practices

Where did TIC Requirements Come From?

- Presidential Directive: HSPD 23, Comprehensive National Cybersecurity Initiative (Initiative #1 is Trusted Internet Connections Initiative)
- TIC Working Group: agency-designated technical experts have participated in several work group sessions to develop TIC technical requirements, clarify architecture, and resolve technical question
- CIO Council: agency CIOs have been briefed on several occasions both on the status and expectations of TIC requirements.
- Government wide meetings: Held in Q1 & Q2FY08, used to outline the expectations of the TIC Initiative, communicate notional architecture, and answer agency questions
- OMB publication of Memo 08-16, Guidance for the TIC Statement of Capability
- "Continue to pursue the goal of the Trusted Internet Connection program to reduce the number of government network connections to the Internet but reconsider goals and timelines based on a realistic assessment of the challenges." – Cyberspace Policy Review, The White House, 2009

TIC – Definition of Success

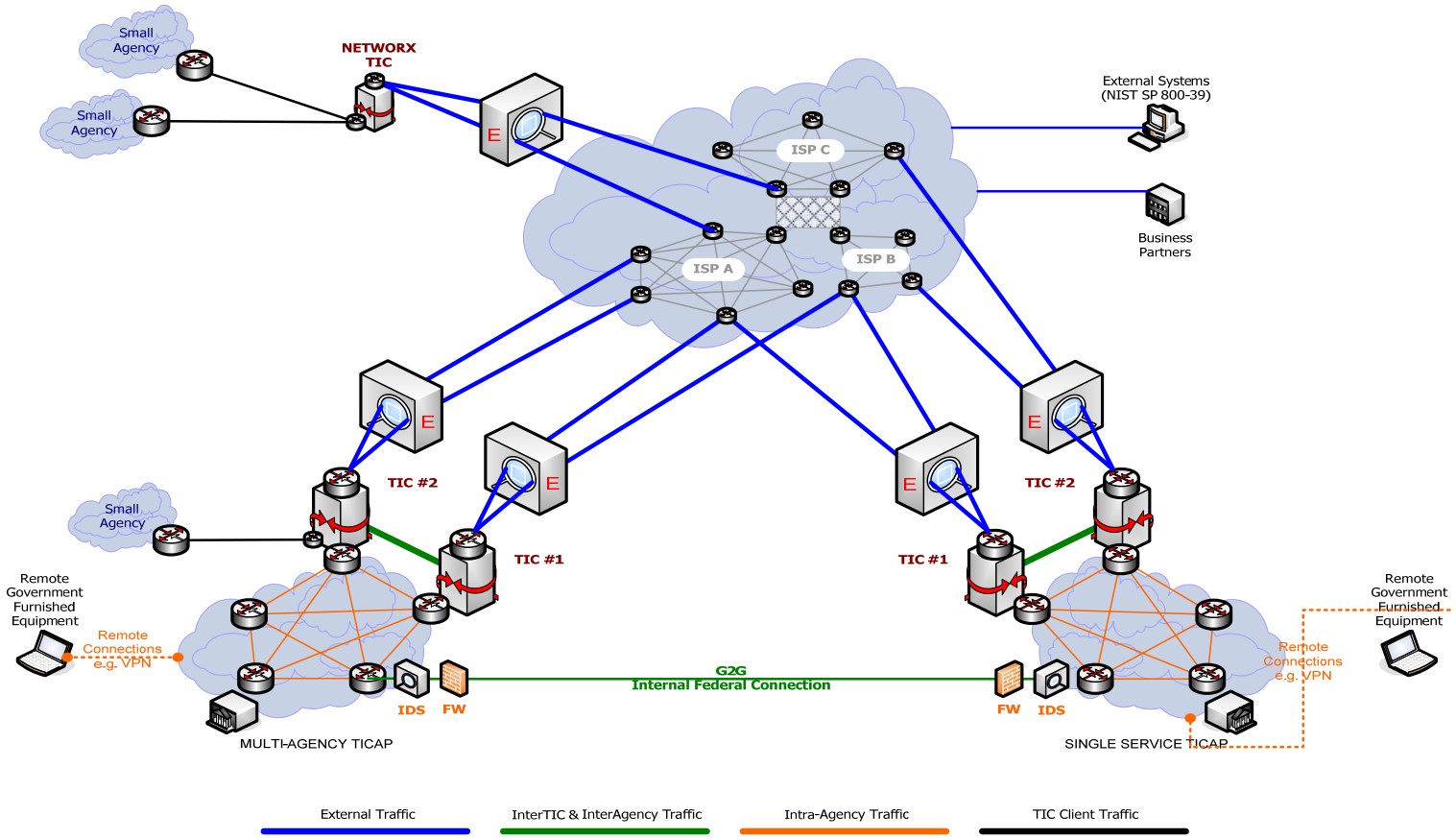
Success:
Federal Government external connections are reduced and consolidated through approved access points

Definitions:
- Federal Government = Approximately 116 Civilian Executive Branch Departments/Agencies (D/As)
  - TIC is not mandatory for the Legislative Branch, Judicial Branch or Department of Defense
- External Connection = Physical or logical network connection to an end-point outside of a D/A's Certification & Accreditation boundary…(formal definition in TIC Reference Architecture V1.0)
- Access Point = Consolidation point for network connections; Trusted Internet Connection (TIC)
- Approved Access Point = TIC in full compliance (100%) with the current TIC Statement of Capabilities (SoC), as validated by a FNS TIC Compliance Visit (TCV)

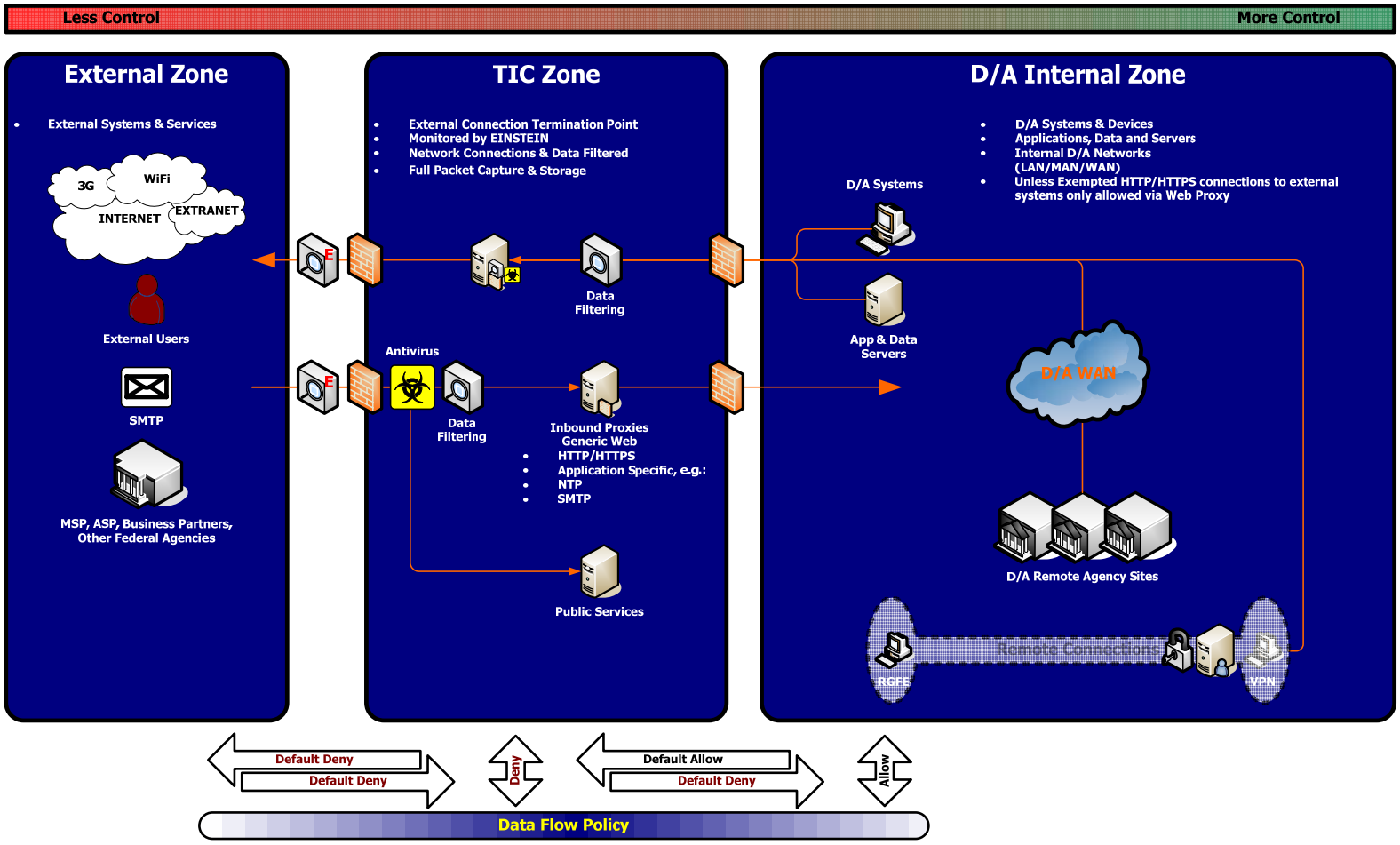
Constraints:
- The total number of access points should be less than 50 to the extent practicable
  - Max of 2 TICs per TIC Access Provider unless exception made by DHS/OMB
  - Combination of MTIPS TICs and D/A TICs means an agency could use 8-10 TIC access points
- Aggressive timelines required because Departments/Agencies already under attack by sophisticated adversaries

Assumptions:
- OMB Memo (M-08-05) target of "50 external connections" is interpreted as "50 access points"
  - Target may need to vary up or down depending on government-wide need and missions
  - Current target is between 50-100 TIC access points
- Consolidation of external connections is more important than reduction of external connections
- Establishing baseline security capabilities across all federal agencies needed to prevent weakest link

Notional TIC Architecture



Conceptual TIC Trust Relationships



Recommended **Inter-zone** Data Flow Policy

Recommended **Intra-zone** Data Flow Policy

RGFE: Remote Government Furnished Equipment

Definition of External Connections

3.1 External Connection: A physical or logical connection between information systems, networks, or components of information systems and networks that are, respectively, inside and outside of specific Department or Agency's (D/A) Certification and Accreditation (C&A) boundaries established by the D/A, where:

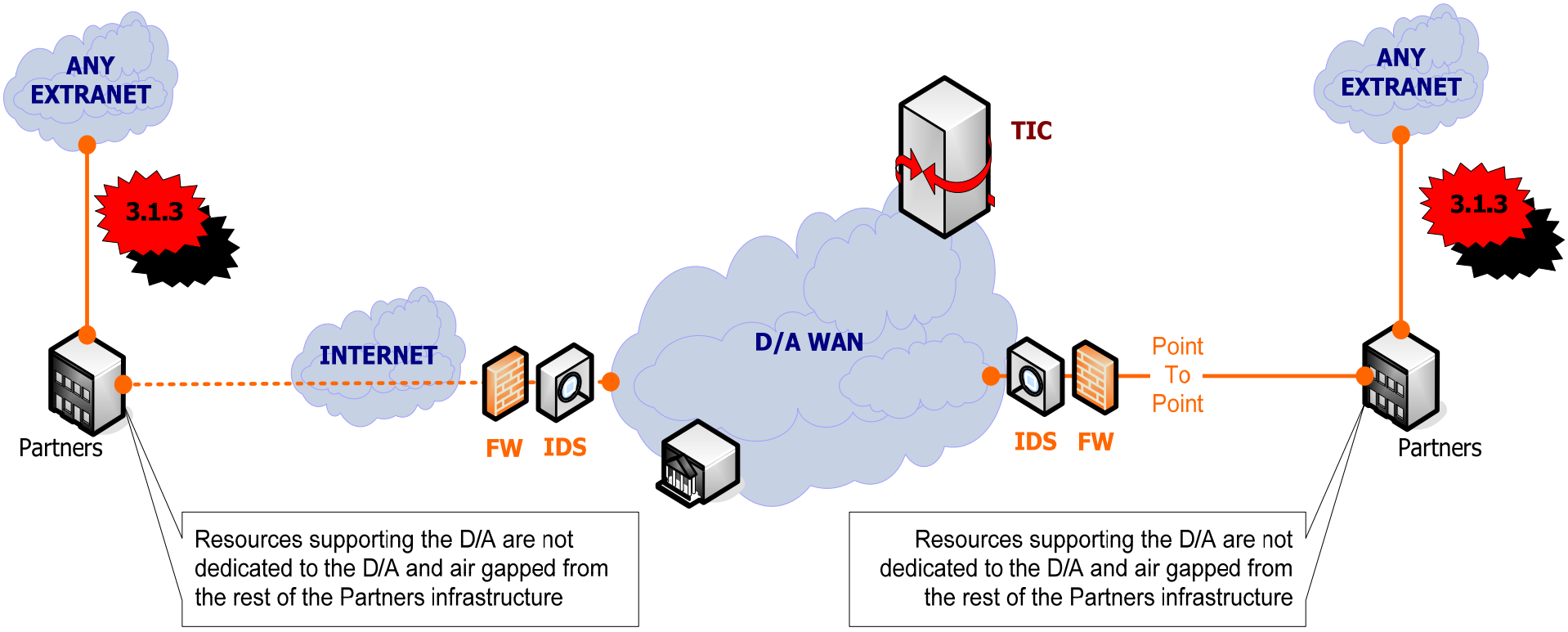
3.1.1 the D/A does not have control over the application of required security controls or the assessment of security control effectiveness on the outside information system, network, or components of information systems or networks, or

3.1.2 the D/A, notwithstanding control over the application of required security controls or the assessment of security control effectiveness, has specific reason to believe that the external system has a substantially reduced set of security controls or an increased threat posture relative to the internal system, or

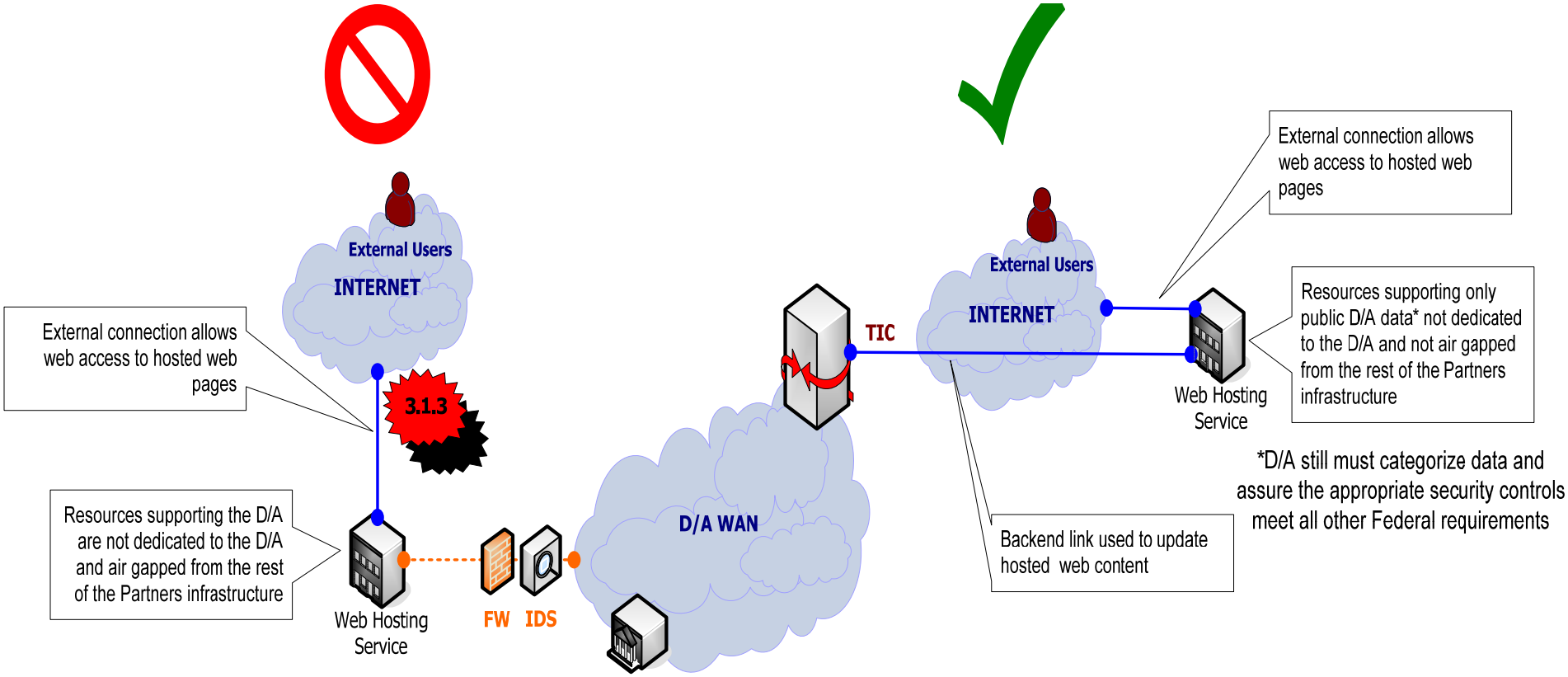
3.1.3 the connection could be used to establish a connection with an external system that is not routed through an approved TIC.

Examples on following slides

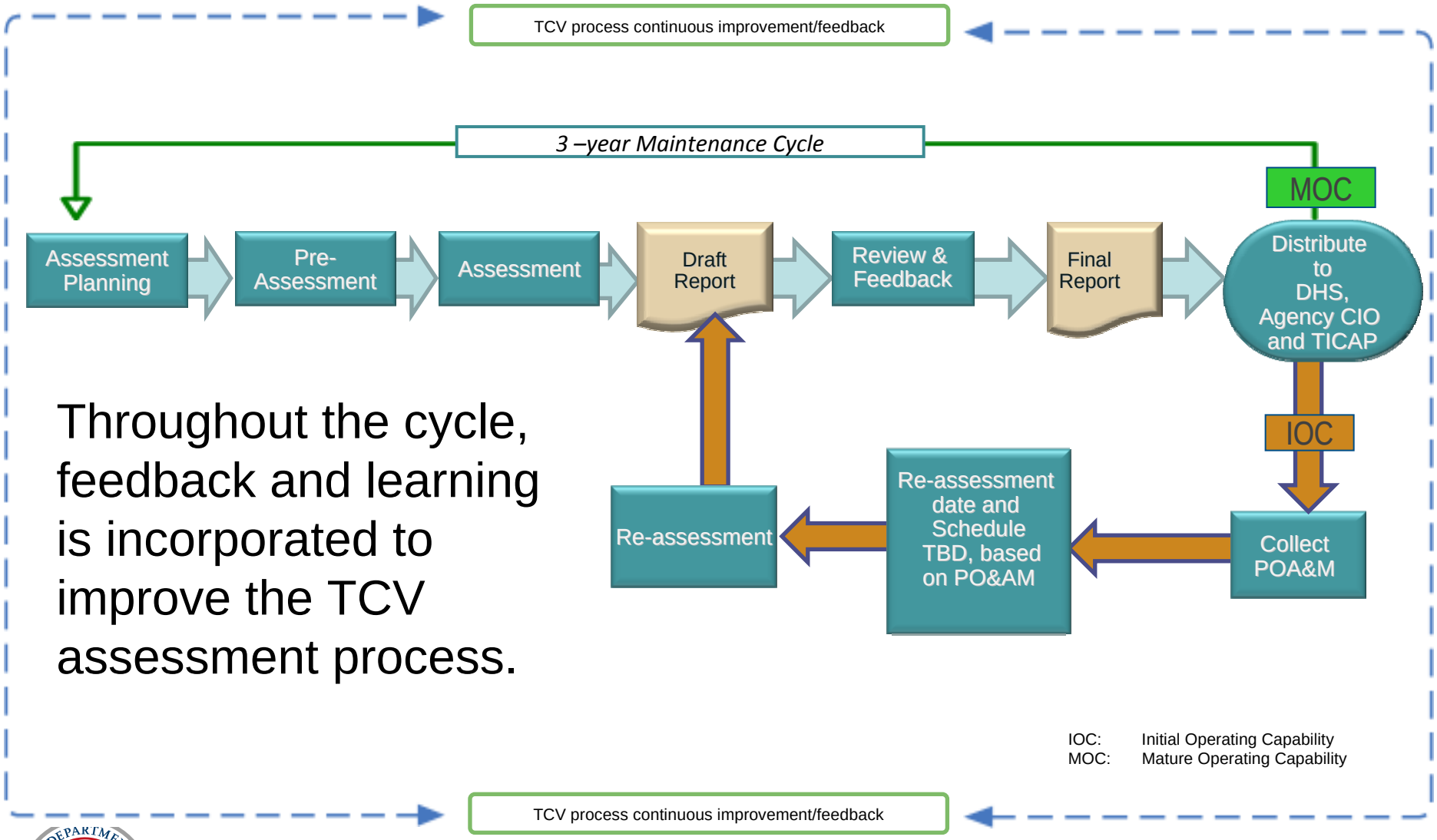
Prohibited external connection through partner



Comparison of Hosting Scenarios



TIC Compliance Validation Feedback



EINSTEIN capabilities as part of TIC

- National Cybersecurity Protection System (also operationally referred to as EINSTEIN) pre-dates the Trusted Internet Connections Initiative
  - Included as one capability in the TIC Statement of Capabilities (requirements) in addition to agency-specific Intrusion Detection/Prevention System capabilities
  - Once fully deployed, will provide an early warning system and situational awareness, near real-time identification of malicious activity, and a more comprehensive network defense across federal civilian agency networks

- The first generation of the EINSTEIN system was primarily a network flow analysis tool
- The second generation of the EINSTEIN system incorporates network intrusion detection technology in addition to network flow analysis
- The third generation of the EINSTEIN system is expected to add a network intrusion prevention technology in addition to the intrusion detection and netflow analysis

- DHS has briefed Congress on several occasions, as well as privacy and civil liberties advocacy groups to ensure adherence to all privacy and civil liberties mandates and guidelines

- For more information about EINSTEIN Privacy Impact Assessments

  http://www.dhs.gov/privacy

  under Privacy Compliance Documentation

Contact Information

Sean Donelan

Network & Infrastructure Security

Federal Network Security

US Department of Homeland Security

Sean.Donelan@dhs.gov

703-235-5122

Trusted Internet Connections Program

tic@dhs.gov

Back Up

FNS Authorities

- Federal Information Security Management Act 44 U.S.C § 3546 (FISMA)
- Homeland Security Act of 2002, Public Law 107-296 (HSA2002)
- Homeland Security Presidential Directive 23 (HSPD23)
- Homeland Security Presidential Directive 7 (HSPD7)
- Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003 (CIIPP)
- National Strategy to Secure Cyberspace, February 2003 (NSSC)
- Comprehensive National Cybersecurity Initiative, 2008 (CNCI)
- OMB Memorandum: M-08-05, Implementation of Trusted Internet Connections, November 20, 2007 (TIC)
- OMB ISSLOB designation letter dated 06/06 (ISSLOB)

TIC Specific Authorities

- Comprehensive National Cybersecurity Initiative, 2008 (HSPD 23)
- OMB Memorandum: M-08-05, Implementation of Trusted Internet Connections, November 20, 2007
- OMB Memorandum: M-08-16, Guidance for Trusted internet Connection Statement of Capability Form, April 4 , 2008
- OMB Memorandum: M-08-27, Guidance for Trusted Internet Connection Compliance, September 30, 2008
- "Continue to pursue the goal of the Trusted Internet Connection program to reduce the number of government network connections to the Internet but reconsider goals and timelines based on a realistic assessment of the challenges." – Cyberspace Policy Review, 2009

OMB TIC Policy Memorandum Summary

OMB Policy

- M-08-05: Announcing the Trusted Internet Connections (TIC) initiative to optimize individual network services into a common solution for the federal government. This common solution facilitates the reduction of our external connections, including our Internet points of presence, to a target of fifty.

- M-08-16: In November 2007, OMB announced the implementation of Trusted Internet Connections (TIC) in Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC)." The TIC initiative is to optimize individual external connections, including internet points of presence currently in use by the federal government. It will improve the federal government's incident response capability through the reduction of external connections and centralized gateway monitoring at a select group of TIC Access Providers (TICAP).

- M-08-27: For those agencies that have been identified as a TIC Access Provider, compliance with the TIC initiative includes the agency taking the following actions:
  1. Complying with critical TIC technical capabilities per the agencies' Statement of Capability
  2. Continuing reduction and consolidation of external connections to identified TIC access points
  3. Collaborating with NCSD in determining agency technical readiness to coordinate/schedule installation of Einstein
  4. Executing a Memorandum of Agreement (MOA) between DHS and your agency Chief Information Officer (CIO)
  5. Executing a Service Level Agreement (SLA) between DHS and your agency CIO

Homeland Security