

Trusted Internet Connections (TIC) Status and Plans



TIC/MTIPS Panel Discussion
American Council for Technology/Industry Advisory Council
July 19, 2010



Comprehensive National Cybersecurity Initiatives (NSPD-54/HSPD-23)

Focus Area 1	Trusted Internet Connections <i>Reduce and Consolidate external access points, manage technical requirements for NOC/SOC, & establish a Compliance Program</i> (OMB/DHS)	Deploy Passive Sensors Across Federal Systems (DHS)	Pursue Deployment of Intrusion Prevention System (DHS/DOD)	Coordinate and Redirect R&D Efforts (OSTP)
	Establish a front line of defense			
Focus Area 2	Connect Current Cyber Centers to Enhance Cyber Situational Awareness (DNI)	Develop Government Wide Cyber Counterintelligence Plan (DNI/DOJ)	Increase the Security of the Classified Networks (DNI/DOD)	Expand Education (DHS/DOD)
	Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success			
Focus Area 3	Define and Develop Enduring Leap Ahead Technology, Strategies & Programs (OSTP)	Define and Develop Enduring Deterrence Strategies & Programs (HSC/NSC)	Develop Multi-Pronged Approach for Global Supply Chain Risk Management (DHS/DOD)	Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains (DHS)
	Shape the future environment to demonstrate resolve to secure U. S. technological advantage and address new attack and defend vectors			



Trusted Internet Connection Summary

Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.

The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal Government's external access points (including those to the Internet).

This consolidation will result in a common security solution which includes:

- Facilitating the reduction of external access points,
- Establishing baseline security capabilities; and,
- Validating agency adherence to those security capabilities.

Agencies participate in the TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle.

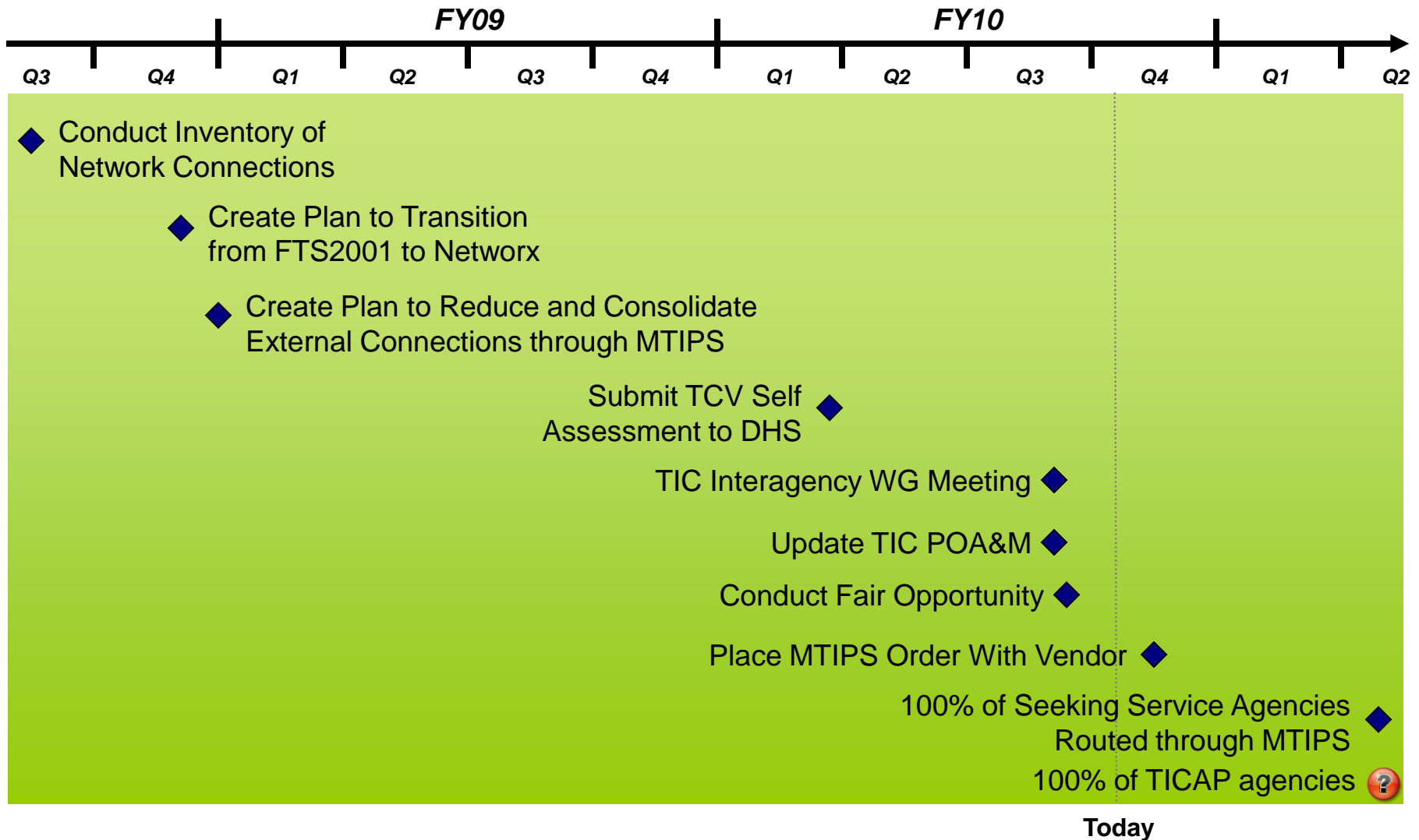


Selected TIC Highlights

- Each TIC access point must meet 51 critical security capabilities
 - 50 baseline security capabilities (TIC 1.0)
 - National Cyber Protection System (Einstein)
- 19 Agencies Designated as TIC Access Providers (07/19/2010)
 - TICAP agencies may build their own TIC locations and use MTIPS (Hybrid)
- 4 Network vendors awarded Managed Trusted IP Service (MTIPS)
- Approximately 90 Seeking Service agencies will utilize MTIPS
 - Includes all civilian Executive Branch departments and agencies
 - Does not include Legislative Branch, Judicial Branch or Department of Defense
 - January 31, 2011 target date for agencies to complete migration
- Plans for TIC 2.0 Technical Architecture



Agency TIC and MTIPS Milestones



Subject To Change



Definition of External Connection

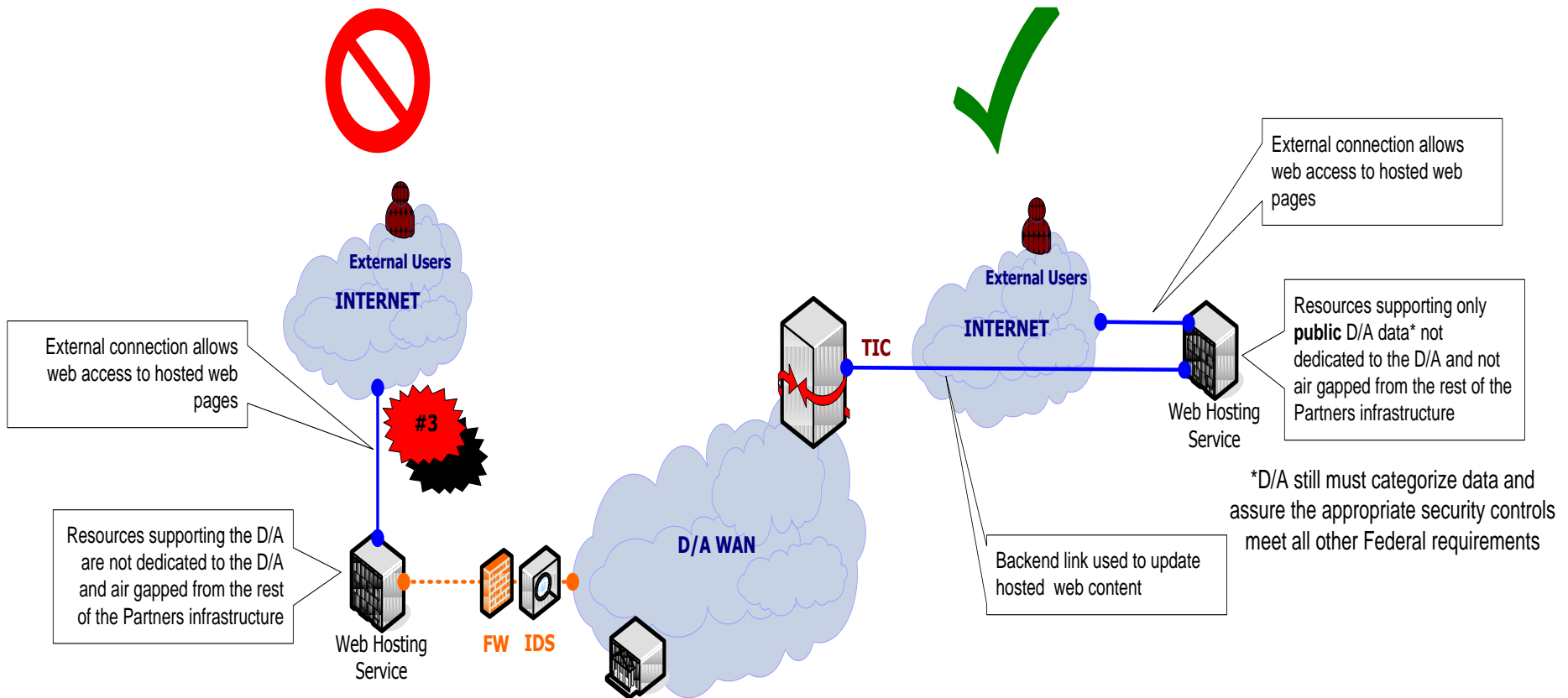
External Connection: A physical or logical connection between information systems, networks, or components of information systems and networks that are, respectively, inside and outside of specific Department or Agency's (D/A) Certification and Accreditation (C&A) boundaries established by the D/A, where:

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

Source: TIC Reference Architecture V1.0, Appendix A



Examples of Connections

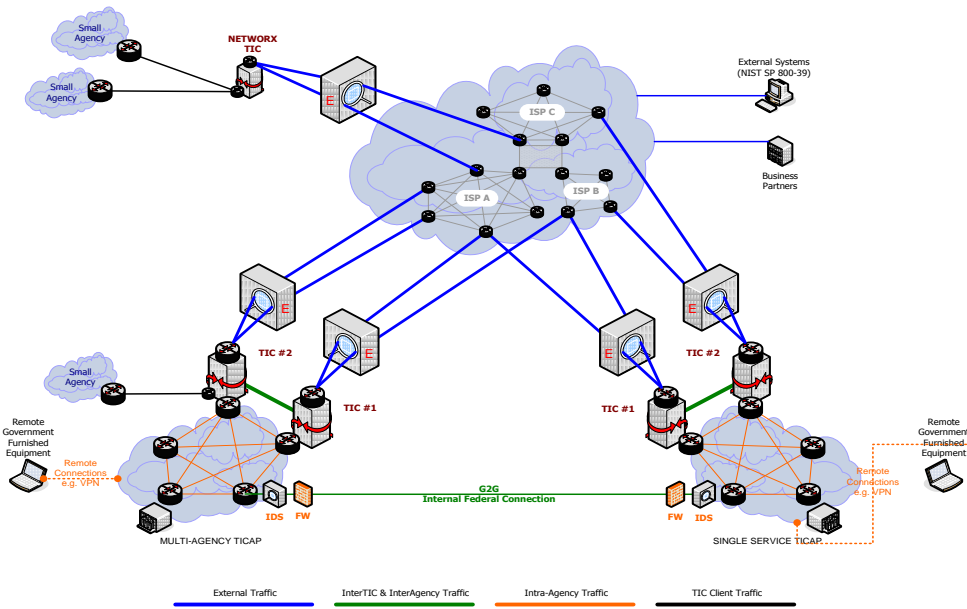


Source: TIC Reference Architecture V1.0, Appendix A

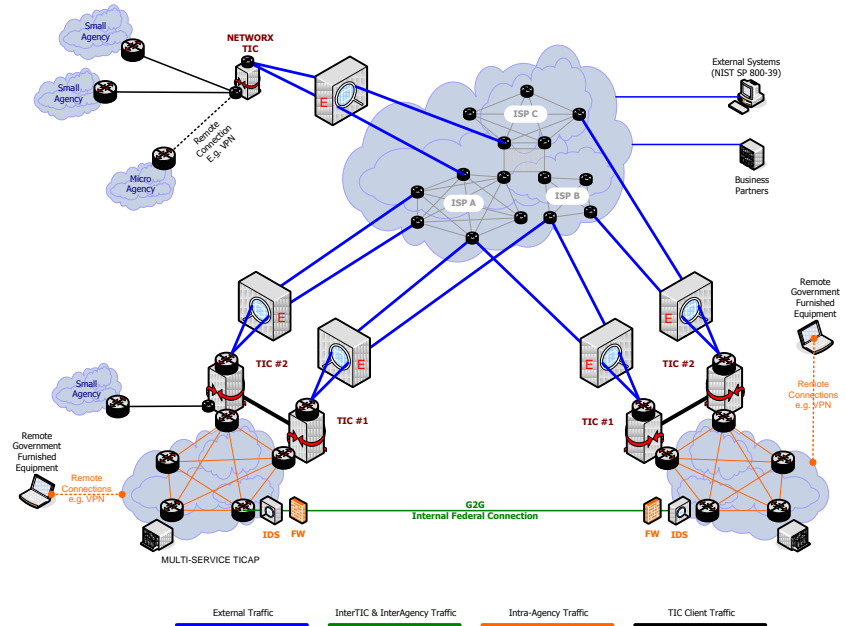


TIC1.0 and TIC2.0 Architecture Comparison

TIC 1.0



TIC 2.0



Subject To Change



Homeland Security

Federal Network Security

Backup



Contact Information

Sean Donelan

Network & Infrastructure Security
Department of Homeland Security
National Cyber Security Division
Federal Network Security
office: 703-235-5122
email: sean.donelan@dhs.gov

For TIC questions:
tic@dhs.gov

For US Government (.GOV or .MIL account required):

<https://max.omb.gov/community/display/Egov/Trusted+Internet+Connections>



What Agencies are included in TIC?

The Trusted Internet Connection Initiative includes all civilian Executive Departments and Agencies; which does not include the Department of Defense, Legislative Branch agencies and Judicial Branch agencies.

National Security Presidential Directive-54 (HSPD-23) "National Cyber Security Initiative" including Initiative #1 Trusted Internet Connections (TIC) and National Security Presidential Directive-51 (HSPD-20) "National Continuity Policy" use essentially the same definition of Executive Departments and Agencies.

- "federal departments and agencies" means those executive departments enumerated in U.S.C. Section 101; independent establishments as defined in 5 U.S.C. Section 104(1) ; government corporations as defined by 5 U.S.C. Section 103(1); and the United States Postal Service (USPS); (U)

OMB Circular A-11, Appendix C is the presumptive list of agencies.



TIC Background

- Comprehensive National Cybersecurity Initiative (CNCI, NSPD-54/HSPD 23)
- Cyberspace Policy Review, The White House, 2009
- OMB published Memos
 - M-08-05
 - M-08-16
 - M-08-26
 - M-08-27
 - M-09-32
- TIC Interagency Working Group
- TIC Reference Architecture v1 (Spring 2009)



Deadlines for Agencies Seeking TIC Services

Deadline	Milestone
1/8/2008	Conduct Inventory of Network Connections (M-08-05)
9/30/2008	Create plan to Transition from FTS2001 to Network (M-08-26)
10/15/2008	Create POA&M to Reduce and Consolidate External Connections through MTIPS (M-08-27)
12/31/2009	Submit TCV Self Assessment to DHS (M-09-32)
6/10/2010	TIC Interagency WG Meeting for Agency TIC POCs
7/1/2010	Update TIC POA&M with DHS
6/1/2010	Conduct Fair Opportunity
8/31/2010	Place MTIPS Order with Vendor
1/31/2011	100% of External Connections routed through TIC Access Point



Federal Network Security Responsibilities

Assess Enterprise Needs and Required Capabilities

Through interagency collaboration Identify and prioritize actions required to mitigate risks and improve cyber security posture across the Enterprise

Influence Policy and Strategies to Implement

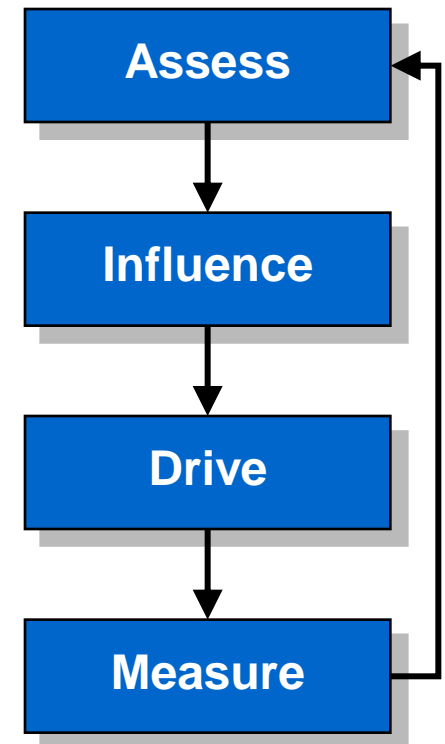
Promote actionable cyber security policies, initiatives, standards, and guidelines for implementation

Drive Implementation of Capabilities

Enable and drive the effective implementation of cyber security risk mitigation activities and capabilities

Measure and Monitor Implementation and Security Posture

Measure and monitor agency implementation strategies and compliance with published cyber security policies, initiatives, standards, guidelines and directives





Homeland Security

