Trusted Internet Connections (TIC) Initiative

Statement of Capability Evaluation Report

Prepared by:

US-CERT/ISS LOB

June 4th, 2008

ACKNOWLEDGEMENTS

Requirements Gathering Team Members

Name	Agency/Organization	Name	Agency/Organization
Cecil Avery	CSOSA	Kshemendra Paul	OMB
Anthony Bailey	DOE	Bill Lakner	DOL
Gerry Barsczewski	SSA	Thomas Leach	Small Agency Council
Don Benack	DHS/US-CERT	Jessica Lee	DOE
Paul Blahusch	DOL	Jim McAuley	DOL
Carlos Blazquez	DOS	Marion Meissner	NASA
John Bourdon	USAID	Stu Mitchell	DOI IOS
George Cartron	GSA	Alex Molina	ITI LoB PMO
Bobby Cates	NASA	Zachary Murray	DNI
Chris Chroniger	DOL	Sara Nasseh-Mosley	DOS
Dan Crosson	USDA	Frederick Reyes	DOEd - Student Aid
Don Cuffee	CSOSA	Mike Sauer	ISS LoB PMO
Roman Danyliw	US-CERT	Jessica Shih-Ning Lee	DOE
Johnny Davis	EPA	Ruchika Sindhi	ISS LoB PMO
John DiLuna	ISS LoB PMO	Mike Smith	DHS ISS LoB PMO
Steve DiMuzio	ISS LoB PMO	Jason Tam	DOL
Tom Donahue	CIA	Bradley Tesh	Smithsonian Institute
Walter Dove	EPA	Troy Thompson	SBA
Everett Dowd	DOT	Gail Tryon	DNI
Adam Doyle	GSA	El-Farouk Umar	Peace Corps
Adam Drzal	OPIC	Michael Van Dyke	DOC - Census
Lee Dudek	DOI	Dan VanBellegham	DOS
David Elliott	DOEd - Student Aid	Linda VanKuren	ISS LoB PMO
John Feldman	DOS	Randy Vickers	DHS/US-CERT
Bill Flowers	USDA	James Warren	DOI
Doug Fry	AFCA	Richard Westfield	Small Agency Council
Bill Gill	EPA	Kenneth White	NASA
Don Hagerling	DHS	Eric Wong	ITI LoB PMO
Walton Hare	DOS	Steve Wright	DOL
Tim Hurr	DOC	Andrew Zinn	DNI
Robert Hyers	IRS - CSIRC	Kevin Walton	DOI
Todd Johnson	TREASURY	Bobby Singh	DOI
Ben Kimes	DNI		

Statement of Capability Evaluation Team Members

Business Model Review Team supported by SRA/Touchstone Consulting Group

Technical Review Team supported by MITRE Corporation

Key Stakeholders

OMB, Office of E-Government and Information Technology

Federal CIO Council

Federal Small Agency CIO Council

DHS National Cyber Security Division (NCSD)

Federal Systems Security Governance Board (FSSGB)

Information Systems Security Line of Business (ISS LoB) - DHS

DHS United States Computer Emergency Readiness Team (US-CERT)

Information Technology Infrastructure Line of Business (ITI LoB) - GSA

All Federal Agencies

Advisors

George Colt, Independent Network Architect

Gary Davis, Independent Network Architect

David Wennergren, Deputy CIO, DoD

Alan Paller, Director of Research, SANS Institute

Scott Bradner, Technology Security Officer, Harvard University

James Williams, Commissioner Federal Acquisition Service (FAS), GSA

EXECUTIVE SUMMARY

In November 2007, the White House Office of Management and Budget (OMB) announced the Trusted Internet Connections (TIC) Initiative via Memorandum M-08-05 – *Implementation of Trusted Internet Connections*. The overall purpose of the TIC Initiative as outlined in the memorandum is to optimize and standardize individual external network connections, to include connections to the internet, currently in use by the federal government. Ultimately the initiative will improve the federal government's security posture and incident response capability through the reduction and consolidation of external internet connections and provide centralized gateway monitoring at a select group of TIC Access Providers (TICAPs).

> **CURRENT AND TARGET CONNECTIONS**
> **(AGENCY REPORTED)**
>
> ♦ Existing Connections (Jan 2008) = 4300+
> ♦ Existing Connections (May 2008) = 2758
> ♦ Target Connections = <100

TICAPs will be modeled similarly to existing government-hosted Shared Service Centers that are currently operating within Lines of Business (LoBs). The technical, physical security, business model, and service level requirements were developed by an interagency workgroup, reviewed by the CIO Council, and approved by OMB. These requirements were integrated into a Statement of Capability (SOC) Form which provided agencies with the opportunity to propose their existing or planned capability to function as a TICAP and their preference to serve as a TICAP only to themselves (Single Service TICAP), other agencies through a shared services model (Multi-Agency TICAP), or seek services from an approved TICAP (Seeking Services). In total, 35% of solicited federal agencies submitted a Statement of Capability (92% of scorecard agencies). These SOCs were evaluated to determine whether or not agencies sufficiently addressed the technical and business model capabilities; the evaluation results determined that an agency either: a) met the required TIC capabilities, b) met 90% or more of the capabilities and have a plan to address the gaps, or c) met less than 90% of the capabilities and plans to address the gaps need to be more comprehensive. All agencies not specifically designated as Single Service or Multi-Agency TICAPs are directed to seek services from another TICAP.

> **TIC ACCESS PROVIDERS (TICAPs)**
>
> ♦ 2 Multi-Agency Service Providers with 7 potential TICs
> ♦ 16 Single Service Providers with 72 potential TICs
> ♦ NETWORX Providers with approximately 10 potential TICs

Multi-Agency TICAPs: Two agencies were determined to be capable Multi-Agency TICAPs or have aggressive plans to implement TIC requirements within the next six months. These two Multi-Agency TICAPs represent seven potential TICs. One of these agencies has demonstrated a current ability to meet the technical and business capabilities required of a Multi-Service TICAP. One additional agency is conditionally recommended as Multi-Service TICAPs. This agency has existing gaps regarding the technical and business capabilities required of a Multi-Service TICAP, but have indicated plans to address the identified gaps.

Single Service TICAPs: 16 agencies were identified as capable Single Service TICAPs. These agencies have demonstrated a current ability to meet the technical capabilities required of a Single Service TICAP or have sufficiently addressed gaps in their implementation plans. These 16 Single Service TICAPs represent 72 potential TICs. Five additional agencies met less than 90% of the capabilities and required more comprehensive implementation plans.

Seeking Service: The remaining 121 agencies shall seek service from an approved TICAP. Agencies that did not submit a Statement of Capability were also categorized as seeking service.

BACKGROUND

TIC Initiative

The Trusted Internet Connections (TIC) Initiative commenced in November 2007 with the issuance of Office of Management and Budget (OMB) Memorandum M-08-05 – *Implementation of Trusted Internet Connections* to optimize each individual federal agency's network services into a common solution for the federal enterprise and establish guidelines for agencies to provide a plan of action and milestones (POA&Ms) for meeting TIC deadlines. The purpose of the POA&Ms was to document the agency's existing connections as of January 2008 and provide plans to reduce and consolidate those connections. Additionally, with the release of OMB Memorandum M-08-16 – *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)* on April 4, 2008, agencies were requested to propose their solution and outline their level of capability to become a Single or Multi-Agency TIC Access Provider (TICAP). On May 1, 2008, agencies also provided a business justification that outlines the number of TICs that are necessary in order to support their current mission requirements and customer base.

Between the two referenced guidance memorandums, milestones have been outlined that help define the current state of external connections within the federal enterprise as well as articulate the actions to achieve the objectives of the TIC Initiative. Specifically, the milestones are highlighted in Figure 1 below.

Figure 1: TIC Initiative Timeline

3
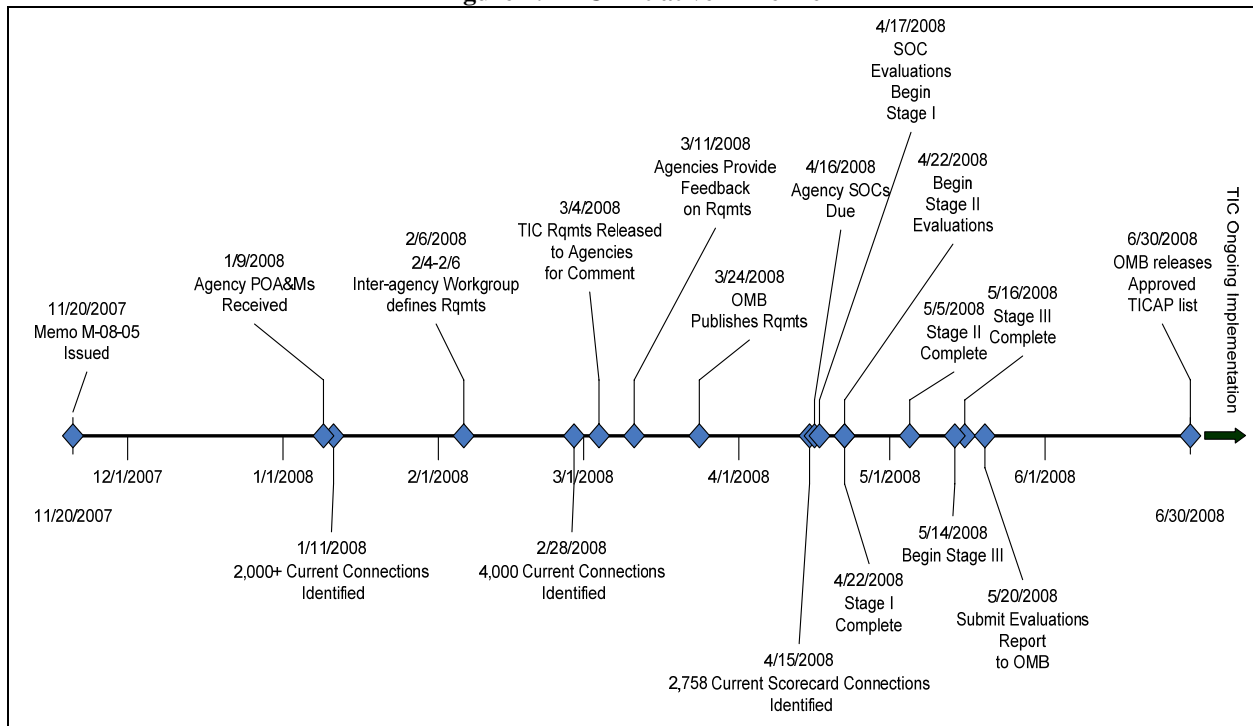
The overall approach is being executed in three concurrent phases:

> Phase I: Agency Plan for Reduction and Consolidation of External Connections: In January 2008, agencies submitted POA&Ms that inventoried their existing number of external connections and outlined a plan to optimize their existing connections. Agencies were required to update this plan on April 15, 2008.

> Phase II: TICAP Initial Capability: In February, 2008, OMB and DHS led an interagency workgroup to define the technical capabilities required of a Trusted Internet Connection and the business model capabilities for TIC Access Providers. Once completed, the requirements were vetted through all agency CIOs; their feedback was considered and incorporated into the final requirements document.

> The primary focus is on approving Single Service TICAPs, scorecard agencies serving their internal customer base, and Multi-Agency TICAPs, scorecard agencies serving other agencies as external customers that sufficiently meet the technical and business model capabilities published in the Statement of Capabilities Form. Work is being done with GSA to provide agencies with a TIC-compliant managed security solution through the NETWORX contract vehicle so that several NETWORX TICAPs will also be designated. It is envisioned that a majority of agencies will utilize NETWORX as a source of TICAP services both as a managed solution or implemented as part of an agency's Single Service TICAP solution. DHS is also developing an independent compliance capability modeled after the DoD's Computer Network Defense Service Provider (CNDSP) that will be chartered to ensure initial and ongoing compliance with the TIC Initiative.

> Phase III: TICAP Mature Capability: Single Service TICAPS will continue to mature their technical and business processes in providing service to their internal customers. As both Multi-Agency and NETWORX TICAPS become available, agencies who have selected that they intend to Seek Service will be expected to transition to one of the approved TICAPs under an aggressive timeline.
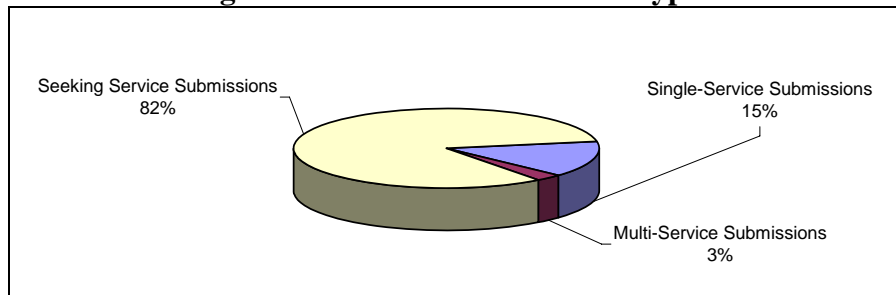
Statement of Capability Form

The requirements that define a TIC and the selection criteria for becoming a TICAP were defined in February 2008 by an interagency work group comprised of approximately 30 federal civilian agencies. The technical requirements were categorized as "Critical", "Important", or "Desired"; at a minimum, every TICAP must comply with the "Critical" requirements and may also choose to incorporate other elements of the "Important" and "Desired" requirements to enhance their solution. The draft requirements were reviewed by OMB and distributed to agency CIOs for final feedback and approval; this feedback was incorporated and agencies were solicited to propose their solution. The SOC Form provides agencies the opportunity to demonstrate their existing and future capability to meet technical and business capabilities that define a TICAP. Submitted Statements of Capability were evaluated and the results are provided in this report for input and feedback from the Federal Systems Security Governance Board (FSSGB), the CIO Council, and OMB.

The Statement of Capability Form requested information on how an agency planned to provide services as a TICAP whether to service their internal customer base or external customers from other agencies. Alternatively, Agencies could indicate whether they intended to fulfill the TIC requirements by seeking service from an authorized TICAP. The SOC Form was comprised of three sections: Business Model Capabilities, Technical Capabilities; and Seeking Service Explanation. Agencies were asked to fill out specific portions of the form depending on their requested TICAP type.

Statement of Capability Submission Data

Figure 2: Self-Selected TICAP Types[1]

Statement of Capability Form Review Process

Commencing on April 15, 2008 the Statement of Capability submissions have undergone a three-staged evaluation process to ensure that all information required by M-08-16 was provided. As outlined in Figure 3, Agencies were engaged in a continuous feedback cycle throughout Stage I and Stage II to address questions as they arose.

The evaluation team followed an approved evaluation plan outlining a transparent process that offered a repeatable and consistently-scored assessment of an agency's capability to sustain the operations of a TICAP. The Plan is divided into three stages, each with a specific purpose and focus:

- **STAGE I – Quality Assurance**: The initial process was focused on document control, inventory of required information, and compliance with M-08-16. Evaluators logged submitted Statement of Capability Forms and supporting documentation then performed an initial check of the information to assure that it responded to all necessary elements with appropriate information. Submissions requiring additional or amplifying information were returned to the agency for update and follow-up meetings with the agencies were conducted to ensure clear communication for all stakeholders.

- **STAGE II – Technical and Business Model Review**: Two independent teams focused on individual aspects of the SOC; a technically-oriented team evaluated the technical

---

[1] Data presented is based upon 144 Agencies that were provided an opportunity to submit a Statement of Capability. The data in the chart was derived from submitted agency Statement of Capability forms.

capabilities while a separate team evaluated the agency's response to the business model capabilities.

- **STAGE III – Consensus Review**: Representatives from both Stage II evaluation teams worked together to take a holistic approach in reviewing both the technical and business model capabilities to determine which agencies adequately demonstrated a capability to deliver TICAP services consistent with their self-identified TICAP selection.

Figure 3: Statement of Capability Evaluation Process
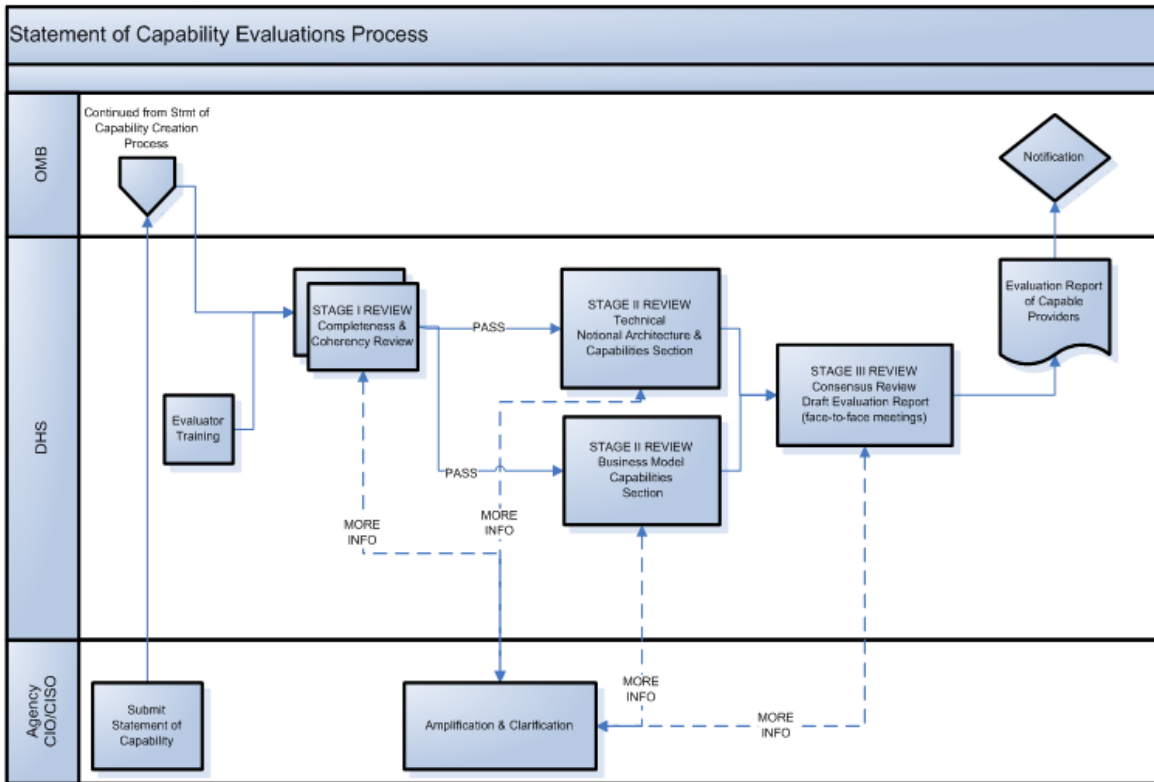
FINDINGS & RECOMMENDATIONS

Findings

A) One agency has demonstrated an immediate ability to meet 100% of the critical technical capabilities for becoming a Multi-Service TICAP. This Multi-Agency TICAP represents two potential TICs.

B) One agency has demonstrated an ability to meet at least 90% of the TIC capabilities for becoming a Multi-Service TICAP and has demonstrated aggressive plans to meet the technical requirements. This Multi-Agency TICAP represent five potential TICs.

C) 16 agencies have demonstrated an ability to meet at least 90% of the TIC capabilities for becoming a Single Service provider. These agencies have planned actions to address any identified gaps. These sixteen Single Service TICAPs represent 72 potential TICs.

D) Five agencies have not met at least 90% of the technical requirements or have not sufficiently indicated plans to meet the requirements to address identified gaps.

E) 121 agencies have indicated a preference to seek service from an approved TICAP or did not submit a Statement of Capability form.

F) The total number of TICs target connections identified by agencies outlined in Findings A, B, C, and D[2] is 79.

G) Agencies have indicated a significant reduction and consolidation of existing external connections from more than 4,300 in January 2008 to 2,758 (39%) as of May 2008.

H) The evaluation team noted a difference between the number of agency-reported target connections (235) and the calculated number of target connections (79). Additional effort will be required to reconcile this difference.

I) Based on SOC submittal information and evaluations, additional coordination with agencies will be needed regarding implementation of technical requirements such as: deep packet inspection of encrypted sessions, storage volume requirements, uniform time services, the sharing and use of custom IDS signatures, and Sensitive Compartmentalized Information Facility (SCIF) requirements..

J) NETWORX will provide flexibility to those agencies that do not currently have the capability to function in a Single-Service or Multi-Service capacity. Most agencies indicated an intention to incorporate NETWORX managed security capabilities as part of their TIC implementation.

---

[2] One agency in this grouping has engaged in ongoing efforts to project their target number of target connections. Additional dialogue will be required and will likely increase the number of overall target connections.

K) Prospective Multi-Service provider responses concerning business capabilities focused primarily on IT security risks and did not address other technical, financial, or operational risks.

Summary Recommendations

A) Designate two agencies as Multi-Service TICAPs; all must demonstrate an ability to meet 100% of the technical requirements to a CNDSP audit team prior to being authorized to accept external customers.

B) Designate 16 Agencies as Single-Service TICAPs; all must demonstrate an ability to meet 100% of the technical requirements to a CNDSP audit team prior to acknowledging a mature operating capability.

C) Agencies that did not sufficiently meet the requirements must resubmit a statement of capability to the ISS LoB by August 01, 2008 that demonstrates plans to meet 100% of the technical requirements for becoming a Single Service TICAP within 3 months or consider seeking service from an approved TICAP.

D) Schedule follow-up meetings to address existing gaps with the 17 (16 Single Service and 1 Multi-Service TICAPs) agencies that have demonstrated an ability to meet at least 90% of the TIC capabilities for becoming a Single or Multi-Service provider.

E) The total number of TICs that should be allocated is less than 100 (79 target connections identified by agencies and approximately 10 TIC locations for future use by NETWORX TICAPs).

F) Schedule meetings to discuss federal enterprise level considerations to include: network topology, bandwidth, fault tolerance, baseline audit compliance, EINSTEIN deployment, and to address international TIC locations.

G) Schedule meetings with agencies to finalize TIC locations and reconcile differences between the number of agency-reported target connections and calculated number of target connections.

H) Establish a government-wide TICAP program plan to include implementation and CONOPS. The plan should be coordinated with DHS and agency CIOs.

I) Establish a cross-agency coordinating group to provide practical feedback into the government-wide TIC implementation plan.

J) Modify the existing ISS LoB FSSGB charter to include TIC governance and oversight.

K) Explore overall impact of TIC on state, municipal and local governments.

L) Provide TICAPs and customer agencies with guidelines to assist in transition planning.

Appendix A – Definition of Acronyms

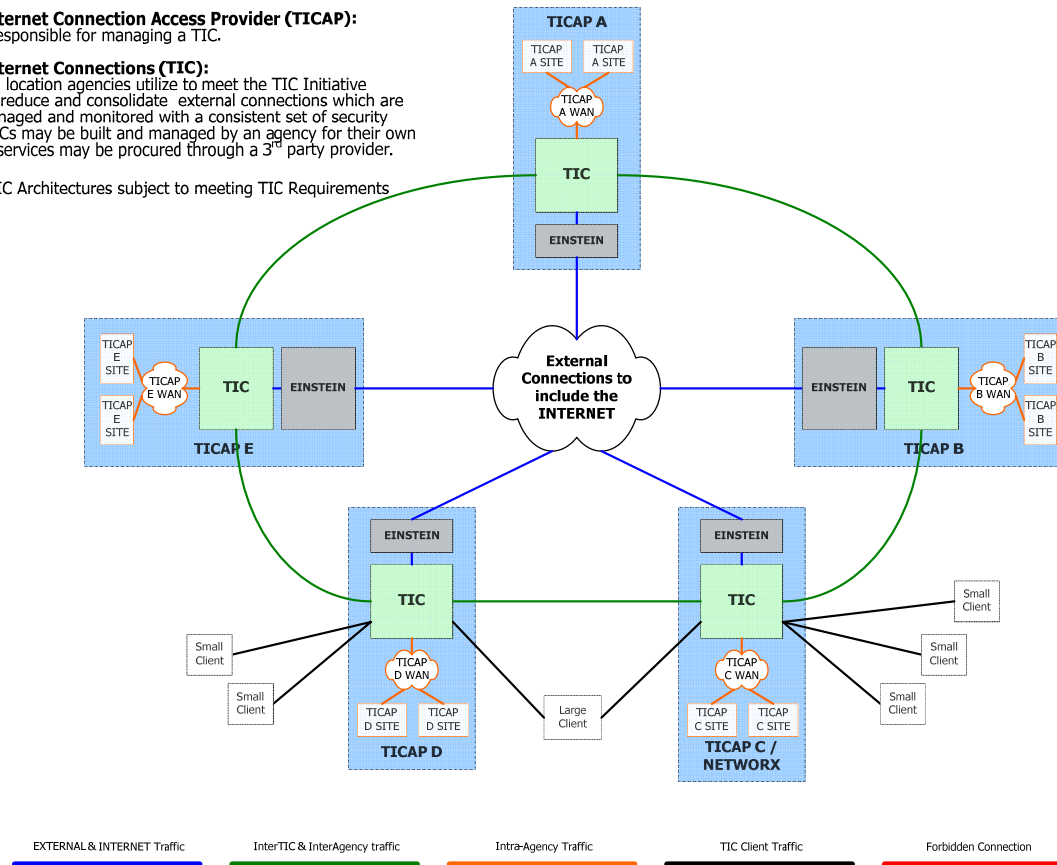| Acronym	Definition
CNDSP	Computer Network Defense Service Provider
DHS	Department of Homeland Security
FSSGB	Federal Systems Security Governance Board
ISS LoB	Information Systems Security Line of Business
ITI LoB	Information Technology Infrastructure Line of Business
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SOC	Statement of Capability
TIC	Trusted Internet Connections
TICAP	Trusted Internet Connections Access Provider

Appendix B – Conceptual TIC Architecture Diagram

Conceptual TIC Architecture:
TIC Enterprise Level Architecture

Trusted Internet Connection Access Provider (TICAP):
The entity responsible for managing a TIC.

Trusted Internet Connections (TIC):
The physical location agencies utilize to meet the TIC Initiative objective to reduce and consolidate external connections which are securely managed and monitored with a consistent set of security controls. TICs may be built and managed by an agency for their own use, or TIC services may be procured through a 3rd party provider.

* Internal TIC Architectures subject to meeting TIC Requirements

TICAP A
- TICAP A SITE
- TICAP A SITE
- TICAP A WAN
- TIC
- EINSTEIN

External Connections to include the INTERNET

TICAP E
- TICAP E SITE
- TICAP E SITE
- TICAP E WAN
- TIC
- EINSTEIN

TICAP B
- EINSTEIN
- TIC
- TICAP B WAN
- TICAP B SITE
- TICAP B SITE

TICAP D
- EINSTEIN
- TIC
- TICAP D WAN
- TICAP D SITE
- TICAP D SITE
- Small Client
- Small Client
- Large Client

TICAP C / NETWORX
- EINSTEIN
- TIC
- TICAP C WAN
- TICAP C SITE
- TICAP C SITE
- Small Client
- Small Client
- Small Client
- Small Client

Legend:
- EXTERNAL & INTERNET Traffic
- InterTIC & InterAgency traffic
- Intra-Agency Traffic
- TIC Client Traffic
- Forbidden Connection

Appendix C – Agencies Seeking Service[3]

Agencies Seeking TIC Services	
Advisory Council on Historic Preservation	JFK Assassination Records Review Board
Affordable Housing and Bank Enterprise	Legal Services Corporation
Affordable Housing Program	Marine Mammal Commission
American Battle Monuments Commission (ABMC)	Merit Systems Protection Board
Appalachian Regional Commission	Millennium Challenge Corporation (MCC)
Architectural and Transportation Barriers Compliance Board	Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation
Arlington National Cemetery	National Archives and Records Adminstration (NARA)
Barry Goldwater Scholarship and Excellence in Education Foundation	National Capital Planning Commission
Broadcasting Board of Governors (BBG)	National Commission on Libraries and Information Science
Chemical Safety and Hazard Investigation Board	National Council on Disability
Christopher Columbus Fellowship Foundation	National Credit Union Administration
Commission of Fine Arts	National Education Goals Panel
Commission on Ocean Policy	National Endowment for Humanities (NEH)
Committee for Purchase from People who are Blind or Severely Disabled	National Endowment for the Arts (NEA)
Commodities Futures Trading Commission (CFTC)	National Gallery of Art (NGA)
Community Empowerment Board	National Labor Relations Board (NLRB)
Consumer Product Safety Commission	National Mediation Board
Corporation for National and Community Service	National Science Foundation (NSF)
Corporation for Public Broadcasting	National Transportation Safety Board (NTSB)
Corps of Engineers	National Veterans Business Development Corporation
Court Services & Offender Supervision Agency (CSOSA)	Neighborhood Reinvestment Corporation
Defense Nuclear Facilities Safety Board	Nuclear Regulatory Commission (NRC)
Delta Regional Authority	Nuclear Waste Technical Review Board (NWTRB)
Denali Commission	Occupational Safety and Health Review Commission (OSHRC)
Department of Labor (DOL)	Office of Federal Housing Enterprise Oversight (OFHEO)
District of Columbia Courts	Office of Government Ethics
Election Assistance Commission	Office of Navajo and Hopi Indian Relocation
Electric Reliability Organization	Office of Special Counsel
Equal Employment Opportunity Commission (EEOC)	Oklahoma City National Memorial Trust
Export Import Bank	Other Civil Defense Programs
Farm Credit Administration (FCA)	Other Commissions and Boards
Farm Credit System	Overseas Private Investment Corporation (OPIC)
Farm Credit System Financial Assistance Corporation	Pacific Chapter Commission
Farm Credit System Insurance Corporation	Panama Canal Commission
Federal Communications Commission	Peace Corps
Federal Deposit Insurance Corporation	Pension Benefit Guaranty Corporation (PBGC)
Federal Drug Control Programs	Postal Regulatory Commission (PRC)
Federal Election Commission	Postal Service
Federal Financial Institutions Examination Council Appraisal Subcommittee	Presidio Trust
Federal Home Loan Bank System	Resolution Trust Corporation
Federal Home Loan Mortgage Corporation	SEC Public Accounting Oversight Board
Federal Housing Enterprise Regulator	SEC Standard Setting Body
Federal Housing Finance Board (FHFB)	Selective Service
Federal Labor Relations Authority	Small Business Administration (SBA)
Federal Law Enforcement Training Center	State Justice Institute
Federal Maritime Commission	Student Loan Marketing Association
Federal Mediation and Conciliation Service	Telecommunications Development Fund
Federal Mine Safety and Health Review Commission	Tennessee Valley Authority
Federal National Mortgage Association	U.S. Agency for International Development (USAID)
Federal Retirement Thrift Investment Board	U.S. Canada Alaska Rail Commission
Federal Trade Commission	U.S. Commision on Civil Rights (USCCR)
Financing Vehicles and the Board of Governors of the Federal Reserve	U.S. Court of Appeals for Veterans Claims
Harry S. Truman Scholarship Foundation	U.S. Enrichment Corporation Fund
Institute of American Indian and Alaska Native Culture and Arts Development	U.S. Holocaust Memorial Museum
Institute of Museum and Library Services	U.S. Institute of Peace
Intelligence Community Management Account	U.S. Interagency Council on Homelessness
Inter-American Foundation	U.S. Patent and Trademark Office (USPTO)
International Assistance Programs (does not include USAID)	U.S. Trade and Development Agency (USTDA)
International Trade Commission	United Mine Workers of America Benefit Funds
James Madison Memorial Fellowship Foundation	US Railroad Retirement Board (USRRB)
Japan-United State Friendship Commission	Vietnam Education Foundation
	White House Commission on the National Moment of Remembrance

---

[3] This is not an exhaustive list and will be continually updated.