Trusted Internet Connections (TIC) Reference Architecture Document Version 2.2

Federal Interagency Technical Reference Architectures
June 19, 2017

Homeland Security

Federal Network Resilience

Revision History

Date	Version	Description	Approved By
4/20/09	1.0	Agency feedback incorporated and released	M.A. Brown, RADM, USN DAS Cybersecurity & Communications, DHS
3/24/2011	2.0	Capabilities and architecture updated by the TIC 2.0 Working Group. Final version prepared by DHS.	M. Coose Director, Federal Network Security, DHS
9/1/2011	2.0	Final approval by OMB and reference to M-11-11.	M. Coose Director, Federal Network Security, DHS
9/16/2013	2.0	Added Appendix H – Cloud Considerations.	John Streufert Director, Federal Network Resilience, DHS
6/9/2017	2.2	Modified Secure communications from Critical to Recommended	Mark Kneidinger Director, Federal Network Resilience, DHS

Table of Contents

Table of Figures

Acknowledgements

This document is the product of ongoing multi-agency collaboration to provide additional guidance for the successful implementation of the Trusted Internet Connections (TIC) Initiative. A number of agencies have provided resources to support the creation and revision of the TIC Technical Architecture Document and have made information systems security a priority in their strategic plans. We especially thank the Department of Interior for providing the original template for the document.

This document will be reviewed on an annual basis and will be updated as necessary to incorporate required capabilities and applicable interoperability standards.

Original TIC Technical Architecture Strategy Team Members

Name	Agency	Name	Agency
Bill Vajda	OMB	Ed Roback	Treasury
Kshemendra Paul	OMB	David Sczepanski	EPA
David Wheelock	UCIA	Tim Thorpe	EPS
Earl Crane	DHS	Frank Tiller	GSA
Alma Cole	DHS	Brett Moseley	NIH
Ken Reynolds	DHS	Renita Andersen	NIH
Mike Kern	DHS/US-CERT	Scott Cory	NIH
Mischel Kwon	DHS/US-CERT	Mike Milazzo	HUD
Brian Done	DHS	Porter Davis	HUD
Dennis Ruff	DISA	Don Sheehan	VA
Damian Hayes	DISA	Brian Campbell	VA
David Sacha	DISA	Eric Won	GSA
John Unekis	NOAA	Betsy Edwards	NASA
Bernie Werwinski	NOAA	Jerry Davis	NASA
Jeff Bugler	DISA	Ken White	NASA
Paul Filios	DISA	Andrew Good	OPM
Tony Bailey	DOE	James Berry	OPM
Jim Sledge	DOE	Joseph Song	OPM
David Elliott	EDU	Hung Dinh	SEC
Harry Feely	EDU	Evan Trebing	SEC
James Albin	EDU	Bhupinder Singh	SEC
Leland Dudek	DOI	Brad Tesh	Smithsonian
Stu Mitchell	DOI	Bruce Daniels	Smithsonian
Matt Raymer	DOJ	Bob Nicholson	SSA
Nathan Rickman	DOJ	Gerry Barsczewski	SSA
Robert Martin	DOJ	Jack Leipold	SSA
Jacob D. (Danny) Toler	DOS	John Donovan	USDA
Sara Nasseh-Mosley	DOS	Bill Flowers	USDA
Douglas Roseboro	FAA	Chuck Christopherson	USDA
Rick Swartz	Treasury	Dan Crosson	USDA
Timothy Clinton	Treasury	Steve Wilson	USDA
Ranny Reynolds	Treasury	Everett Dowd	DOT

Key Stakeholders

Office of Management and Budget (OMB), Office of E-Government and Information Technology

Federal Chief Information Office (CIO) Council

Federal Small Agency CIO Council

Department of Homeland Security (DHS) National Cyber Security Division (NCSD)

Federal Systems Security Governance Board (FSSGB)

DHS Information Systems Security Line of Business (ISS LoB)

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

General Services Administration (GSA) Information Technology Infrastructure Line of Business (ITI LoB)

All Federal Executive civilian agencies

Advisors

Alan Paller, Director of Research, SANS Institute

Scott Bradner, Technology Security Officer, Harvard University

TIC 2.0 Update Participants

In FY2010, TIC Access Provider (TICAP) representatives from across the Federal government participated in the TIC 2.0 Working Group to provide updates to this architecture document.

Sean Donelan	DHS TIC PMO	David Elliott	EDU
Marilyn Rose	DHS TIC PMO	Stephen Luhan	FBI
Samuel Vazquez	DHS TIC PMO	Harry Trebing	SEC
Matt Coose	DHS	Evan Trebing	SEC
Donald Benack	DHS	John Heppler	SEC
Blake Nguyen	DHS	Dave Wilson	SEC
Kara McKenzie	DHS	Bhupinder Singh	SEC
Alma Cole	DHS	Gerry Barszczewskie	SSA
Brian Done	DHS	Sean Connelly	State
Keith Trippie	DHS	Ranny Reynolds	Treasury
Jack Burriesci	DHS	Tom Tran	IRS
Earl Crane	ISIMC NISSC	James Maginnis	VA
John Migliaccio	GSA	Don Sheehan	VA
Olga Aparicio	GSA	Georgia Killcrece	SEI
William Lakner	DOL	Russell Griffin	SEI
Rana Faisal	DOL	Rob Moore	TIC PMO
Stu Mitchell	DOI	Neil Paine	TIC PMO
Martha Pogue	DOT	Mike Robinson	TIC PMO
Chuck Eng	DOT/FAA		

TIC Technical Architecture Document Team Members

SRA/Touchstone Consulting Group

The Software Engineering Institute

Blue Glacier Management Group

The MITRE Corporation

Introduction

The overall purpose of the Trusted Internet Connection (TIC) Initiative, as outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet. The initiative will improve the Federal Government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections.

Updates and Changes in the TIC 2.0 Architecture

Several new sections and appendices have been added in this version of the TIC Architecture. They include an update of applicable TIC policy references, additional guidance for securing remote access connections, a clarification of agency responsibilities for securing inter-agency and intra-agency connections, recommendations for network time protocols, and guidance for agency Domain Name System (DNS) deployment. Appendices for glossary and acronyms have also been added to help in clarifying language within the document.

One of the most important updates to the TIC Architecture is a refresh of the TIC Critical Capabilities for securing TIC access points. The purpose of this update was to enhance the security posture of federal departments and agencies by defining more robust network security defense capabilities by updating, clarifying, adding and removing capabilities as deemed necessary. Recommendations and comments from various agencies and security groups are incorporated into this document and are presented in the revised capability list in Appendix B.

Scope of the Document

The TIC Architecture document is intended as a reference to provide insight and guidance for Departments/Agencies (D/As) striving to comply with the requirements of the TIC Initiative. The TIC Architecture document was developed by the TIC 2.0 Working Group. The team consisted of representatives from a diverse group of agencies in order to define end user technical needs and to select approaches to meet those needs. The document is descriptive in nature, recognizing that many organizations face unique challenges that do not lend themselves to "one size fits all" solutions. The document does not prescribe specific solutions. Its intent is to enable agencies to leverage existing capabilities in order to achieve the overall objectives of the TIC Initiative.

This document is applicable to all Federal civilian agencies, but particularly to TIC Access Providers (TICAPs). A TICAP is the entity responsible for managing a TIC access point's physical location and corresponding security capabilities. Single Service TICAPs serve as a TIC Access Provider only to themselves. Multi-Service TICAPs provide TIC services to other agencies through a shared services model.

All other Federal civilian agencies are designated as "Seeking Service" and must acquire TIC services from an approved Multi-Service TICAP. Most Seeking Service Agencies will procure TIC services through a third party provider such as the GSA NETWORX contract vehicle.

Participation and cooperation between the National Cyber Protection Program (NCPP) and the TIC Initiative is necessary to ensure all external connections are monitored by a National Cyber Protection System (NCPS) sensor, operationally known as EINSTEIN. NCPP is a distinct program with its own set of requirements, which are not repeated in this document. A TICAP is responsible for interconnection with NCPS components according to the terms and conditions outlined in the memorandum of agreement, interconnection security agreement and service level agreement between the TICAP and US-CERT.

The information in this document is based upon the definitions and requirements in the Federal Information Systems Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance and standards, and Office of Management and Budget (OMB) memoranda.

TIC Policy References

The Trusted Internet Connections (TIC) Initiative is derived from the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23. The TIC Initiative is the first of twelve initiatives in the President's Comprehensive National Cybersecurity Initiative (CNCI). The following OMB Memoranda have been published to help agencies comply with the TIC Initiative[1]:

- OMB M-08-05: Implementation of Trusted Internet Connections (TIC)
- OMB M-08-16: Guidance for Trusted Internet Connection Statement of Capability (SOC) Form
- OMB M-08-26: Transition from FTS2001 to NETWORX
- OMB M-08-27: Guidance for Trusted Internet Connection (TIC) Compliance
- OMB M-09-32: Update on the Trusted Internet Connections Initiative

A comprehensive list of applicable legislation, policies, directives, regulations, memoranda, standards, and guidelines can be found in Appendix I.

---

[1] The OMB memos can be found at the following link: http://www.whitehouse.gov/omb/memoranda/

TIC Clarification

The term "TIC" is used throughout the Federal Government to denote different aspects of the TIC Architecture; including the overall TIC initiative, a physical TIC access point and a TIC Access Provider. In order to avoid confusion, this document will minimize use of the term "TIC" to describe the machinery of the TIC Architecture. "Appendix C – Glossary: Common Terms and Definitions" and "Appendix D – Acronyms: Common Abbreviations" can be referenced in the Appendices of this document to help clarify content.

TIC Trust Relationships

Conceptually, the TIC Architecture is organized around three zones of trust: an external zone, a TIC Zone, and a D/A Internal Zone. Although there are generally more security zones within a D/A network, this document conceptually simplifies the zones associated with network connections.

Figure 1 depicts the target TIC Trust Relationships and is intended to articulate two points. First, the amount of control an agency has over the environment decreases as traffic flows away from the Internal Zone toward the External Zone. Second, as the agency's level of control decreases, the level of trust an agency places on the relationship between the two entities exchanging traffic also decreases.

Figure 1: Conceptual Model for TIC Trust Relationships
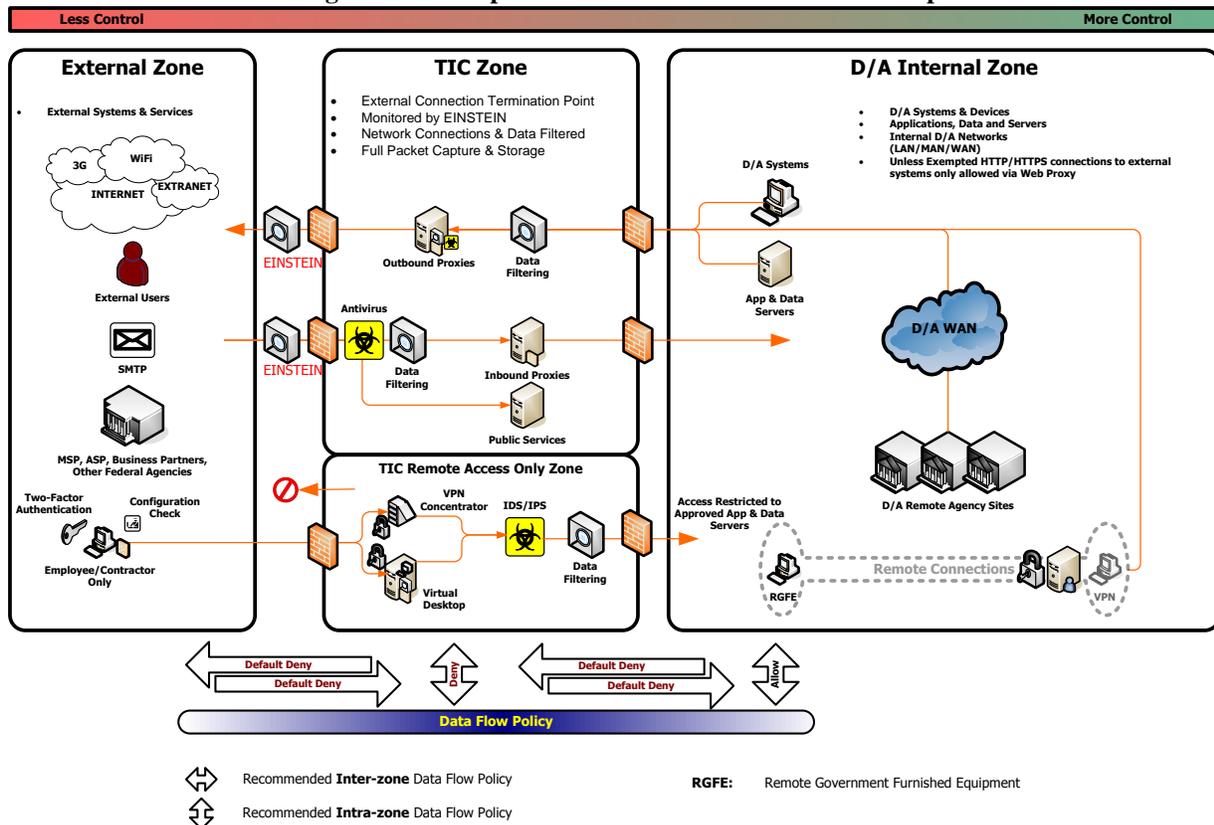
- External Zone: Information systems or components of information systems that are outside of the accreditation boundary established by the organization and over which the organization typically has no direct control for the application of required security controls or the assessment of security control effectiveness.
- Internal Zone: Information systems or components of information systems that are within the accreditation boundary established by the organization and for which the organization typically has direct control for the application of required security controls or the assessment of security control effectiveness.
- TIC Zone: Border between an organization's internal infrastructure (users, systems, data) and external resources. Serves as the termination point for external connections and utilizes a standard set of security controls to monitor, authenticate, and filter data flows that enter/exit the TIC access point.

Each zone (External, Internal, and TIC Zone) requires specific security functions applied to the systems and networks in order to provide specific security capabilities. When designing and implementing secure and trusted connections, agencies should consider all of the controls mentioned in the *TIC Taxonomy and Associated Security Patterns* Section. The security patterns described in this document define level of trust criteria for different connection classes, and therefore guide application of specific security functions and capabilities.

Conceptual TIC Architecture

Figure 2 depicts the conceptual TIC Architecture. The graphic illustrates three different models that Federal civilian agencies may employ to reduce and consolidate their external network traffic via a secure and trusted connection: (1) Agency Multi-Service TICAP, (2) Agency Single Service TICAP and (3) Managed Trusted IP Service (MTIPS) TICAP (via approved NETWORX Vendor).

Figure 2: Conceptual TIC Architecture
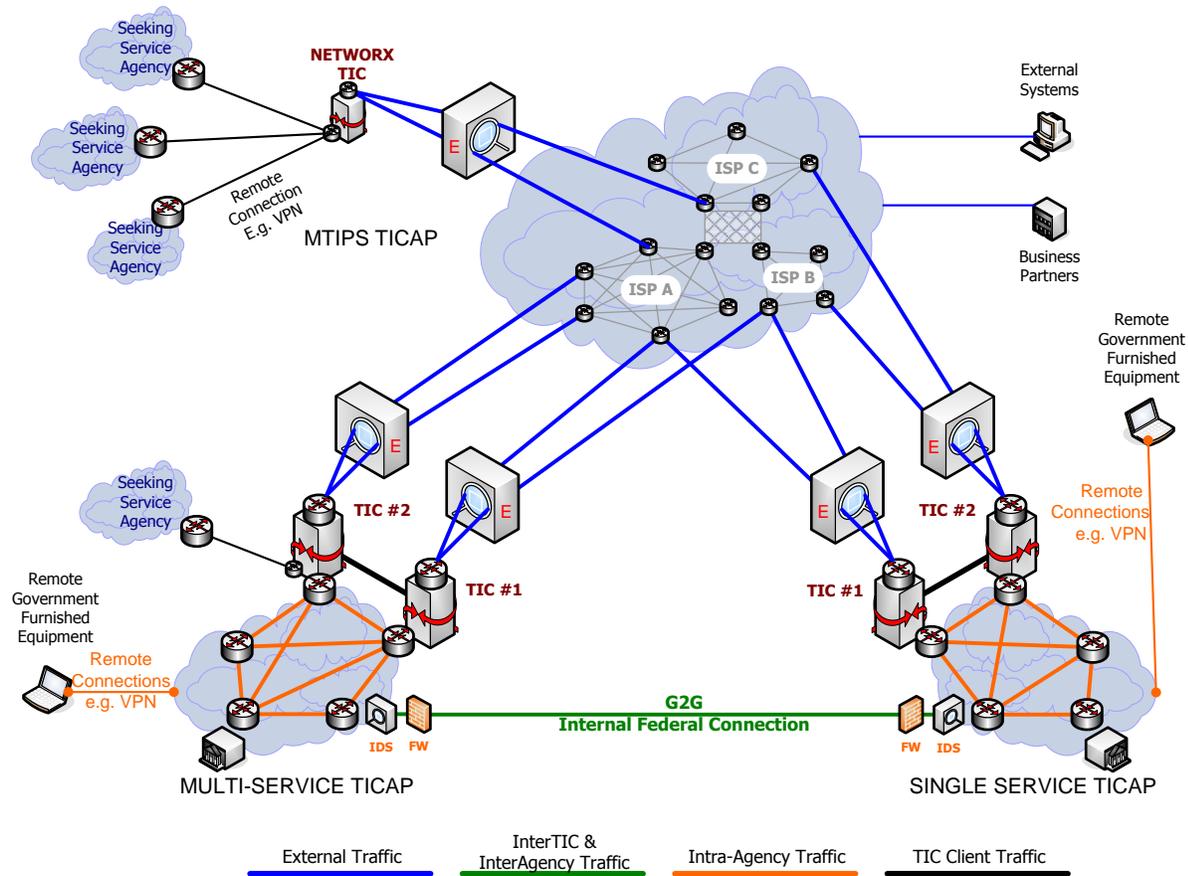
The Architecture classifies all agency network connections according to four connection classes: External, Inter-Agency, Intra-Agency, and TIC System. Regardless of the agency's reduction and consolidation model, note how all external connections are secured through a TIC access point. The connection classes are explained in further detail in the next section of this document, *TIC Taxonomy and Associated Security Patterns*.

Security Pattern for each Connection Class

Each of the four connection classes in Figure 2 requires a unique security pattern in order to build a necessary level of trust between connections. Each security pattern consists of specific security functions, capabilities, guidelines, and characteristics. The patterns describe collections of systems operating under a common security policy (i.e., same level of security) and the same security functions may span multiple security patterns. Figure 3 illustrates the Taxonomy of a Security Pattern; specifically the relationship between a Connection Class, the Security Functions necessary to support that Connection Class, and the resulting TIC Capabilities attained when those Security Functions are met.

Figure 3: Taxonomy of a Security Pattern
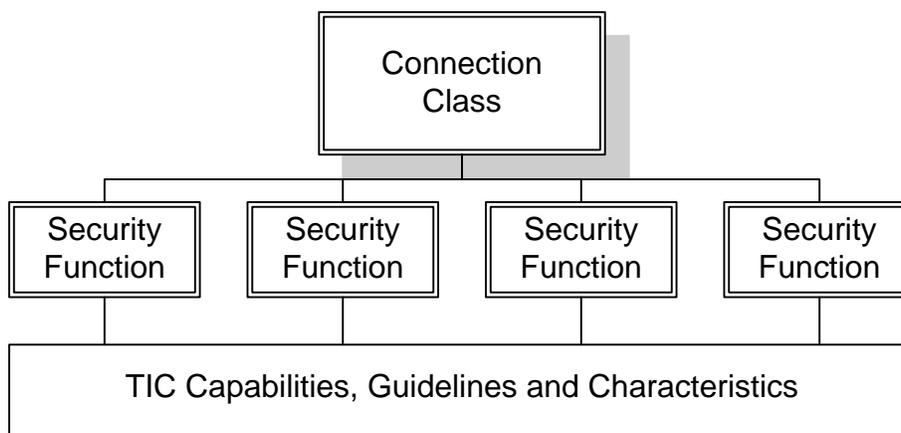
The taxonomy of a security pattern consists of three major components:

- **Connection Class:** A telecommunications class or pattern for data/information flow into and out of D/A information systems, networks, or components of information systems and networks. As demonstrated in Figure 2, the four Connection Classes are: External, Inter-Agency, Intra-Agency, and TIC-System. Each connection class requires a unique security pattern in order to build a necessary level of trust.

- **Security Function:** The operations that must be performed and functionalities that must be provided in order to secure a connection class. TICAPs are responsible for managing these security functions by meeting the appropriate TIC Capabilities outlined in Appendix B. Security Functions are explained in more detail in the next section of this document, *Security Functions, Descriptions and Characteristics*.

- **TIC Capabilities:** The tasks, configurations, requirements and specifications that must be delivered to provide specific security function(s). Many capabilities may contribute to the performance of multiple security functions. Appendix B provides a complete list of the TIC Capabilities and correlates each capability to its associated Security Function.

  Each capability is categorized as Critical or Recommended. All Critical capabilities must be satisfied to be compliant with the TIC Architecture. Recommended capabilities are best practice guidelines, and while not currently required for compliance, are strongly suggested as best practices. Appendix B contains the complete list of TIC Capabilities.

Security Pattern #1: External Connections

External Connection Class Definition: A physical or logical connection between information systems, networks, or components of information systems and networks in which one is inside and the other outside of the specific Certification and Accreditation (C&A) boundaries established by the D/A, where:

(a) 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

(b) 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

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

Further clarification is available in Appendix A, which provides the OMB-approved "Definition of External Connection."

Corresponding Security Functions: Each TICAP must demonstrate that external connections are secured by a TIC access point providing four specific security functions:

a. Packet Filtering (Critical)
b. Content Filtering (Critical)
c. Proxy (Critical)
d. Intrusion Detection and Prevention System (IDPS) (Critical)

Figure 4 below indicates the four security functions that are associated with the External Connections security pattern. NCPS Monitoring is highlighted to indicate that agencies must participate in and work with the NCPP to ensure all external connections are monitored by an NCPS device.

Figure 4: External Connection Security Pattern
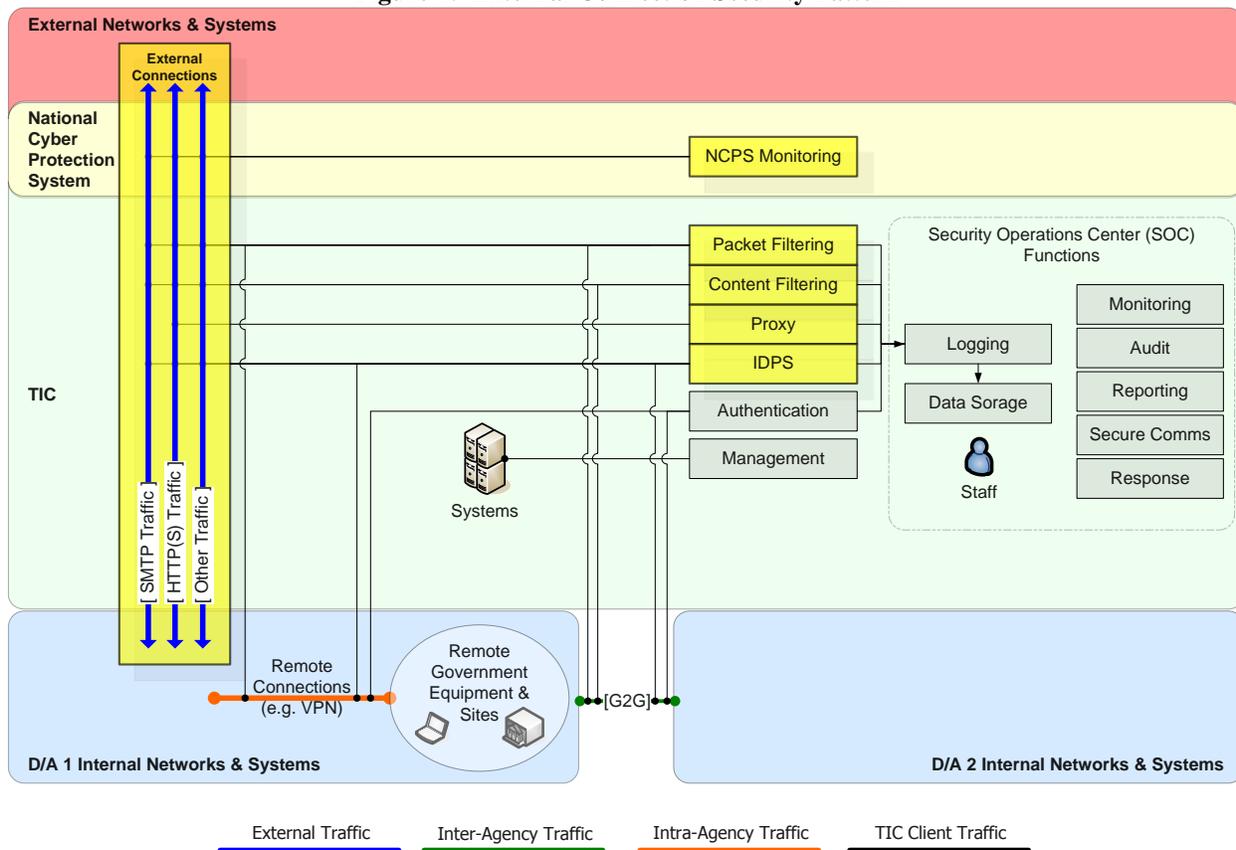
Security Pattern #2: Inter-Agency (Internal Partners) Connections

Inter-Agency Connection Class Definition: Connections that allow for the flow of network traffic between D/As in support of mission objectives and business operations.

Interconnections among D/As may be considered "internal connections" when all D/As involved in the interconnect are fully behind TIC access points and the following four criteria are met:

- All of the D/As' external connections route through a TIC access point
- All of the D/As' other connections (Intra-Agency, Inter-Agency) are consistent with the definition of an external connection in sections (4.1) and (4.2) in Appendix A
- All D/As perform packet screening to ensure that only authorized traffic is permitted to flow between the interconnected D/As
- All D/As maintain the ability to suspend/temporarily deactivate the connection in the event that suspicious activity is detected

It is also recommended that all D/As monitor the connection at the point of ingress into their C&A boundary using the following security functions: content filtering, IDPS, and authentication.

In an instance where there is reasonable doubt as to whether a connection is "internal" or "external", the traffic must be considered "external" and routed through a TIC access point. Additional guidance for managing risk of information systems, including consideration factors agencies should employ when establishing direct control, is further articulated in Appendix A.

Corresponding Security Functions: Federal civilian agencies secure their inter-agency connections with the following security functions:

    a. Packet Filtering (Critical)
    b. Content Filtering (Recommended)
    c. IDPS (Recommended)
    d. Authentication (Recommended)

Figure 5 below indicates the four security capabilities that are associated with the Inter-Agency Connections security pattern.

Figure 5: Inter-Agency Connection Security Pattern
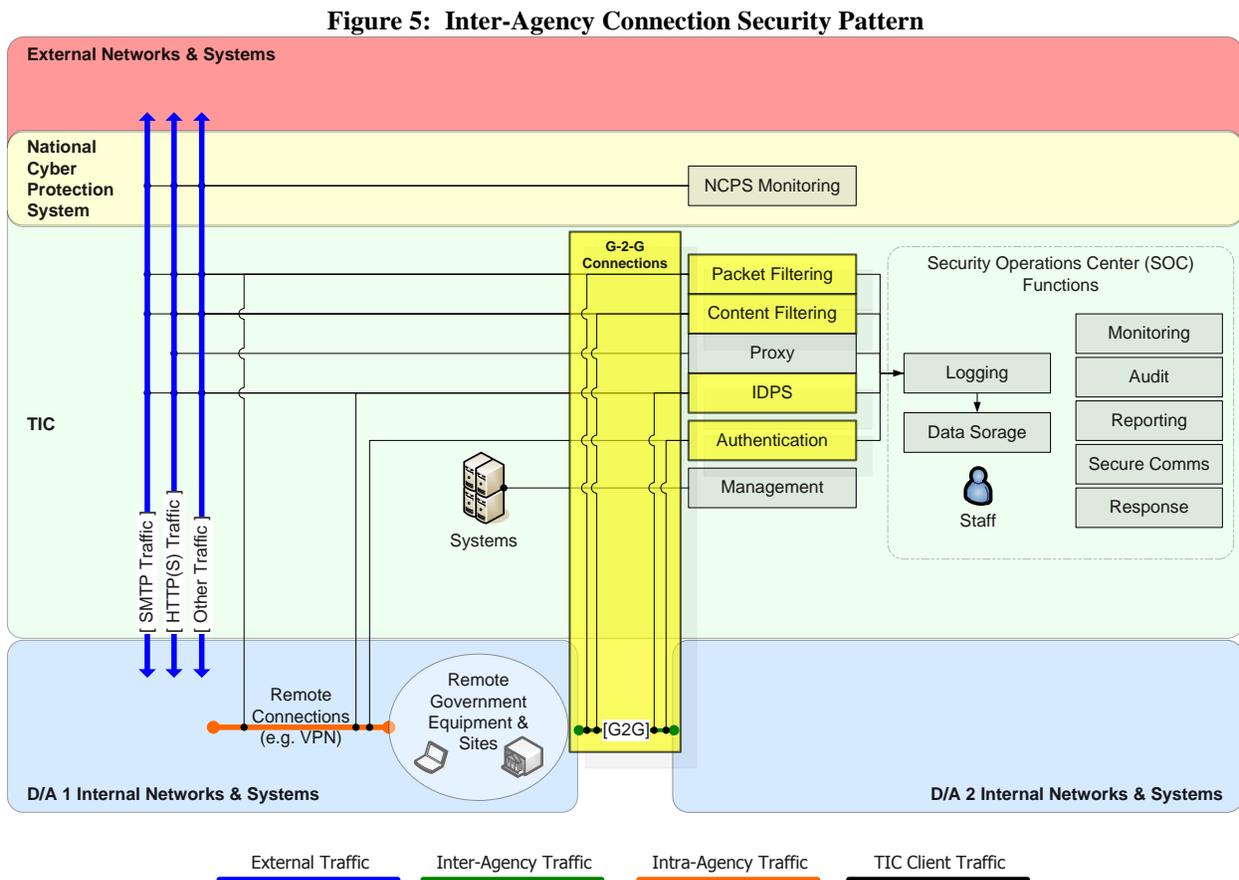
Security Pattern #3: Intra-Agency (Internal Partners) Connections

Intra-Agency Connection Class Definition: Secure connections that link D/A systems, networks, or components to the D/A enterprise. These resources reside outside of the enterprise security perimeter but become part of the enterprise security perimeter via required security services such as authentication and virtual private network (VPN). Since these resources are considered a logical extension of the internal network, these types of connections are also referred to as "internal connections." Further clarification about the distinction between External connections and Intra-Agency connections can be found in Appendix A.

Connections which meet the following criteria can be classified as Intra-Agency connections and will <u>NOT</u> typically be considered "external connections". As a result, they would not be required to route through a TIC access point, though may do so at the D/A's discretion:

- Dedicated secure point-to-point connections that link information systems, networks, or components of information and systems and networks of a single D/A under a single certification and accreditation authority, provided that the connections do not access the globally-addressable internet

- Connections established through VPN technology utilizing security controls that at a minimum are compliant with FIPS 140-2 and NIST 800-53 and are audited and monitored by the D/A

Corresponding Security Functions: Federal civilian agencies secure their Intra-Agency connections with the following security functions:
  a. Packet Filtering (Critical)
  b. IDPS (Recommended)
  c. Authentication (Recommended)

Further details regarding Remote Access connections can be found in Appendix E – Guidance for Remote Access Connections.

Figure 6 depicts the three security capabilities that are associated with the Intra-Agency Connections security pattern.

Figure 6: Intra-Agency Connection Security Pattern
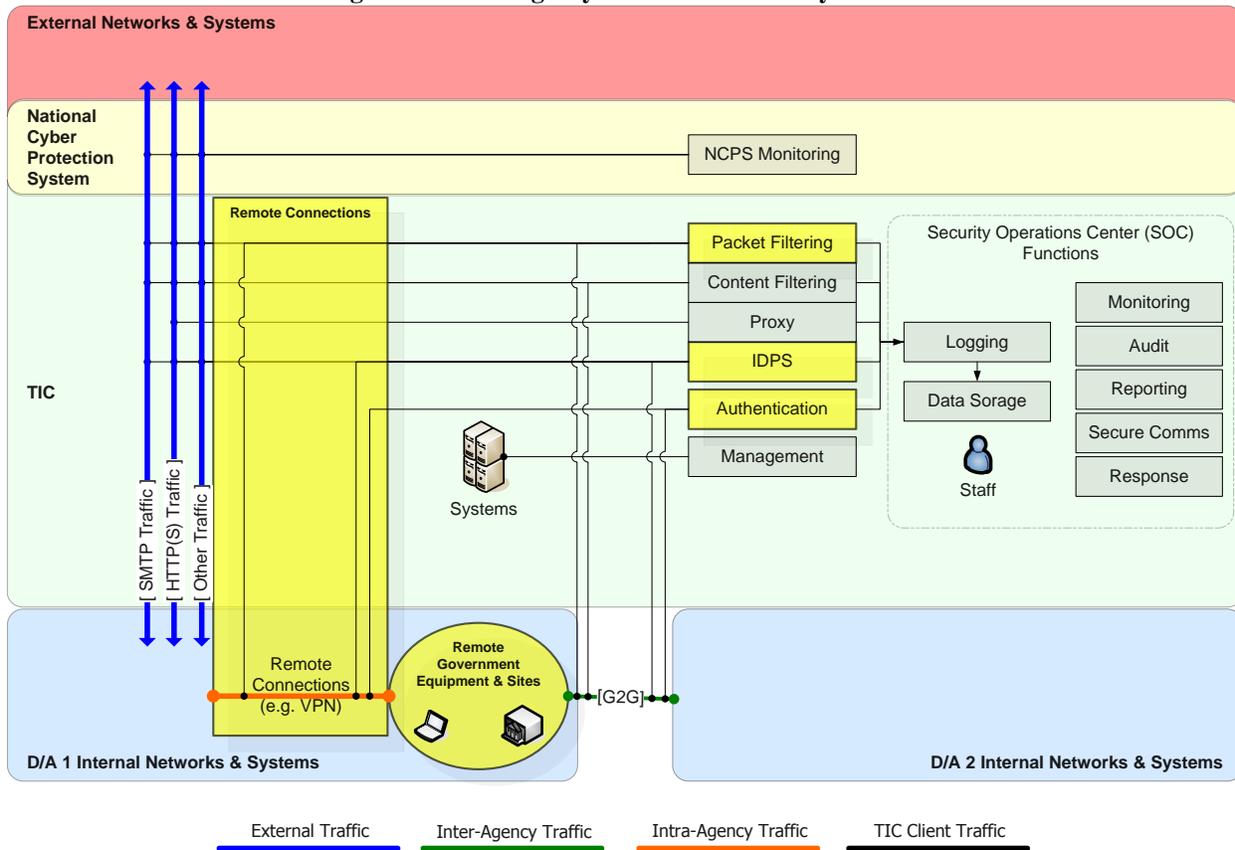
Security Pattern #4: TIC Systems

TIC System Connection Class Definition: TIC systems are components and services that support the overall security operations and policies of the TIC access point, including components that collect, normalize, and analyze log data as well as those involved in incident response and reporting. This includes overall management of TIC components as well as capabilities associated with managing a Security Operations Center (SOC), and a Network Operations Center (NOC). Periodic validation of TIC operations and security posture is required.

The Functional Block diagram (Figure 7) is intended to show the relationship between the components and systems that exist at a TIC access point. All functions and services contained in this diagram are included as Critical TIC Capabilities and are elaborated in more detail in Appendix B.   This graphic is not intended to be an engineering schematic but rather an illustration of the components and services included in a TIC system.

Figure 7: TIC Access Point Functional Block Diagram[2]

Prepared By:
Federal Network Security
US Dept of Homeland Security
Last Updated: January 20, 2011
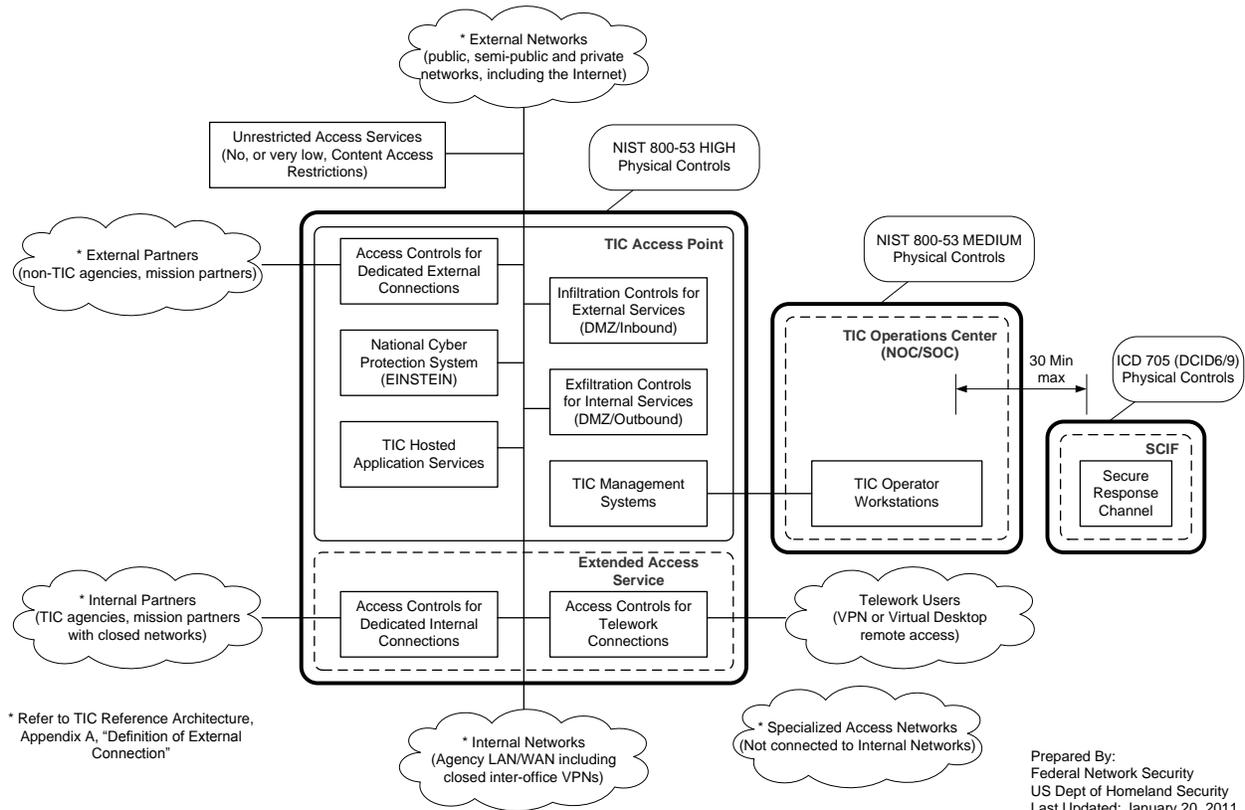
Corresponding Security Functions: Securing a TIC system depends on a D/A's ability to provide a mix of management and security operations functions. Security capabilities for TIC systems protect the TIC layer itself and specify monitoring, logging and reporting capabilities that the TIC access point must provide. Each TICAP must demonstrate that TIC systems and components meet the following security functions:

        a.   Management
           i.   Physical Controls
          ii.   TIC Configuration
         iii.   Authentication
        b.   Remote Access
        c.   Secure Communications
        d.   Data Storage
        e.   Logging
        f.   Response
        g.   Monitoring
        h.   Audit
        i.   Reporting

---

[2] Many of the terms and acronyms used in Figure 7 are defined in Appendix C or spelled out in Appendix D.

Figure 8 depicts the management and security capabilities that are associated with TIC system Connections security pattern.

Figure 8: TIC Systems Security Pattern
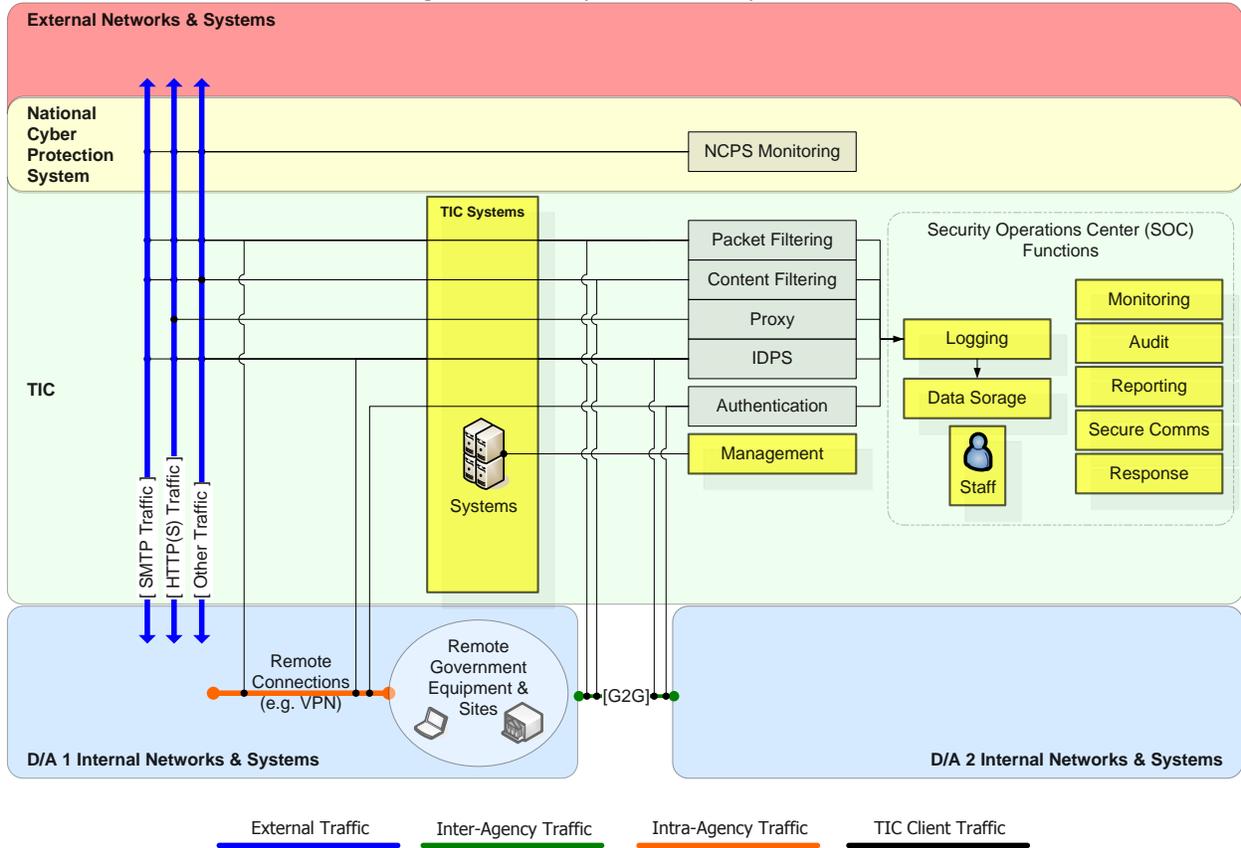
Security Functions, Descriptions and Characteristics

Based upon the concepts developed in previous sections, this section provides a brief description of each security capability for future reference. Selected applicable characteristics associated with each capability are listed in the tables below the respective heading. These characteristics are not new requirements, but highlights of existing NIST guidance and standards set forth in NIST Special Publication 800-53, 800-53A and subsequent publications, federal laws, standards and guidelines.

When securing external connections, the first four security functions are mandatory and are performed "*by* the TIC access point." For Inter-Agency and Intra-Agency connections, these security functions are recommended, but would not be required to route through a TIC access point. The last 10 security functions all relate to securing the TIC systems and components themselves. These functions are performed "*on* the TIC access point." The mandatory security functions below can be traced to one or more TIC Critical Capabilities in Appendix B.

Figure 9: Relationship Between Security Functions and Connections Classes

		Security Pattern			
		External Connections	Inter-Agency Connections	Intra-Agency Connections	TIC Systems
Security Functions	Packet Filtering	**M**	**M**	**M**	
	Content Filtering	**M**	**R**		
	Proxy	**M**			
	IDPS	**M**	**R**	**R**	
	Authentication		**R**	**R**	**M**
	Remote Access				**M**
	Management				**M**
	Logging				**M**
	Data Storage				**M**
	Monitoring				**M**
	Audit				**M**
	Reporting				**M**
	Secure Communications				**M**
	Response				**M**
M= Mandatory Security Function			**R= Recommended Security Function**		

a) NIST Guidance:

Packet Filter: Firewalls that are only packet filters - also known as stateless inspection firewalls - are essentially routing devices that provide access control functionality for host addresses and communication sessions. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a rule set. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists (NIST 800-41 rev1).

Stateful Inspection: Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule. Unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.

Three major states exist for Transmission Control Protocol (TCP) traffic - connection establishment, usage, and termination (which refers to both an endpoint requesting that a connection be closed and a connection with a long period of inactivity). Stateful inspection in a firewall examines certain values in the TCP headers to monitor the state of each connection. Each new packet is compared by the firewall to the firewall's state table to determine if the packet's state contradicts its expected state. For example, an attacker could generate a packet with a header indicating it is part of an established connection, in hopes it will pass through a firewall. If the firewall uses stateful inspection, it will first verify that the packet is part of an established connection listed in the state table (NIST 800-41 rev1).

Deep Packet Inspection: A newer trend in stateful inspection is the addition of a stateful protocol analysis capability, referred to by some vendors as deep packet inspection. Stateful protocol analysis improves upon standard stateful inspection through adding basic intrusion detection technology - an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations. This enables the identification of unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent. These suspicious commands often originate from buffer overflow attacks, denial of service (DoS) attacks, malware, and other forms of attack carried out within application protocols such as Hypertext Transfer Protocol (HTTP). Another common feature is input validation for individual commands, such as minimum and maximum lengths for arguments. For example, a username argument with a length of 1000 characters is suspicious - even more so if it contains binary data (NIST 800-41 rev1).

b) Selected Packet Filtering Characteristics:

Common Characteristics	Source
▪ Firewall policies should only permit appropriate source and destination IP addresses to be used.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Traffic with invalid source or destination addresses should always be blocked.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an "external" address) should be blocked at the network perimeter.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Incoming traffic with a destination address of the Packet Filtering device should be blocked unless the firewall is offering services for incoming traffic that require direct connections - for example, if the firewall is acting as a proxy.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Organizations should also block traffic containing IP source routing information, which allows a system to specify the routes that packets will employ while traveling from source to destination.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ Organizations should also block traffic containing directed broadcast addresses, which are broadcast addresses that are not in the same subnet as the originator.	SP 800-41 Rev 1 (paragraph 4.1.1)
▪ The Packet Filtering device should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.	SP 800-41 Rev 1 (paragraph 4.1.2)
▪ The administrative interface should allow administrators to clone IPv4 rules to IPv6 addresses to make administration easier.	SP 800-41 Rev 1 (paragraph 4.1.2)
▪ If the layer 3-5 device can filter based on DNS lookup of domain names, it needs to use AAAA (IPv6 address records) records in the same way as A records (those used for IPv4 addresses).	SP 800-41 Rev 1 (paragraph 4.1.2)
▪ The Packet Filtering device needs to be able to filter ICMPv6, as specified in RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls.	SP 800-41 Rev 1 (paragraph 4.1.2)
▪ SSL VPN devices should be configured so they log sufficient details regarding successful and failed login attempts to support troubleshooting and incident response activities.	SP 800-113 (Section 4.3.6)

a) NIST Guidance:

Content filtering is the process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. Two common types of content filtering are spam filtering software and Web content filtering software (NIST SP800-114).

Spam – unsolicited email – is often used to deliver spyware and other forms of malware to users (NIST SP800-114).

Web content filtering software typically works by comparing a Web site address that a user attempts to access with a list of known bad Web sites (NIST 800-114).

b) Selected Content Filtering Characteristics:

Common Characteristics	Source
▪ Content filtering should be done as close to the content receiver as possible.	SP 800-41 Rev 1 Section 5.2.2
▪ All content filtering products that are used should be kept up-to-date to ensure that their detection is as accurate as possible.	SP 800-114 Section 5.4.3

▪ In general, rules are defined to forward, quarantine, park, clean, block, or delete any data passing through the server depending upon the results of the scan. Typical items that would be caught by the filter and possible actions taken on them could be as follows:
    a) Email that contains suspicious active content (e.g., ActiveX, JavaScript) is stripped of the active code and forwarded to the recipient.
    b) Spam email and phishing attempts may be deleted or tagged as suspicious.
    c) Extra-large files might be held for delivery during off-peak hours.
	SP 800-45 Version 2 Section 6.2.2.1

▪ Another key feature of content filtering packages is the scanning of outbound data. A lexical analysis can be performed that scans email messages for words and phrases that might be viewed as inappropriate for use in organizational email.	SP 800-45 Version 2 Section 6.2.2.1

Common Characteristics	Source
▪ For maximum effectiveness, content filtering should be performed on all incoming and outgoing messages and conducted in the same locations as malware scanning - on the firewall/mail relay/mail gateway, mail servers, and end users' hosts.	SP 800-45 Version 2 Section 6.2.2.1

Security Function: Proxy

a) NIST Guidance:

Proxy: A proxy is an information system that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network, processes it, and forwards it. This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal IP addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hypertext Transfer Protocol (HTTP) proxy used for Web access and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail (NIST 800-44 Ver2).

Other definitions include:
    A server that sits between a client information system, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server; or

    An agent that acts on behalf of a requester to relay a message between a requester agent and a provider agent.

b) Selected Proxy Characteristics:

Common Characteristics	Source
▪ When a proxy is used, each successful connection attempt actually results in the creation of two separate connections.	SP 800-94
▪ The proxy may reject client requests that appear to be invalid (which could include some forms of attacks) and log information regarding these requests.	SP 800-94
▪ HTTP proxies should be configured on the firewall to block all inbound scripts and Java applications.	TIC 2.0 WG, FY2010

Security Function: IDPS

a) NIST Guidance:

Intrusion Detection: Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of potential incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (NIST 800-94).

Intrusion Prevention: Intrusion prevention is the process of performing intrusion detection and attempting to stop detected potential incidents. Intrusion Detection and Prevention Systems (IDPSs) are primarily focused on identifying potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPS technology has become a necessary addition to the security infrastructure of nearly every organization (NIST 800-94).

b) Selected IDPS Characteristics:

Common Characteristics	Source
▪ Detects attacks and other security violations that are not prevented by other security measures by monitoring and analyzing events to identify undesirable activity.	SP 800-94
▪ Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.	SP 800-94
▪ Notifying security administrators of important observed events. This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.	SP 800-94
▪ Producing reports. Reports summarize the monitored events or provide details on particular events of interest.	SP 800-94
▪ Detects a wide range of network attacks, including pings/port scans, login attempts, viruses, backdoor, buffer overflows and other types of exploits.	SANS Institute - Combining IDPS & Vulnerability Management
▪ Provides reports and logs suspected events for review and analysis after the fact.	SANS Institute - Combining IDPS & Vulnerability Management
▪ Intrusion Prevention Systems must build on Intrusion Detection System functionality by adding the ability to "block" the attack.	SANS Institute - Combining IDPS & Vulnerability Management

Common Characteristics	Source
▪ Provides central management and distribution of rules / actions.	SANS Institute - Combining IDPS & Vulnerability Management
▪ Records information related to observed events.	SP 800-94 (paragraph 2.2)
▪ Real-time alerts should also be set up to notify administrators when important events occur on the firewall.	SP 800-41 Rev 1 (paragraph 5.2.3)

Security Function: Authentication

a) NIST Guidance:

The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof (NIST 800-53 Rev 3).

Some Information Systems verify the identity of each user attempting to run the information system. Although this is usually done to prevent unauthorized access to the information system, it may also be done when access is not a concern so that the information system can be customized based on the user's identity. Common authentication methods include the following:

- **External Authentication:** The information system may use an external authentication service, such as a directory server. Although the information system may contain some records related to authentication, the external authentication service is likely to contain more detailed authentication information.
- **Proprietary Authentication:** The information system may have its own authentication mechanism, such as user accounts and passwords that are part of the information system, not the operating system (OS).
- **Pass-Through Authentication:** Pass-through authentication refers to passing OS credentials (typically, username and password) unencrypted from the OS to the information system.
- **Host/User Environment:** Within a controlled environment (e.g., managed workstations and servers within an organization), some information systems may be able to rely on previous authentication performed by the OS (NIST 800-86 Section 7.1.2).

b) Selected Authentication Characteristics:

Common Characteristics	Source
▪ Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.	NIST SP 800-53-Rev 3
▪ The information system employs multifactor authentication for local and remote system access that is NIST Special Publication 800-63 compliant.	NIST SP 800-53 Rev 3 (User Identification & Authentication)
▪ The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	NIST SP 800-53-Rev 3
▪ The organization controls all remote accesses through a limited number of managed access control points.	NIST SP 800-53 Rev 3 Excerpt (Remote Access)
▪ The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	NIST SP 800-53 Rev 3 Excerpt (Remote Access)
▪ The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable federal laws, directives, policies (e.g. OMB M-11-11), regulations, standards, and guidance.	NIST SP 800-53 Rev 3 Excerpt (User Identification & Authentication)
▪ The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks.	NIST SP 800-53-Rev 3

▪ The organization manages information system authenticators for users and devices by:
  a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.
  b. Establishing initial authenticator content for authenticators defined by the organization.
  c. Ensuring that authenticators have sufficient strength of mechanism for their intended use.
  d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
  e. Changing default content of authenticators upon information system installation.
  f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate).
  g. Changing/refreshing authenticators (Assignment: organization-defined time period by authenticator type).
  h. Protecting authenticator content from unauthorized disclosure and modification
  i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
	NIST SP 800-53-Rev 3

▪ The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	NIST SP 800-53-Rev 3
▪ Restrict Access to Authentication Data. Authentication data should be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators or hackers from obtaining the data.	NIST SP 800-14 Section 3.11.2

Security Function: Remote Access

a) NIST Guidance:

The security controls (i.e., safeguards or countermeasures) for Remote Access Connections are included in NIST Special Publications 800-46 and 800-114. Security capabilities are needed to filter (inspect), monitor, and authenticate network traffic between D/As. The authentication of network traffic (as well as confidentiality) is often supported via an established VPN and can be coupled with strong user authentication.

b) Selected Management Characteristics:

Common Characteristics	Source
▪ Remote configuration check that connecting systems meet D/A minimum security standards, including at a minimum: a) Active, up-to-date anti-virus application and signatures. b) Active host-based firewall, preventing split-tunneling. c) Critical patches installed.	TIC 2.0 WG, FY2010
▪ Only two-factor authenticated, encrypted inbound connections through the external TIC Remote Access Only Zone boundary.	TIC 2.0 WG, FY2010
▪ No outbound connections through the external TIC Remote Access Only Zone boundary.	TIC 2.0 WG, FY2010
▪ Virtual Desktop, Remote Shell or other system to maintain logical separation of the remote system and D/A applications and system. a) The virtual desktop or system must meet and be maintained to at least the same security standards as required for an equivalent physical system. b) The system supporting the virtual desktop or remote shell must be hardened and maintained as a network security boundary device.	TIC 2.0 WG, FY2010
▪ Filter (inspect) and monitor traffic between the TIC Remote Access Only Zone and the internal D/A network boundary.	TIC 2.0 WG, FY2010
▪ Internal D/A network boundary only permits access to authorized D/A applications and data servers.	TIC 2.0 WG, FY2010

Security Function: Management

a) NIST Guidance:

The security controls (i.e., safeguards or countermeasures) for an information system that focuses on the management of risk and the management of information system security (NIST 800-18 Rev 1).

Management Control: A security control that focuses on the management of a system or the management of risk for a system (NIST 800-123).

The Management Controls section addresses security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization (NIST 800-12 Section 1.3).

There are three sub-functions related to the Management security function:

- **TIC Configuration:** Logical and physical configuration settings that are deployed to secure the TIC access point itself, including TIC Component Locations (NOC, SOC).
- **Physical Controls:** Physical controls specify facility, physical security and maintenance standards that are necessary to ensure the physical security and operational resiliency of the TIC.
- **Authentication of TIC Systems:** TIC systems and components are secured with strong authentication controls.

b) Selected Management Characteristics:

Common Characteristics	Source
▪ For new information systems, management control can be interpreted as having budgetary/programmatic authority and responsibility for the development and deployment of the information systems.	SP 800-18 Rev 1
▪ For information systems currently in the federal inventory, management control can be interpreted as having budgetary/operational authority for the day-to-day operations and maintenance of the information systems.	SP 800-18 Rev 1
▪ The term management controls is used in a broad sense and encompasses areas that do not fit neatly into operational or technical controls.	SP 800-12

Security Function: Logging

a) NIST Guidance:

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. Log management infrastructures typically perform several functions that support the analysis and security of log data. After establishing an initial log management policy and identifying roles and responsibilities, an organization should next develop one or more log management infrastructures that effectively support the policy and roles. Organizations should consider implementing log management infrastructures that include centralized log servers and log data storage. When designing infrastructures, organizations should plan for both the current and future needs of the infrastructures and the individual log sources throughout the organization. Major factors to consider in the design include the volume of log data to be processed, network traffic, online and offline data storage, the security requirements for the data, and the time and resources needed for staff to analyze the logs (NIST 800-92).

Although some information systems (primarily very simple ones) do not record any information to logs, most information systems perform some type of logging. An information system may

record log entries to an OS-specific log (e.g., syslog on UNIX systems, event logs on Windows systems), a text file, a database, or a proprietary file format. Some information systems record different types of events to different logs. Common types of log entries are as follows:

- Event
- Audit
- Error
- Installation
- Debugging (NIST 800-86 Section 7.1.3)

Operating system, service and application logs: Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs. Logs can provide a wealth of information, such as which accounts were accessed and what actions were performed. Additionally, logs can assist in event aggregation to determine the number of hosts scanned in one occurrence. Unfortunately, in many incidents, the logs contain no evidence because logging was either disabled or configured improperly on the host. To facilitate effective incident handling, organizations should require a baseline level of logging on all systems, and a higher baseline level of logging on critical systems. All systems should have auditing turned "on" and should log audit events, particularly administrative-level activity traffic. All systems should be checked periodically to verify that logging is functioning properly and adheres to the logging standards (NIST 800-61 Revision 1, Section 3.2.3).

Network device logs: Logs from network devices such as firewalls and routers are not typically used as a primary source of precursors or indications. Although these devices are usually configured to log-blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying trends (e.g., a significantly increased number of attempts to access a particular port) and in correlating events detected by other devices (NIST 800-61 Revision 1, Section 3.2.3).

IDPS: An IDPS typically performs extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDPS and other logging sources. Data fields commonly used by IDPS include event date and time, event type, importance rating (e.g., priority, severity, impact, confidence), and prevention action performed (if any). Specific types of IDP systems log additional data fields, such as network-based IDPS' performing packet captures and host-based IDPS' recording user IDs. IDPS technologies typically permit administrators to store logs locally and send copies of logs to centralized logging servers (e.g., syslog, security information and event management software). Generally, logs should be stored both locally and centrally to support the integrity and availability of the data (e.g., a compromise of the IDPS could allow attackers to alter or destroy its logs). Also, IDPS' should have their clocks synchronized using the Network Time Protocol (NTP) or through frequent manual adjustments so their log entries have accurate timestamps (NIST 800-94 Section 3.2.2).

b) Selected Logging Characteristics:

Common Characteristics	Source
▪ Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.	SP 800-100 (paragraph 13.2)
▪ Requirements and recommendations for logging should be created in conjunction with a detailed analysis of the technology and resources needed to implement and maintain them, their security implications and value, and the regulations and laws to which the organization is subject (e.g., FISMA, HIPAA, SOX).	SP 800-92

▪ Organizations should:
  a) Establish policies and procedures for log management.
  b) Prioritize log management appropriately throughout the organization.
  c) Create and maintain a secure log management infrastructure.
  d) Provide proper support for all staff with log management responsibilities.
  e) Establish standard log management processes for system-level administrators.
	SP 800-92

▪ System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.	SP 800-12 (paragraph 18.2.2.1)
▪ It is also often desirable to employ higher levels of system logging or network monitoring as part of the recovery process.	SP 800-100 (paragraph 13.3)
▪ Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.	SP 800-61 Rev 1 (paragraph 3.6)
▪ Use centralized logging and create a log retention policy.	SP 800-61 Rev 1 (paragraph 3.6)

Security Function: Data Storage

a) NIST Guidance:

Organizations should also provide sufficient data storage to keep logs associated with computer security incidents for a substantially longer time than other logs, as needed. For example, General Records Schedule (GRS) 24, Information Technology Operations and Management Records, specifies that "computer security incident handling, reporting and follow-up records"

should be destroyed "3 years after all necessary follow-up actions have been completed" (NIST 800-86, 6.3.2).

Typically, system, network, and security administrators are responsible for managing logging on their systems, performing regular analysis of their log data, documenting and reporting the results of their log management activities, and ensuring that log data is provided to the log management infrastructure in accordance with the organization's policies. Administrators typically are responsible for managing the storage of their logs. They should be aware of the organization's requirements and guidelines for log data storage, so that logs are retained for the required period of time. If log data has already been transferred to the log management infrastructure, system-level administrators might not need to do any long-term storage of log data. If administrators need to store the log data for a retention period, and this period is relatively short (days or weeks), it might be adequate to keep them online and capture them in regular system backups. If the retention period is relatively long (months or years), administrators typically need to do the following:

1. Choose a log format for the data to be archived.
2. Archive the log data.
3. Verify the integrity of the transferred logs.
4. Store the media securely (NIST 800-92 Section 5.4).

Administrators are also responsible for ensuring the archived logs are destroyed properly when the required data retention period has ended. This includes logs stored on systems, regular backups, and archival media. Administrators should follow their organization's media sanitization policies and procedures when destroying the logs. Examples of how logs might be destroyed include logical destruction (e.g., repeatedly overwriting data with random values) and physical destruction (e.g., shredding media, degaussing hard drives) (NIST 800-92 Section 5.4).

b) Selected Data Storage Characteristics:

Common Characteristics	Source
▪ Ensuring that sufficient log capacity is available is a concern because logs often take considerably more space than administrators initially estimate, especially when logging is set to a highly detailed level.	SP 800-123 (paragraph 6.1.1)
▪ Organizations should estimate typical and peak log usage, determine how many hours or days worth of data should be retained, and ensure that systems and applications have sufficient storage available to meet those goals.	SP 800-86 (paragraph 6.3.2)

When selecting an offsite storage facility and vendor, the following criteria should be considered: • **Geographic area:** distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site. • **Accessibility:** length of time necessary to retrieve the data from storage and the storage facility's operating hours. • **Security:** security capabilities of the shipping method, storage facility and personnel; all must meet the data's security requirements. • **Environment:** structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls). • **Cost:** cost of shipping, operational fees, and disaster response/recovery services.	SP 800-34 Rev. 1 (Draft)

Security Function: Monitoring

a) NIST Guidance:

To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring (NIST 800-14 Section 3.4.5, NIST 800-12).

Monitoring Types: There are many types and methods of monitoring a system or user.

1. Review of System Logs
2. Automated Tools
3. Configuration Management/Managing Change
4. Trade Literature/Publications/Electronic News
5. Periodic Reaccreditation (NIST 800-14 Section 3.4.5).

Security monitoring is an ongoing activity that looks for vulnerabilities and security problems. Many of the methods are similar to those used for audits, but are done more regularly or, for some automated tools, in real time (NIST 800-12, Section 9.4.2).

b) Selected Monitoring Characteristics:

Common Characteristics	Source
▪ The organization monitors the security controls in the information system on an ongoing basis.	SP 800-53 Rev 3

	Source
▪ These monitoring activities include configuration management and control, security impact analyses of changes to the information system, ongoing assessment of security controls, and status reporting.	SP 800-110 (paragraph 3.3.8)
▪ System performance monitoring analyzes system performance logs in real time to look for availability problems, including active attacks (1988 Morris Worm, causing system and network slowdowns as well as crashing some systems).	SP 800-12 (paragraph 9.4.2.2)

Security Function: Audit

a) NIST Guidance:

The organization reviews and analyzes information system audit records for indications of inappropriate or unusual traffic and reports findings to designated organizational officials (NIST 800-53 Revision 3).

System Audit: System audit records are generally used to monitor and fine-tune system performance. Application audit trails may be used to discern flaws in applications or violations of security policy committed within an information system. User audit records are generally used to hold individuals accountable for their actions (NIST 800-12, Section 18.2.2).

Interconnections: Install or configure mechanisms to record activities occurring across the interconnection, including information system processes and user activities. Activities that should be recorded include event type, date and time of event, user identification, workstation identification, the success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs should have read-only access and only authorized personnel should have access to the logs. In addition, logs should be stored in a secure location to protect against theft and damage, and they should be retained for a period approved by both parties (NIST 800-47, Section 4.2.1).

b) Selected Audit Characteristics:

Common Characteristics	Source
▪ The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity traffic, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	SP 800-53 Rev 3

▪ If a system-level audit capability exists, the audit trail should capture, at a minimum:
    a) Any attempt to log on (successful or unsuccessful).
    b) The log-on ID.
    c) Date and time of each log-on attempt.
    d) Date and time of each log-off.
    e) The devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke).
	SP 800-12 (paragraph 18.2.2.1)

Security Function: Reporting

Refer to NIST 800-61 for guidance on all facets of reporting in terms of incident handling.

a) NIST Guidance:

The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified timeframes designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials. References: NIST Special Publication 800-61, and NIST 800-53 Revision 3.

In support of FISMA, Federal agencies are required to report all computer security incidents to US-CERT based on the incident categories and reporting timeframes detailed in the US-CERT Federal Concept of Operations (CONOPS). These incident categories and descriptions were developed and agreed upon by an interagency body during the development of the US-CERT Federal CONOPS. The Office of Management and Budget (OMB) released a memorandum in May 2007 directing all Federal agencies to adhere to the incident categories and their specified timeframes when reporting incidents to US-CERT (NIST 800-61 Revision 1).

b) Selected Reporting Characteristics:

Common Characteristics	Source
▪ The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	SP 800-53 Rev 3
▪ Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.	SP 800-53 Rev 3
▪ The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.	SP 800-61

Security Function: Secure Communications

a) NIST Guidance:

A secure terminal must be provided adequate physical security to protect it and its physical environment from unauthorized use, acquisition, access, modification, or installation of monitoring devices. A physical and logical access control system must be supported. Terminal and user identification systems are required and must be administratively supported for authorized users. Terminals capable of operating in unattended data communication modes must have adequate internal access control mechanisms to prevent unauthorized outgoing or incoming transmissions. Adequate cryptographic key control is required. Since the entire security of the terminal is based on protecting the cryptographic key from unauthorized disclosure, replacement, or use, such protection must be continuously provided. Keys should be destroyed when no longer useful. (NIST Computer Systems Laboratory Bulletin, March 1992).

b) Selected Security Communications Characteristics:

Common Characteristics	Source
▪ Secure Communication Protocol - A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection.	NIST 800-57 paragraph 2.1

▪ Civil government voice systems, which carry traffic of significant Intelligence value, be secured.	NSTISSP 101 section I - Policy

Security Function: Response

Refer to NIST 800-61 for guidance on all facets of response in terms of incident handling.

a) NIST Guidance:

An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms. An incident-handling capability can provide the ability to react quickly and efficiently to disruptions in normal processing. Effective incident handling can be achieved by developing and instituting effective processes and procedures for the six phases of incident response: preparation, identification, containment, eradication, recovery, and follow-up. The incident handling process should be consistent and compatible with any forensic services the organization may require to ensure critical evidence is handled properly (NIST 800-35, Section 5.2.2).

Each agency must designate a primary and secondary POC with US-CERT, report all incidents, and internally document corrective actions and their impacts to the organization (NIST 800-61, Section 2.3.4.3).

Information regarding reporting requirements, categories, and timeframes for reporting incidents to US-CERT can be found in Appendix J of NIST 800-61 (NIST 800-61, Section 2.3.4.3).

All Federal agencies must ensure their incident response procedures adhere to US-CERT's reporting requirements and that the procedures are followed properly. This is not only mandatory for Federal agencies, but also beneficial for them because US-CERT can provide better information to agencies if they receive better incident data. All organizations are encouraged to report incidents to US-CERT (NIST 800-61, Section 2.3.4.3).

Incident Prioritization: Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on two factors:

- ▪ Current and Potential Technical Effect of the Incident.
- ▪ Criticality of the Affected Resources.

An organization can best quantify the effect on its own incidents because of its situational awareness. Therefore, organizations that report incidents to US-CERT should assign a severity rating to each incident that reflects its effect on the agency, the Federal government, and the national critical infrastructure (NIST 800-61 Section 3.2.6).

b.) Selected Response Characteristics:

Common Characteristics	Source
▪ Incident-Handling Services: Incident-handling capability should be available 24 hours per day, 7 days a week.	NIST 800-35, Section 5.2.2

▪ Incident-Handling Services:
   a) D.4.2 Incident Handling
   b) D.4.2.1 Establish Incident Response Team
	NIST 800-35, Section D.4.2.1

▪ Sharing Information with Outside Parties: The organization may need to communicate with outside parties regarding an incident.	NIST 800-61, Section 2.3.4
▪ Incident Handling: FISMA requires Federal agencies to report incidents to US-CERT which is a government-wide incident response organization that assists Federal civilian agencies in their incident handling efforts.	NIST 800-61, Section 2.3.4.3
▪ Incident Notification: When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations.	NIST 800-61, Section 3.2.7

Appendices

Appendix A – Definition of External Connection

REFERENCES: *(a) OMB Memo M-08-05, Implementing the Trusted Internet Connections (TIC)*
    (b) OMB Memo M-07-06, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
    (c) HSPD 23, Cybersecurity Policy [classified document]
    (d) NIST Special Publication 800-39, Managing Risk from Information Systems – An Organizational Perspective
    (e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
    (f) FIPS 140-2 Publication, Security Requirements for Cryptographic Modules

1. **PURPOSE:** To ensure that the definition of "external connection" is consistently applied across the federal government as it relates to the reduction and consolidation of external government access points required in Reference (a) and enables other dependent initiatives outlined in Reference (c).

2. **BACKGROUND:** In late August 2008, a cross-agency work group met for the fourth in a series of deep dives to develop a roadmap for the implementation of the TIC (Trusted Internet Connection) Initiative, clarify the TIC technical architecture, and better understand the interconnectivity business requirements of TIC Access Providers (TICAP). During the discussion, participants realized that different interpretations of the definition of an external connection, when cascaded across the several thousand network connections managed by the federal government, could impact the achievement of TIC milestones and ultimately the situational awareness in respect to government data traffic envisioned by the Comprehensive National Cybersecurity Initiative (CNCI). By October 1, 2008, the cross-agency group committed to work collaboratively to produce a TIC Technical Architecture document that would include a draft definition of an "external connection." In March 2009, the cross-agency group will work collaboratively to approve a revised definition of an "external connection".

3. **DEFINITION:** The cross-agency work group leveraged the existing definition of an "external system" provided in the second public draft of Reference (d) released in April 2008. To differentiate an external system[3] from an external connection, the following definition is recommended as it relates to the implementation of the TIC Initiative:

    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] External System: An information system or components of information systems that are outside of the Department or Agency (D/A) accreditation boundaries established by the D/A and for which the D/A typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [NIST SP 800-39]

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.

4. **CONNECTION SCENARIOS**: The intent of the following connection scenarios is to further illustrate the definition in Section 3 above. Per reference (a), all external connections must be routed through a Trusted Internet Connection (TIC), but this does not preclude agencies from routing other connections through a TIC.

4.1. The following types of connections will be considered "external connections":

4.1.1. Connections between a D/A information system, network, or components of information systems and networks and the globally-addressable Internet.

4.1.2. Connections between a D/A information system, network, or components of information systems and networks and a remote information system, network, or components of information systems and networks located on foreign territory or where a foreign entity may have any level of physical or logical access to the D/A's information system, network, or components of information systems or networks.

4.2. The following types of connections will NOT typically be considered "external connections" and would not be required to, but could at the D/A's discretion, route through a TIC:

4.2.1. Dedicated secure point-to-point connections that link information systems, networks, or components of information and systems and networks of a single D/A under a single certification and accreditation authority, provided that the connections do not provide access to the globally-addressable Internet, or

4.2.2. Connections that link information systems, networks, or components of information and systems and networks of a single D/A under a single Certification and Accreditation authority established through virtual private network technology utilizing security controls that at a minimum are compliant with FIPS 140-2 and NIST 800-53 coupled with D/A auditing and

monitoring of the connections, provided that the connections do not also provide access to the globally-addressable Internet, or

4.2.3. Remote Government Furnished Equipment (GFE), or authorized non-GFE configured to provide an equivalent level of security, using connections described in 4.2.2.

4.3. Interconnections among D/As may be considered "internal connections" when all D/As involved in the interconnect are fully behind TICs and the following five criteria are met:

4.3.1. All of the D/As' external connections route through a TIC, and,
4.3.2. All of the D/As' other connections are consistent with sections 4.1 and 4.2 above, and;
4.3.3. All D/As monitor the connection at the point of ingress into their C&A boundary using COTS/GOTS IDPS software, and;
4.3.4. All D/As perform packet screening to ensure that only authorized traffic is permitted to flow between the interconnected D/As, and;
4.3.5. All D/As maintain the capability to isolate or temporarily deactivate the connection in the event that suspicious activity is detected.

Additional guidance for managing risks to information systems, networks, or components of information and systems and networks, including consideration of factors agencies should employ when establishing direct control, are further articulated in Reference (d). If there is reasonable doubt as to whether or not a connection should be deemed an external connection, the traffic should be routed through a TIC.

The figures below depict examples of the some of the connection scenarios described above.

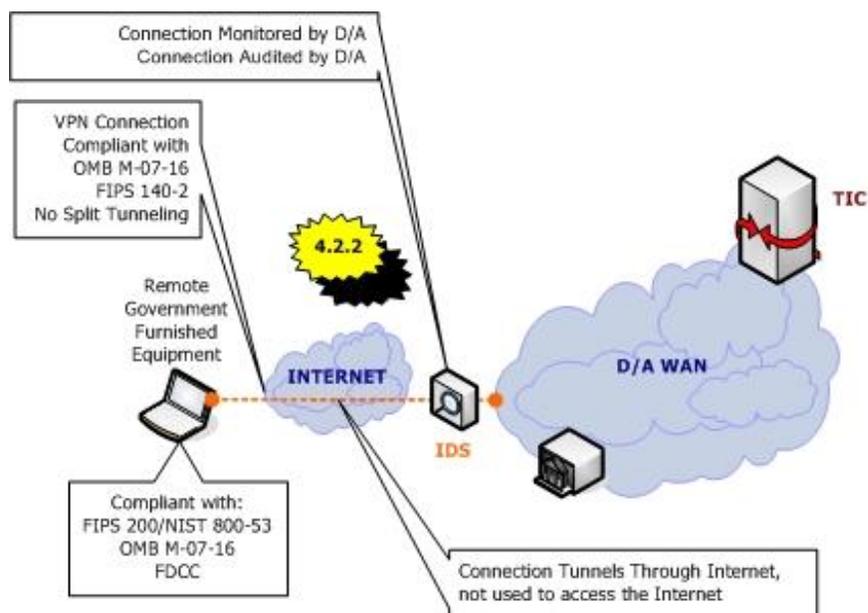Figure 1- Internal Connection Example: Remote Employee VPN

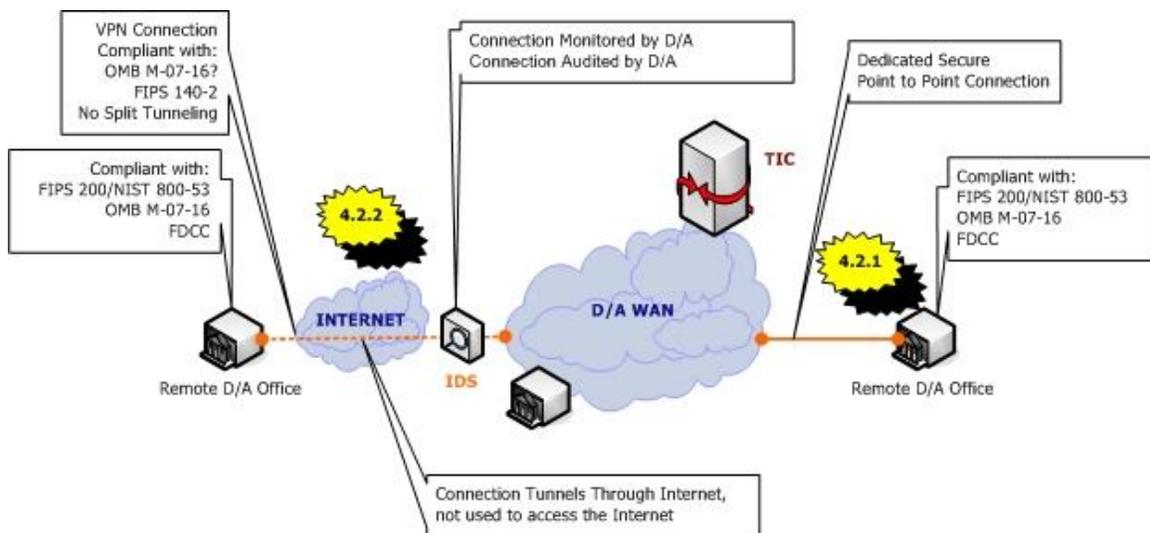Figure 2 - Internal Connection Example: Remote D/A Site

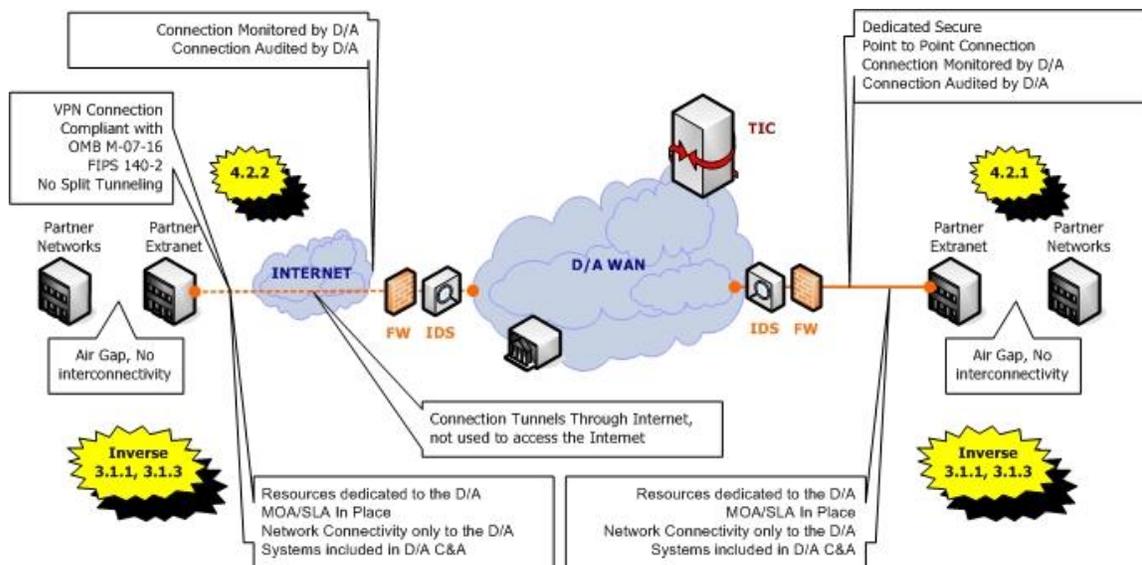Figure 3 - Internal Connection Example: Partner Extranet
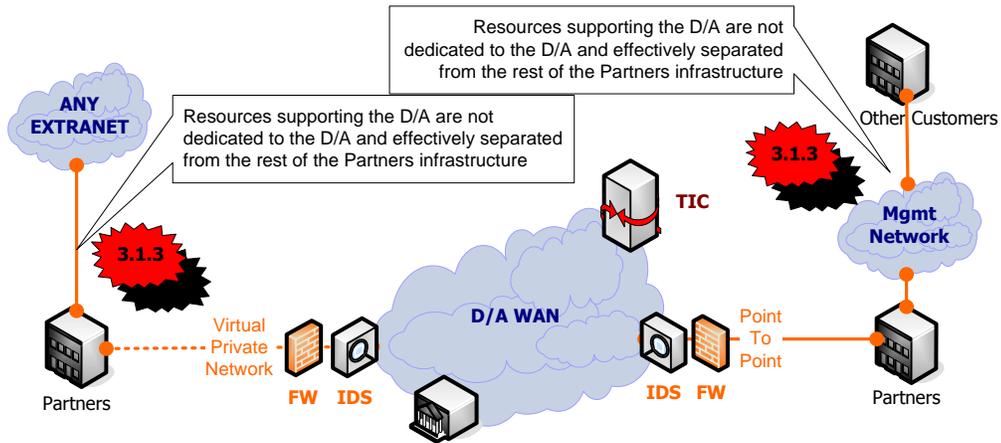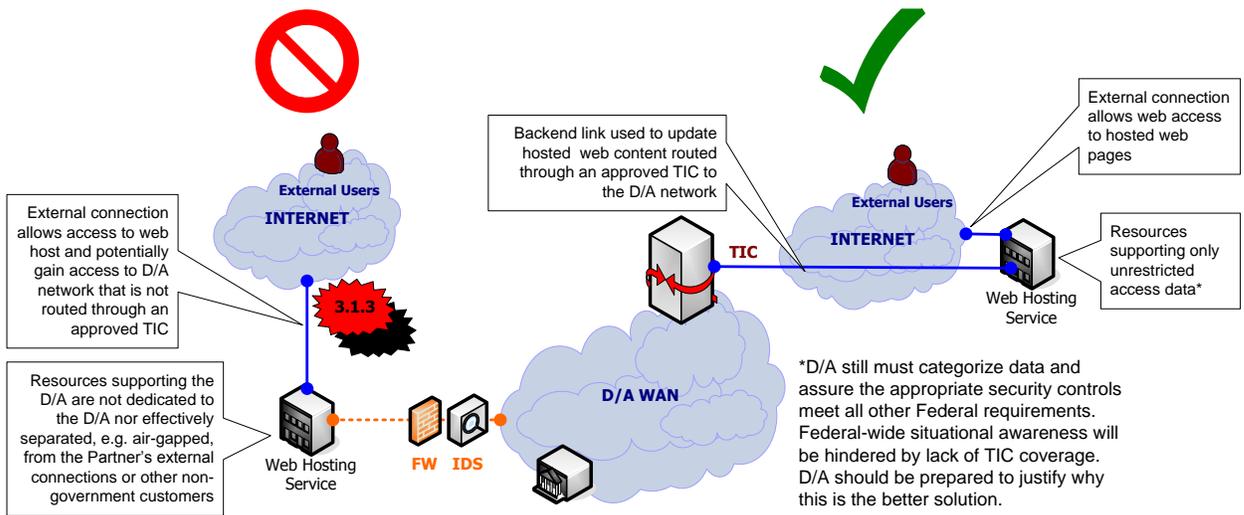
Figure 4 – Example of a Prohibited Scenario

Figure 5 - Comparison of Web-Hosting Scenarios

Appendix B – TIC Capabilities List

This appendix of TIC Capabilities outlines the technical requirements to properly secure, manage and operate a TIC access point.

Each capability is categorized as Critical or Recommended. All Critical Capabilities must be satisfied to be compliant with the TIC Architecture. Recommended Capabilities are best practice guidelines, and while not currently required now for compliance, are strongly suggested as part of agency future planning. Recommended Capabilities are expected to become Critical Capabilities in the next revision of the TIC Reference Architecture in 3 to 5 years.

In the first column below, Capabilities are organized according to Security Family and then Security Function. There are three types of Security Families, designated by the first two letters in the Formal ID: TIC Services (TS), TIC Management (TM), and TIC Operations (TO). The TIC Services Family is a grouping of capabilities performed *by the TIC access point* in order to secure agency networks. The TIC Management Family is a grouping of capabilities performed *on the TIC access point* in order to secure TIC Systems and components. The TIC Operations family is a grouping of capabilities performed *by the TIC Access Provider* in order to ensure TIC access points are properly operated and maintained.

The second two letters in the TIC 2.0 Formal ID relate to the capabilities' Security Function. The *Security Functions, Descriptions, and Characteristics* section of the TIC Reference Architecture provides more information about the associated Security Function of each capability.

PF - Packet Filtering	COM - Secure Communications
CF - Content Filtering	DS - Data Storage
INS - Inspection	LOG - Logging
RA - Remote Access	RES - Response
AU - Authentication	MG - General Management
PC - Physical Controls	MON - Monitoring and Audit
TC - TIC Configuration	REP - Reporting

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TS.PF.01	All external connections are routed through a TIC access point, scanned and filtered by TIC systems and components according to the TICAP's documented policy, which includes critical security policies when published by US-CERT. The definition of "external connection" is in accordance with the TIC Reference Architecture, Appendix A (Definition of External Connection).	Critical
TS.PF.02	By default, the TIC access point blocks network protocols, ports and services. The TIC access point only allows necessary network protocols, ports or services with a documented mission requirement and approval.	Critical
TS.PF.03	The TIC access point implements stateless blocking of all inbound and outbound connections without being limited by connection state tables of TIC systems and components. Attributes inspected by stateless blocks include, but are not limited to: - Direction (inbound, outbound, interface) - Source and destination IPv4/IPv6 addresses and network masks - Network protocols (TCP, UDP, ICMP, etc.) - Source and destination port numbers (TCP, UDP) - Message codes (ICMP)	Critical

TIC Reference Architecture V2.2   41

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TS.PF.04	By default, the TIC access point blocks unsolicited inbound connections. For authorized outbound connections, the TIC access point implements stateful inspection that tracks the state of all outbound connections and blocks packets which deviate from standard protocol state transitions. Protocols supported by stateful inspection devices include, but are not limited to: - ICMP (errors matched to original protocol header) - TCP (using protocol state transitions) - UDP (using timeouts) - Other Internet protocols (using timeouts) - Stateless network filtering attributes	Critical
TS.PF.05	The TIC access point only permits outbound connections from previously defined TICAP clients using Egress Source Address Verification. It is recommended that inbound filtering rules block traffic from packet source addresses assigned to internal networks and special use addresses (IPv4-RFC5735, IPv6-RFC5156).	Critical
TS.PF.06	The TIC access point stateful inspection devices correctly process traffic returning through asymmetric routes to a different TIC stateful inspection device; or documents how return traffic is always routed to the same TIC access point stateful inspection device.	Critical
TS.PF.07	The TIC access point supports Federal Video Relay Service (FedVRS) for the Deaf (www.gsa.gov/fedrelay) network connections, including but not limited to devices implementing stateful packet filters. Please refer to http://www.fedvrs.us/supports/technical for FedVRS technical requirements. Agencies may document alternative ways to achieve reasonable accommodation for users of FedVRS.	Critical
TS.CF.01	The TIC access point uses a combination of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means to implement inbound and outbound application layer filtering. The TICAP will develop and implement a risk-based policy on filtering or proxying new protocols.	Critical
TS.CF.02	The TIC access point filters outbound web sessions from TICAP clients based on, but not limited to: web content, active content, destination URL pattern, and IP address. Web filters have the capability of blocking malware, fake software updates, fake antivirus offers, phishing offers and botnets/keyloggers calling home.	Critical
TS.CF.03	The TIC access point filters inbound web sessions to web servers at the HTTP/HTTPS/SOAP/XML-RPC/Web Service application layers from, but not limited to, cross site scripting (XSS), SQL injection flaws, session tampering, buffer overflows and malicious web crawlers.	Recom-mended
TS.CF.04	The TIC access point performs malware scanning, filters content, and blocks spam-sending servers as specified by NIST 800-45, "Guidelines for Electronic Mail Security," for inbound and outbound mail. These TIC access point protections are in addition to malware scanning and content filtering performed by the agency's mail servers and end-user's host systems. The TICAP takes agency specified actions for potentially malicious or undesirable mail, including at least the following actions: block messages, tag undesirable content, sanitize malicious content, and deliver normally. Multi-Service TICAPs tailor their malware and content filtering services for individual agency mail domains.	Critical
TS.CF.05	The TIC access point uses an agency-specified custom-processing list with at least the combinations of senders, recipients, network IP addresses or host names. The agency specified custom-processing list has custom TICAP malware and content filtering actions. Mail allowed by an agency-specified custom-processing list is still scanned by the TICAP for malware or undesirable content and tagged if found. Multi-Service TICAPs tailor their malware and content filtering services for individual agency mail domains.	Critical
TS.CF.06	For email received from other agency mail domains known to have domain-level sender authentication (for example Domain Keys Identified Mail or Sender Policy Framework) the TIC access point includes the results of the domain-level sender forgery analysis when determining potentially suspicious or undesirable email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Scoring criteria for this capability will be aligned with the National Strategy for Trusted Identities in Cyberspace (NSTIC). The TICAP takes agency specific actions for email determined to be suspicious or undesirable.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TS.CF.07	For email sent to other agency mail domains, the TICAP ensures the messages have been digitally signed at the Domain Level (for example Domain Keys Identified Mail) in order to allow receiving agencies to verify the source and integrity of email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Signing procedures will be in alignment with the National Strategy for Trusted Identities in Cyberspace, and may occur at the bureau or agency sub-component level instead of the TIC access point.	Recommended
TS.CF.08	The TICAP quarantines mail categorized as potentially suspicious while the agency's mail domain reviews and decides what action to take. The agency's mail domain can take at least the following actions: block the message, deliver the message, sanitize malicious content and tag undesirable content. Note: this is intended to be an additional option which agency mail operators can specify with capability TS.CF.04. It does not require agencies to quarantine potentially suspicious mail.	Recommended
TS.CF.09	The TICAP validates routing protocol information using authenticated protocols. The TICAP configures Border Gateway Protocol (BGP) sessions in accordance with, but not limited to, the following recommendation from NIST SP 800-54: BGP sessions are protected with the MD5 signature option. NIST and DHS are collaborating on additional BGP robustness mechanisms, and plan to publish future deployment recommendations and guidance.	Recommended
TS.CF.10	The TIC access point limits and documents the use of unauthenticated, clear text protocols for TIC management and will phase out such protocols or enable cryptographic authentication where technically and operationally feasible.	Critical
TS.CF.11	The TICAP has a documented procedure or plan that explains how it inspects and analyzes encrypted traffic. The document includes a description of defensive measures taken to protect TICAP clients from malicious content or unauthorized data exfiltration when traffic is encrypted. The TIC access point analyzes all encrypted traffic for suspicious patterns that might indicate malicious activity and logs at least the source, destination and size of the encrypted connections for further analysis.	Critical
TS.CF.12	The TICAP has a documented procedure or plan that explains how it inspects and analyzes connections by particular TICAP client end-users or host systems which have custom requirements for malware and content filtering. Connection content is still scanned by the TICAP for malware or undesirable content and logged by the TICAP when found.	Recommended
TS.CF.13	The TIC access point filters DNS queries, and performs validation of DNS Security Extensions (DNSSEC) signed domains, for TICAP clients. The TICAP configures DNS resolving/recursive (also known as caching) name servers in accordance with, but not limited to, the following recommendations from NIST SP 800-81 Revision 1 (Draft): 1. The TICAP deploys separate recursive name servers from authoritative name servers to prevent cache poisoning. 2. The TICAP filters DNS queries for known malicious domains. 3. The TICAP logs at least the query, answer and client identifier.	Critical
TS.INS.01	The TIC access point participates in the National Cyber Protection System (NCPS, operationally known as Einstein).	Critical
TS.INS.02	The TIC access point passes all inbound/outbound network traffic through Network Intrusion Detection Systems (NIDS) configured with custom signatures, including signatures for the application layer. This includes, but is not limited to, critical signatures published by US-CERT.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TS.RA.01	The TIC access point supports telework/remote access for TICAP client authorized staff and users using ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. This capability is not intended to include permanent VPN connections for remote branch offices or similar locations. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities are supported for telework/remote access at the TIC Access Point: 1. The VPN connection terminates behind NCPS and full suite of TIC capabilities which means all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected by NCPS. 2. The VPN connection terminates in front of TICAP-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected. 3. NIST FIPS 140-2 validated cryptography is used to implement encryption on all VPN connections (see NIST SP 800-46 Rev1). 4. Split tunneling is not allowed (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of NCPS. 5. Multi-factor authentication is used (see NIST SP 800-46 Rev1, OMB M-11-11). 6. VPN concentrators and Virtual-Desktop/Application Gateways use hardened appliances maintained as TICAP network security boundary devices. 7. If telework/remote clients use Government Furnished Equipment (GFE), the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways. 8. If telework/remote clients use non-GFE, the VPN connection uses only access through specific Virtual Desktops/Application Gateways. TICAP clients may support additional telework/remote access connections for authorized staff and users using equivalent agency-managed security controls at non-TIC Access Point locations. The agency-level NOC/SOC is responsible for maintaining the inventory of additional telework/remote access connections and coordinating agency-managed security controls. Because of the difficulty verifying the configuration, sanitizing temporary and permanent data storage, and analyzing possible compromises of non-Government Furnished Equipment, it is the agency's responsibility to document in accordance with OMB M-07-16 if sensitive data may be accessed remotely using non-GFE, and informing the TIC Access Provider of the appropriate security configuration policies to implement.	Critical
TS.RA.02	The TIC access point supports dedicated external connections to external partners (e.g., non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities are supported for external dedicated VPN and private line connections at the TIC Access Point: 1. The connection terminates in front of NCPS to allow traffic to/from the external connections to be inspected. 2. The connection terminates in front of the full suite of TIC capabilities to allow traffic to/from external connections to be inspected. 3. VPN connections use NIST FIPS 140-2 validated cryptography over shared public networks, including the Internet. 4. Connections terminated in front of NCPS may use split tunneling.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TS.RA.03	The TIC access point supports dedicated extranet connections to internal partners (e.g., TIC federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other internal networks. The following baseline capabilities are supported for extranet dedicated VPN and private line connections at the TIC Access Point: 1. The connection terminates behind NCPS and full suite of TIC capabilities which means all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected by NCPS. 2. The connection terminates in front of TICAP-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected. 3. VPN connections use NIST FIPS 140-2 validated cryptography over shared public networks, including the Internet. 4. Split tunneling is not allowed. Any VPN connection that allows split tunneling is considered an external connection, and must terminate in front of NCPS. TICAP clients may support dedicated extranet connections with internal partners using equivalent agency-managed security controls at non-TIC Access Point locations. The agency-level NOC/SOC is responsible for maintaining the inventory of extranet connections with internal partners and coordinating agency-managed security controls.	Recom-mended
TM.AU.01	TIC systems and components comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access to TIC access point devices requires multi-factor authentication (OMB M-11-11).	Critical
TM.PC.01	The TIC access points comply with NIST SP 800-53 physical security controls for high impact systems (FIPS 199).	Critical
TM.PC.02	The TIC management locations, such as a Network Operations Center (NOC) and a Security Operations Center (SOC), comply with NIST SP 800-53 physical security controls for medium impact systems (FIPS 199).	Critical
TM.PC.03	The TICAP maintains access to an accredited Sensitive Compartment Information Facility (SCIF) that complies with ICD 705, "Sensitive Compartmented Information Facilities."	Recom-mended
TM.PC.04	The TIC access points and TIC management functions, such as NOC/SOC, are located in spaces dedicated for exclusive use or support of the U.S. Government. The space is secured by physical access controls to ensure that TIC systems and components are accessible only by authorized personnel. Examples of dedicated spaces include, but are not limited to, secured racks, cages, rooms, and buildings.	Critical
TM.PC.05	The TIC access point is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: - Electrical systems meet or exceed the building, operating and maintenance standards as specified by the GSA Public Buildings Service Standards, PBS-100. - TIC systems and components are connected to uninterruptable power in order to maintain mission and business-essential functions including, but not limited to, TIC systems, support systems and powered telecommunications facilities, including at the DEMARC or MPOE. - Uninterruptable power systems, HVAC and lighting are connected to an on-site, automatic, standby/emergency generator capable of operating continuously (without refueling) for at least 24 hours.	Critical
TM.PC.06	The Multi-Service TICAP has geographic separation between its TIC access points, with at least 10 miles separation recommended. It is also recommended that single-agency TICAPs have geographic separation between their TIC access points.	Critical
TM.TC.01	The TIC access point follows the National Communications System (NCS) recommendations for Route Diversity, including at least two physically separate points of entry at the TIC access point and physically separate cabling paths to an external telecommunications provider or Internet provider facility.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TM.TC.02	TIC systems and components in the TIC access point are configured according to the principal of "least functionality," in that they provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services.	Critical
TM.TC.03	All TIC systems and components of the TIC access point support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22 and Federal CIO memorandum "Transition to IPv6." - The TICAP supports both IPv4 and IPv6 addresses and can transit both native IPv4 and native IPv6 traffic (i.e. dual-stack) between external connections and agency internal networks. The TICAP may also support other IPv6 transit methods such as tunneling or translation. - The TICAP ensures that TIC access point systems implement IPv6 capabilities (native, tunneling or translation), without compromising IPv4 capabilities or security. IPv6 security capabilities should achieve at least functional parity with IPv4 security capabilities.	Critical
TM.TC.04	The TIC access point supports hosted DNS services, including DNSSEC, for TICAP client domains. The TICAP configures DNS services in accordance with, but not limited to, the following recommendations from NIST SP 800-81 Rev 1: 1. The TICAP deploys separate authoritative name servers from caching (also known as resolving/recursive) name servers or an alternative architecture preventing cache poisoning. 2. The TICAP implements DNSSEC by meeting NIST SP 800-81 Rev 1 for key generation, key storage, key publishing, zone signing and signature verification.	Recom-mended
TM.TC.05	The TICAP maintains normal delegations and devolution of authority to ensure essential incident response performance to a no-notice event. This includes, but is not limited to, terminating, limiting or modifying access to external connections, including to the Internet, based on documented criteria, including when advised by US-CERT.	Critical
TM.TC.06	The TIC management location, such as a Network Operations Center (NOC) and/or Security Operations Center (SOC), is staffed 24x7. On-scene personnel are qualified and authorized to initiate appropriate technical responses, including when external access is disrupted.	Critical
TM.TC.07	TICAP Operations personnel have 24x7 physical or remote access to TIC management systems which control the TIC access point devices. Using this access, TICAP operations personnel can terminate, troubleshoot or repair external connections, including to the Internet, as required.	Critical
TM.COM.01	The TICAP has a minimum of three qualified people with TOP SECRET/SCI clearance available within 2 hours, 24x7x365, with authority to report, acknowledge and initiate action based on TOP SECRET/SCI-level information, including tear line information, with US-CERT. Authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access to an ICD 705-accredited Sensitive Compartment Information Facility (SCIF) including the following TOP SECRET/SCI communications channels: • Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI, and • Secure FAX machine. Typically personnel with appropriate clearances to handled classified information will include at least the Senior NOC/SOC manager, Chief Information Security Officer (CISO), and Chief Information Officer (CIO), and other personnel as determined by the agency. The SCIF may be shared with another agency and should be within 30 minutes of the TIC management location, during normal conditions, in order for authorized personnel to exchange classified information, evaluate the recommendations, initiate the response and report operational status with US-CERT within two hours of the notification.	Recom-mended
TM.COM.02	The Multi-Service TICAP secures and authenticates the administrative communications (i.e., customer service) between the TICAP operator and each TICAP client.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TM.COM.03	The TICAP has a minimum of one qualified person with SECRET or higher clearance immediately available on each shift, 24x7x365, with authority to report, acknowledge and initiate action based on SECRET-level information; including tear-line information, with US-CERT. Authorized personnel with SECRET clearances or higher have 24x7x365 immediate access at the TIC management location (NOC/SOC) to the following SECRET communications channels: • Secure telephone (STE/STU) and card authorized for SECRET or higher, • Secure FAX machine, • SECRET-level email account able to exchange messages with the Homeland Secure Data Network (HSDN), and • Access to the US-CERT SECRET website. Additionally, authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access within 2 hours of notification to an ICD 705 accredited Sensitive Compartment Information Facility (SCIF) including the following TOP SECRET/SCI communications channels: • Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI, • Secure FAX machine, • TOP SECRET/SCI-level email account able to exchange messages with the Joint Worldwide Intelligence Communications System (JWICS), and • Access to the US-CERT TOP SECRET website.	Recommended
TM.DS.01	Each TIC access point must be able to perform real-time header and content capture of all inbound and outbound traffic for administrative, legal, audit or other operational purposes. The TICAP has storage capacity to retain at least 24 hours of data generated at full TIC operating capacity. The TICAP is able to selectively filter and store a subset of inbound and outbound traffic.	Critical
TM.DS.02	In the event of a TICAP system failure or compromise, the TICAP has the capability to restore operations to a previous clean state. Backups of configurations and data are maintained off-site in accordance with the TICAP continuity of operations plan.	Critical
TM.DS.03	The Multi-Service TICAP documents in the agreement with the customer agency that the customer agency retains ownership of its data collected by the TICAP.	Critical
TM.DS.04	The Multi-Service TICAP identifies and can retrieve each customer agency's data for the customer agency, without divulging any other agency's data.	Critical
TM.DS.05	The TICAP has a Data Loss Prevention program and follows a documented procedure for Data Loss Prevention.	Recommended
TM.LOG.01	Each TIC access point has a Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC). The primary synchronization method is an out-of-band NIST/USNO national reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock. See the TIC Reference Architecture, Appendix F for additional information.	Critical
TM.LOG.02	All TIC access point event recording clocks are synchronized to within 3 seconds relative to Coordinated Universal Time (UTC). All TICAP log timestamps include the date and time, with at least to-the-second granularity. Log timestamps that do not use Coordinated Universal Time (UTC) include a clearly marked time zone designation. The intent is to facilitate incident analysis between TICAPs and TIC networks and devices.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TM.LOG.03	The TICAP provides online access to at least 7 days of session traceability and audit ability by capturing and storing logs / files from installed TIC equipment including, but not limited to firewalls, routers, servers and other designated devices. The TICAP maintains the logs needed to establish an audit trail of administrator, user and transaction activity and sufficient to reconstruct security-relevant events occurring on, performed by and passing through TIC systems and components. Note: This capability is intended for immediate, online access in order to trace session connections and analyze security-relevant events. In addition, TM.LOG.04 requires retaining logs for an additional period of time either online or offline.	Critical
TM.LOG.04	The TICAP follows a documented procedure for log retention and disposal, including, but not limited to, administrative logs, session connection logs and application transaction logs. Record retention and disposal schedules are in accordance with the National Archives and Records Administration existing General Records Schedules, in particular Schedule 12, "Communications Records" and Schedule 20, "Electronic Records;" or NARA approved agency-specific schedule. Note: This capability is intended for the management and operation of the TICAP itself, and does not require the TICAP infer or implement retention policies based on the content of TICAP client communications. The originator and recipient of communications through a TICAP remain responsible for their own retention and disposal policies.	Critical
TO.RES.01	The TICAP has a documented and operational incident response plan in place that defines actions to be taken during a declared incident. In the event of a declared incident or notification from US-CERT, TICAP operations personnel immediately activate incident response plan(s). TICAP operations personnel report operational status to US-CERT within two hours and continue to report based on US-CERT direction.	Critical
TO.RES.02	TIC operations personnel acknowledge, implement, and document tactical threat and vulnerability mitigation guidance provided by US-CERT.	Recom-mended
TO.RES.03	The TICAP manages filters, excess capacity, bandwidth or other redundancy to limit the effects of information flooding types of denial of service attacks on the organization's internal networks and TICAP services. The TICAP has agreements with external network operators to reduce the susceptibility and respond to information flooding types of denial of service attacks. The Multi-Service TICAP mitigates the impact on non-targeted TICAP clients from a DOS attack on a particular TICAP client. This may included diverting information flooding types of denial of service attacks targeting a particular TICAP client in order to maintain service to other TICAP clients.	Critical
TO.MG.01	The TICAP develops, documents, and maintains a current inventory of all TIC information systems and components, including relevant ownership information.	Critical
TO.MG.02	The TICAP follows a formal configuration management and change management process to maintain a proper baseline.	Critical
TO.MG.03	The TICAP communicates all changes approved through the formal configuration management and change management processes to customers, as defined in SLAs or other authoritative documents.	Critical
TO.MG.04	The TICAP maintains an Information Systems Contingency Plan (ISCP) that provides procedures for the assessment and recovery of TIC systems and components following a disruption. The contingency plan should be structured and implemented in accordance with NIST SP 800-34 Rev 1.	Recom-mended
TO.MG.05	The TICAP has telecommunications service priority (TSP) configured for external connections, including to the Internet, to provide for priority restoration of telecommunication services.	Critical
TO.MG.06	The TICAP employs a formal technical review process to schedule, conduct, document and communicate maintenance and repairs. The TICAP maintains maintenance records for TIC systems and components. The intent of this capability is to minimize downtime and operational impact of scheduled maintenance and outages.	Critical

TIC 2.0 Formal ID	Capability Definition	Category Ranking
TO.MG.07	The TICAP maintains a complete map, or other inventory, of all customer agency networks connected to the TIC access point. The TICAP validates the inventory through the use of network mapping devices. Static translation tables and appropriate points of contact are provided to US-CERT on a quarterly basis, to allow in-depth incident analysis.	Recom- mended
TO.MG.08	The Multi-Service TICAP provides each customer with a detailed Service Level Agreement.	Critical
TO.MG.09	The Multi-Service TICAP provides an exception request process for individual customers.	Critical
TO.MG.10	The Multi-Service TICAP accommodates individual customer agencies' security policies and corresponding security controls, as negotiated with the customer.	Critical
TO.MG.11	The Multi-Service TICAP accommodates tailored communications processes to meet individual customer requirements.	Critical
TO.MON.01	The TICAP maintains situational awareness of the TIC and its supported networks as needed to support customer security requirements. Situational awareness can be achieved by correlating data from multiple sources, multiple vendors, and multiple types of data by using, for example, Security Incident & Event Management (SIEM) tools.	Critical
TO.MON.02	At a minimum, the TICAP annually conducts and documents a security review of the TIC access point and undertakes the necessary actions to mitigate risk to an acceptable level (FISMA, FIPS 199 and FIPS 200). Vulnerability scanning of the TIC architecture is a component of the security review.	Critical
TO.MON.03	The TICAP provides access for government authorized auditing of the TIC access point, including all TIC systems and components. Authorized assessment teams are provided access to previous audit results of TIC systems and components, including but not limited to, C&A and ICD documentation.	Critical
TO.MON.04	The TICAP monitors and logs all network services where possible, including but not limited to, DNS, DHCP, system and network devices, web servers, Active Directory, Firewalls, NTP, and other Information Assurance devices/tools. These logs can be made available to US-CERT on request.	Recom- mended
TO.MON.05	The TIC Access Provider participates in operational exercises that assess the security posture of the TIC. The lessons learned from operational exercises are incorporated into network defenses and operational procedures for both the TICAP and its customers.	Recom- mended
TO.REP.01	The TICAP collects customer service metrics about the TIC access point, and reports them to its customers, DHS, and/or OMB as required. Examples of customer service metrics include, but are not limited to, performance within SLA provisions, issue identification, issue resolution, customer satisfaction, and quality of service.	Critical
TO.REP.02	The TICAP collects operational metrics about the TIC access point, and reports them to its customers, DHS, and/or OMB as requested. Examples of operational metrics include, but are not limited to, performance within SLA provisions, network activity data (including normal and peak usage), and improvement to customer security posture.	Critical
TO.REP.03	The Multi-Service TICAP reports threats, alerts, and computer security-related incidents and suspicious activities that affect a subscribing agency to the subscribing agency.	Critical
TO.REP.04	The TICAP reports incidents to US-CERT in accordance with federal laws, regulations and guidance.	Critical

Appendix C – Glossary: Common Terms and Definitions

Comprehensive National Cybersecurity Initiative: HSPD 23 establishes the Comprehensive National Cybersecurity Initiative which authorizes DHS, together with OMB, to establish minimum operational standards for Federal Executive Branch civilian networks. Initiative #1 of CNCI establishes the Trusted Internet Connections Initiative.

Connection Class: A telecommunications class or pattern for data/information flow into and out of D/A information systems, networks, or components of information systems and networks.

Deep Packet Inspection: A stateful protocol analysis capability that improves upon standard stateful inspection by adding basic intrusion detection technology.

Demilitarized Zone (DMZ): The DMZ or Service Network is a perimeter network segment that enforces the internal network information assurance policy for external information exchange.

External Connection Class: A physical or logical connection between information systems, networks, or components of information systems and networks in which one is inside and the other outside of the specific Certification and Accreditation (C&A) boundaries established by the D/A.

External TIC Zone: Outside the accreditation boundary established by the organization and over which the organization typically has no direct control for the application of required security controls or the assessment of security control effectiveness.

Internal TIC Zone: Inside the accreditation boundary established by the organization and for which the organization typically has direct control for the application of required security controls or the assessment of security control effectiveness.

Inter-Agency Connection Class: Connections that allow for the flow of network traffic between D/As in support of mission objectives and business operations.

Intra-Agency Connection Class: Secure connections that link D/A systems, networks, or components to the D/A enterprise.

Intrusion Detection: The process of monitoring the events occurring in a computer system or network and analyzing them for signs of potential incidents.

Intrusion Detection and Prevention System: Identifies potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Intrusion Prevention: The process of performing intrusion detection and attempting to stop detected potential incidents.

Internet Proxy: A third-party proxy service that allows users to surf the web and e-mail anonymously.

Managed Trusted Internet Protocol Services (MTIPS): Services under the NETWORX contract providing TIC solutions to government customers as a managed security service.

National Cyber Protection System: The National Cybersecurity Protection System is the Nation's focal point for cyber activity analysis and response, that works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.

National Cybersecurity Protection Program: The National Cybersecurity Protection Program is the DHS organization responsible for overseeing NCPS.

NETWORX: The contract established in 2007 offering the government comprehensive, best-value telecommunications.

Packet Filter: A device or set of devices which is configured to block unauthorized access while permitting authorized communications.

Physical Controls: Physical controls specify facility, physical security and maintenance standards that are necessary to ensure the physical security and operational resiliency of the TIC.

Proxy: An agent that acts on behalf of a requester to relay a message between a requester agent and a provider agent.

Security Function: The specific operations that must be performed and functionalities that must be provided in order to secure a connection.

Seeking Service Agency: An agency that has not been approved as a TICAP; it must obtain TIC services through an approved Multi-Service TICAP.

Specialized Access Network: Specialized access networks and systems have special access restrictions, and are not connected to agency internal administrative/business systems and networks. National Security Systems are considered specialized access networks, and outside the scope of the TIC services.

Stateful Inspection: Stateful inspection improves on the functions of (stateless) packet filters by tracking the state of connections and blocking packets that deviate from the expected state.

Stateless Inspection (Stateless Blocking): The action performed by a stateless packet filter. Stateless packet filters do not keep track of the state of each flow of traffic that passes though the firewall. This means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering capabilities are built into most operating systems and devices capable of routing. The most common example of a pure packet filtering device is a network router that employs access control lists.

TIC access point: The physical location where a Federal civilian agency reduces and consolidates its external connections.

TIC Access Provider (TICAP): An agency or vendor approved by OMB to manage and host one or more TIC access points.   Single Service TICAPs serve as a TIC Access Provider only to their own department/agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model. MTIPS is a managed service provider version of a Multi-Service TICAP.

TIC Capabilities: The technical, management and oversight criteria required of a TIC Access Provider in order to secure a TIC access point.

TIC Component Locations: The physical locations where TIC systems and components are housed and managed. This includes the TIC access point itself, and any location used for the overall management of TIC components and capabilities, including but not limited to, a Security Operations Center (SOC), and a Network Operations Center (NOC).

TIC Customer: An agency or sub-agency that routes external connections through a TIC access point. Seeking Service Agencies are considered TIC customers of Multi-Service TICAPs (Agencies and/or MTIPS Vendors).

TIC Initiative: Presidential directive to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the Internet.

TIC Management (TIC Configuration): Logical and physical configuration settings that are deployed to secure the TIC access point itself, including TIC Component Locations (NOC, SOC).

TIC Reference Architecture: Architectural guidance document to assist TICAP agencies with establishing compliant TIC access points. The Reference Architecture includes the definition of an external connection, which outlines which types of connections are required to route through a TIC access point.

TIC System Connection Class: TIC systems are components and services that support the overall security operations and policies of the TIC access point.

TIC Zone: Border between an organization's internal infrastructure (users, systems, data) and external resources. Serves as the termination point for external connections and utilizes a standard set of security controls to monitor, authenticate, and filter data flows that enter/exit the TIC access point.

Unrestricted Access Services: Unrestricted access data has no legal or other restrictions on access or usage and may be open to the general public. Networks and systems hosting unrestricted access services still have administrative controls and usage policies to maintain the networks and systems. Agency internal administrative/business systems and networks are not considered unrestricted access.

Appendix D – Acronyms: Common Abbreviations

CNCI - Comprehensive National Cybersecurity Initiative

CONOPS – Concept of Operations

COTS – Commercial Off The Shelf

D/A – Department/Agency

DMZ – Demilitarized Zone

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

EAP – Extensible Authentication Protocol

FIPS – Federal Information Processing Standards

FISMA – Federal Information Systems Management Act

GFE – Government Furnished Equipment

GOTS – Government Off The Shelf

GRS – General Records Schedule

HIPAA – Health Insurance Portability and Accountability Act

HTTP – Hypertext Transfer Protocol

IDPS - Intrusion Detection and Prevention System

IEEE – Institute of Electrical and Electronics Engineers

LAN – Local Area Network

MAC – Media Access Control

MTIPS - Managed Trusted Internet Protocol Services

MSSP – Managed Security Service Provider

NCPP - National Cybersecurity Protection Program

NCPS - National Cyber Protection System

NIST – National Institute of Standards and Technology

NOC – Network Operations Center

OCONUS – Outside the Continental United States

OMB – Office of Management and Budget

SCIF – Sensitive Compartment Information Facility

SOC – Security Operations Center

SOX – Sarbanes Oxley

STE - Secure Terminal Equipment

STU – Secure Telephone Unit

TCP/IP – Transmission Control Protocol/Internet Protocol

TIC - Trusted Internet Connection

TICAP - TIC Access Provider

TLS – Transport Layer Security

US-CERT – United States Computer Emergency Readiness Team

VPN – Virtual Private Network

WAN – Wide Area Network

Appendix E – Guidance for OCONUS Telework/Remote Access Connections

Special Case: Telework Outside the Continental US (OCONUS) Intra-Agency Access

In limited circumstances, such as locations outside the continental United States (OCONUS) where network access and latency prevent using a complete TIC Zone, a TIC Remote Access Only Zone may be proposed as an option. Utilizing the TIC Remote Access Only Zone requires the application of additional security controls to compensate for the additional risk in the remote system; it provides logical separation within the TIC Remote Access Only Zone between external and internal networks, and filters (inspect) and monitors traffic that flows across the D/A external and internal network security boundaries.

These connections will be managed according to the security pattern defined below:

Pattern Definition: Remote Access Only connections are connections that link non-Government Furnished Equipment (GFE) systems, and GFE when available, used by authenticated, authorized staff to a D/A enterprise network. Because non-GFE systems are used, these resources are not completely trusted to become a logical extension of the protected internal D/A enterprise network via authentication and VPN services.

Because of the difficulty verifying the configuration, sanitizing temporary and permanent data storage, and analyzing possible compromises of non-Government Furnished Equipment, it is the agency's responsibility to document in accordance with OMB M-07-16 if sensitive data may be accessed remotely using non-GFE, and informing the agency NOC/SOC of the appropriate security configuration policies to implement at the TIC Remote Access Zone.

In the proposed pattern definition, the TIC Remote Access Zone would be located as part of the agency's OCONUS network. The remote user could connect to the OCONUS network, e-mail server, etc. via a more conveniently located Virtual Desktop Server.

Additional Security Capabilities:

- Multi-factor authentication with an external token or HSPD-12 PIV card
- FIPS 140-2 encrypted inbound connections
- No split-tunnel of the client connection
- No outbound external connections through the external TIC Remote Access Only Zone boundary
- Remote configuration check that connecting systems meet security policies set by the Department or Agency, including at a minimum:
    - Active, up to date anti-virus application and signatures
    - Active host-based firewall, preventing split-tunneling
    - Critical patches installed
- Virtual Desktop, Application Gateway or other system to maintain logical separation of the remote system and D/A enterprise network and/or information system

- o The virtual desktop or system meets and is maintained to at least the same security standards as required for an equivalent physical system
- o The system supporting the virtual desktop or remote shell must be hardened and maintained as a network security boundary device
- Filter (inspect) and monitor traffic between the TIC Remote Access Only Zone and the internal D/A network boundary
- Internal D/A network boundary only permits access to authorized D/A information systems and data servers

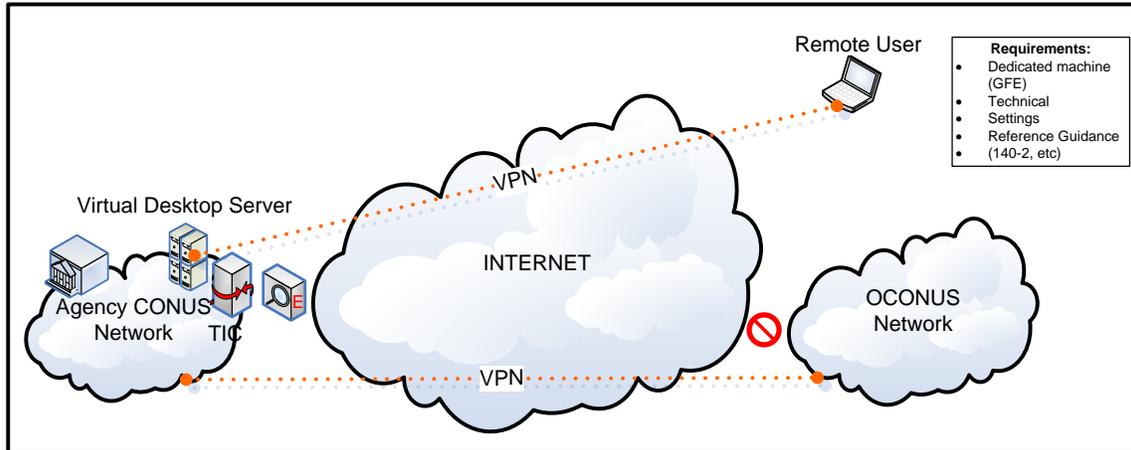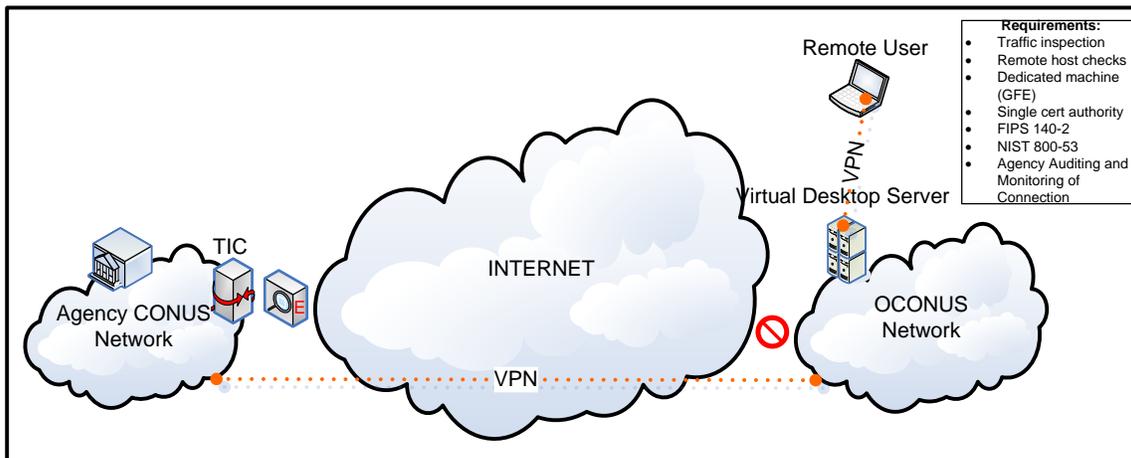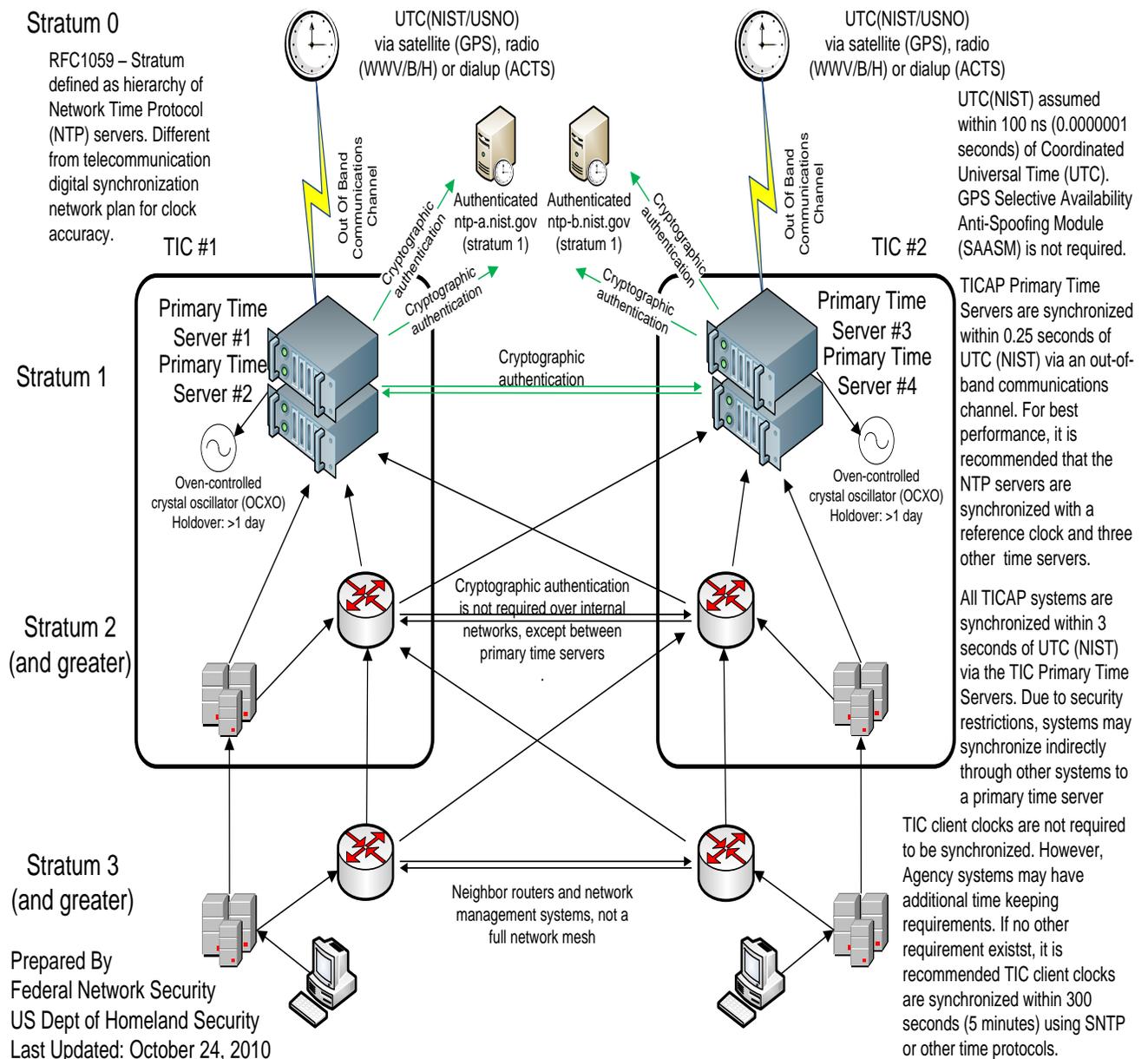**Figure 10: Current TIC OCONUS Solution**

Figure 11: Proposed Remote Access for OCONUS Connections Solution

**Figure 12: Guidance for Implementing Primary Time Servers**

Appendix G – Agency Domain Name System (DNS) Deployment

An agency's DNS is a key component to an agency's network infrastructure. The DNS is a globally distributed database access using a simple query/response protocol. The DNS protocol resolves human readable domain names (e.g., "www.agency.gov") to an IP address and is often the first step in any network communication. Therefore it is vital that the DNS infrastructure is responsive, robust and secure both for agency personnel to reach the Internet and the general public to reach the agency's public facing services.

The DNS separate components into two roles: authoritative servers that maintain a portion of the global DNS database for an enterprise (referred to as its "zone") and clients that send requests to authoritative servers. There is usually a third component, the recursive caching server (usually shortened to "recursive server") that performs work on behalf of clients ("stub" clients without the ability to do a full DNS query) and performs the full query. Recursive servers then store the responses in a cache for the benefit of all the stub clients it services.

When planning the DNS infrastructure for an agency, network architects should take these roles into consideration and separate the systems performing each task. Each role has specific usage and security concerns that should be addressed when setting up the DNS system for the agency. So an agency would need to set up one set of systems for the authoritative service and another to provide recursive service for clients within the agency.

Figure 13: DNS Architecture
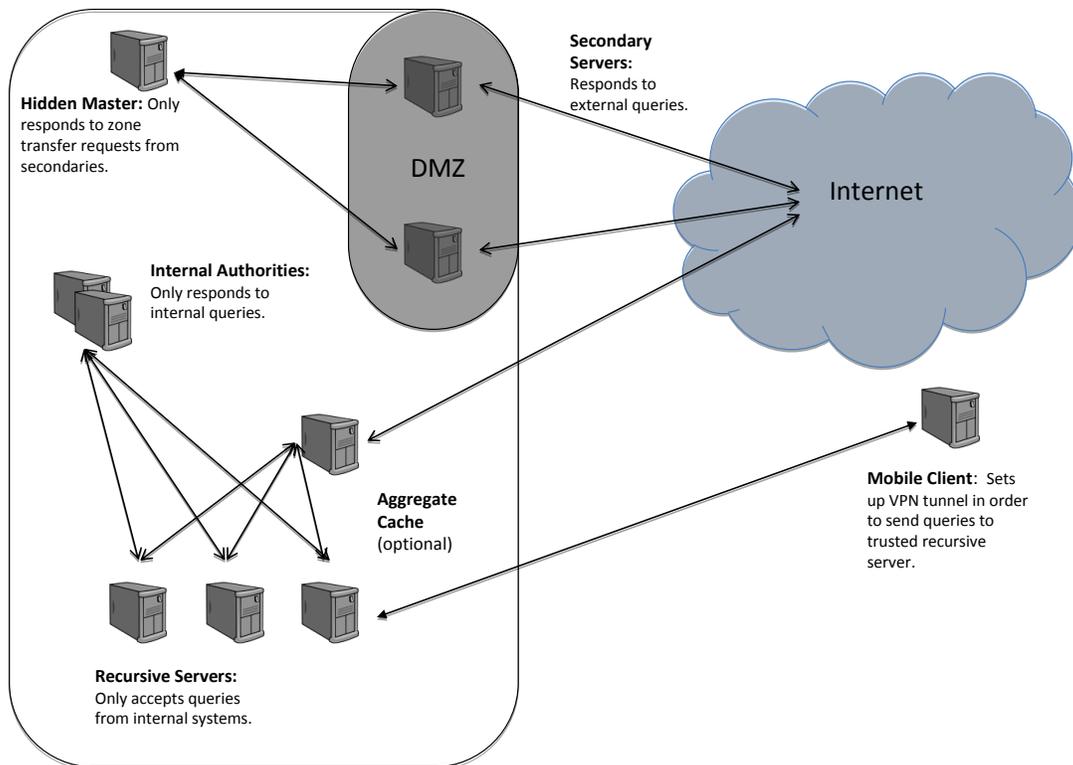
The above guidance is taken from best common practices for DNS and recommendations from NIST Special Publication 800-81r1: Secure Domain Name System (DNS) Deployment Guide.

Authoritative Service
The basic requirement for an agency's authoritative DNS service is high availability in the face of any potential network disruption (intentional or non-intentional). A Denial of Service (DoS) attack or network segment break could take the entire agency off line if all the agency's authoritative servers are located on the same LAN segment. This is accomplished by separating the internal and external authoritative servers (based on the clients they will respond to and the zone information they contain) and dispersing the authoritative servers across different network segments and geographic locations (if possible).

The authoritative servers for the agency should be broken down into two sets: One set to host internal zone data (internal mail servers, application servers, etc.) that resides inside the internal network (i.e., behind the firewall) and only responds to other internal hosts and one set to host externally facing servers that are located on the agency's Demilitarized Zone (DMZ) or Service Network and responds to queries from the external Internet. Both sets of servers should be on separate network segments and geographic locations (if possible). They should also have all other unnecessary network services turned off or uninstalled.

Network administrators should also consider using a hidden master for the external DNS authoritative servers. A hidden master is a DNS server that is the primary server for the zone, but does not appear in the zone data itself and is often located behind a firewall and cannot be queried from the external Internet. Its sole function is to host the zone and perform zone transfers to a collection of secondary zones on the DMZ.

To insure the integrity of zone data, DNS administrators should also deploy the DNS Security Extensions (DNSSEC) with their zone data. DNSSEC provides source authentication and integrity protection for DNS data through the use of digital signatures. To insure the integrity of the process, the generation of these digital signatures should be done as close to the authentic data source as possible, with the signed zone then transferred to the hidden master (for external zones) and internal authoritative zones. More information on how to plan and deploy DNSSEC can be found in NIST SP 800-81r1.

Recursive Service
Recursive servers should be located within the internal network and configured to only accept queries from internal hosts (i.e., other systems on the LAN). There should not be any externally facing recursive servers, as they can be used by attackers to launch DoS attacks against a third party.

For small agencies, one or two recursive servers may be enough. Larger agencies may need several recursive servers and may want to consider having a larger agency-wide aggregate cache to provide faster response time for users and provide a single gateway for any monitoring by IDS (or similar systems). Separate departments within an agency would have their own recursive

server that would forward its queries to the aggregate cache, which would then build an agency-wide cache of responses.

Agencies that do DNSSEC validation of responses have additional configuration options to consider when setting up recursive systems. As of the time of writing, most stub clients (i.e., desktop and laptop systems) do not perform DNSSEC validation, and must rely on a validating recursive server. Therefore, it is important to perform validation as close to the end system as possible to minimize any potential hijack of the response. This risk can be further minimized by the use of IPSec or similar security measures (e.g., DNS transaction signatures; TSIG) for communication between end systems and the validating recursive server.

Administrators also need to configure DNSSEC public keys as trust anchors. There are automated protocols and tools to keep trust anchors up-to-date, but initial configuration requires human action. The administrator would need to identify and obtain the desired trust anchors to install on the validating recursive servers and perform regular key maintenance.

Special Note Regarding Mobile Hosts: Administrators need to provide one or more recursive servers for mobile uses connecting back to the agency's network via a VPN. Mobile users may not be able to trust the recursive server provided by the remote network and the recursive server may not perform DNSSEC validation and if it does validation, the user has no idea what trust anchors are used. Mobile uses should have a means to connect back to the home agency's network and use one of the trusted recursive servers (or a special recursive server for VPN users).

Appendix H – Cloud Considerations

Overview
The information in this appendix is based on direct interviews with Departments and Agencies (D/As) and the TIC v2.1 Working Group sessions. Given the rapid pace of Cloud Service Provider (CSP) offerings—as well as the economic benefits and risks of using CSPs—working group session participants were unsure how these offerings integrated with the TIC 2.0 Reference Architecture. An outcome of these working group sessions was a clarification of the use of D/A network connections when using a CSP within the framework of the TIC.

The goals of this appendix are to

- illustrate the network connections with respect to the D/A, TIC, CSP, and end user
- provide guidance regarding the segmentation and connectivity requirements of D/A data assets and the infrastructure that manages them at the D/A and the CSP

Note that these goals adhere to both the TIC 2.0 Reference Architecture and FedRAMP approaches and methodologies.

The scenarios depicted in this document are meant to outline common solutions. Agencies are encouraged to work with their CSPs and FedRAMP to identify appropriate solutions for their environments that fit within the TIC framework and meet the following criteria:
- If the CSP is considered an external network to the D/A (the D/A's information at the CSP is not included in the D/A's Assessment & Authorization [A&A] boundary), then the traffic between the D/A's boundary and the CSP must transit a TIC.
- If the D/A has both private and publicly accessible data at the CSP, then the D/A must have a D/A-designated boundary (physical or logical) between the public and private data, with the private data protected by a TIC boundary.
- A D/A remote-access user's connection must transit a TIC access point before accessing the CSP.
- If the CSP is considered an extension of the D/A internal network (the D/A's information at the CSP is included in the D/A's A&A boundary), then the traffic between the D/A's boundary and the CSP is not required to transit a TIC.

This appendix does not create new TIC capabilities or policies. Instead, it provides clarification through real-world scenarios being used by D/As; it can also serve as a reference for ensuring that cloud and mobile implementations meet the requirements specified in the TIC v2.0 Reference Architecture. Neither the requirements nor the specific TIC capabilities (listed in Appendix B) have changed.

FedRAMP[4]
The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, continuous

---

[4] http://www.gsa.gov/portal/category/102371 as of 30 July 2013

monitoring, and certification and authorization boundaries for cloud products and services. The FedRAMP approach served as a reference for the use cases in this appendix.
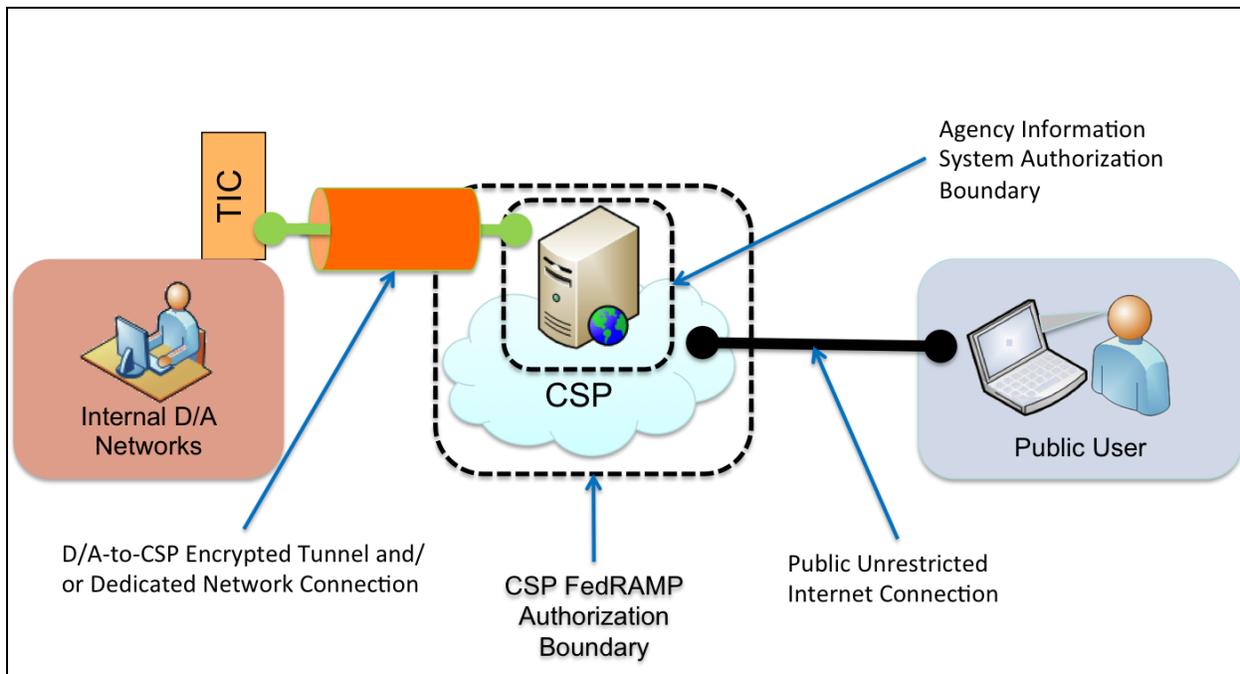
Use Cases

The following use cases were derived from working group session discussions attended by various D/As as well as DHS sponsors and contributors from May through August 2013. The sessions unearthed a wide range of topics with various degrees of interest and importance. The foremost topic by far was the clarification of the use and integration of CSP services with D/A assets and how the TIC 2.0 Reference Architecture applies to these activities. The following use cases attempt to clarify the major issues and concerns raised during the working group session discussions.

Use Case 1: D/A Unrestricted-Access Data

In this use case, a D/A establishes a public-facing website at an authorized CSP that contains unrestricted-access data.

Figure 14: D/A Unrestricted-Access Data
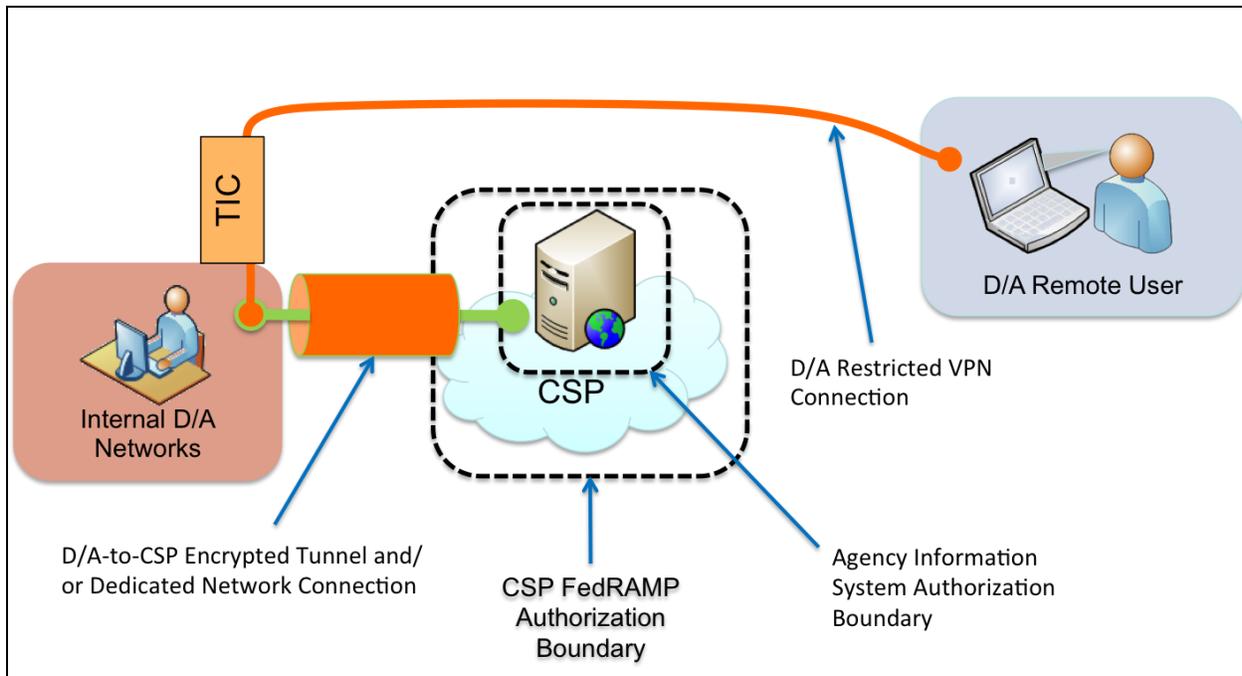

Use Case 1 Assumptions

- A public user is accessing unrestricted-access data.
- The encrypted tunnel and/or dedicated connection between the D/A and the CSP is required to pass through the TIC because the CSP is providing services to the public Internet.

Figure 14 illustrates a public-facing service hosted at a FedRAMP-authorized CSP. The public-facing data service is inside the CSP FedRAMP authorization boundary but outside the agency information system authorization boundary. The TIC is located at the D/A's administrative boundary; note that the data service does not pass through it when accessed from public networks because the data within the service is defined by the D/A as unrestricted-access data. The D/A user connects to the service (depending on the data management or service access policy of the D/A) using a communication method agreed upon by the agency and CSP (e.g., the TIC traverses the public Internet, the user communicates via a dedicated network connection). The public remote user accesses the service via an unrestricted public Internet connection.

Use Case 2: D/A Restricted-Access Data

In this use case, a D/A establishes a controlled-access website hosted by a FedRAMP-authorized CSP for restricted-access data.

Figure 15: D/A Restricted-Access Data

Use Case 2 Assumptions

- A D/A remote user is accessing restricted-access data.
- The connection between the D/A and the CSP is an encrypted tunnel and/or dedicated connection.
- There are no services offered at the CSP to the public Internet.

Figure 15 shows a D/A using a CSP-hosted service that contains restricted-access data. The agency information system authorization boundary contains the system hosting the restricted-access service. The FedRAMP authorization boundary encompasses the entire instance at the CSP that hosts the service being used by the D/A. The agency user in the D/A internal zone connects to the CSP via a secure communication channel such as an encrypted tunnel and/or dedicated connection. Because the service being used in this example is for internal use only, there is no authorized access from an external zone.

Use Case 3: D/A-to-CSP Connectivity Requirements

Another issue for D/As is identifying data path requirements for

- the public Internet to the CSP for D/A unrestricted-access services
- the D/A and the CSP for D/A restricted-access services

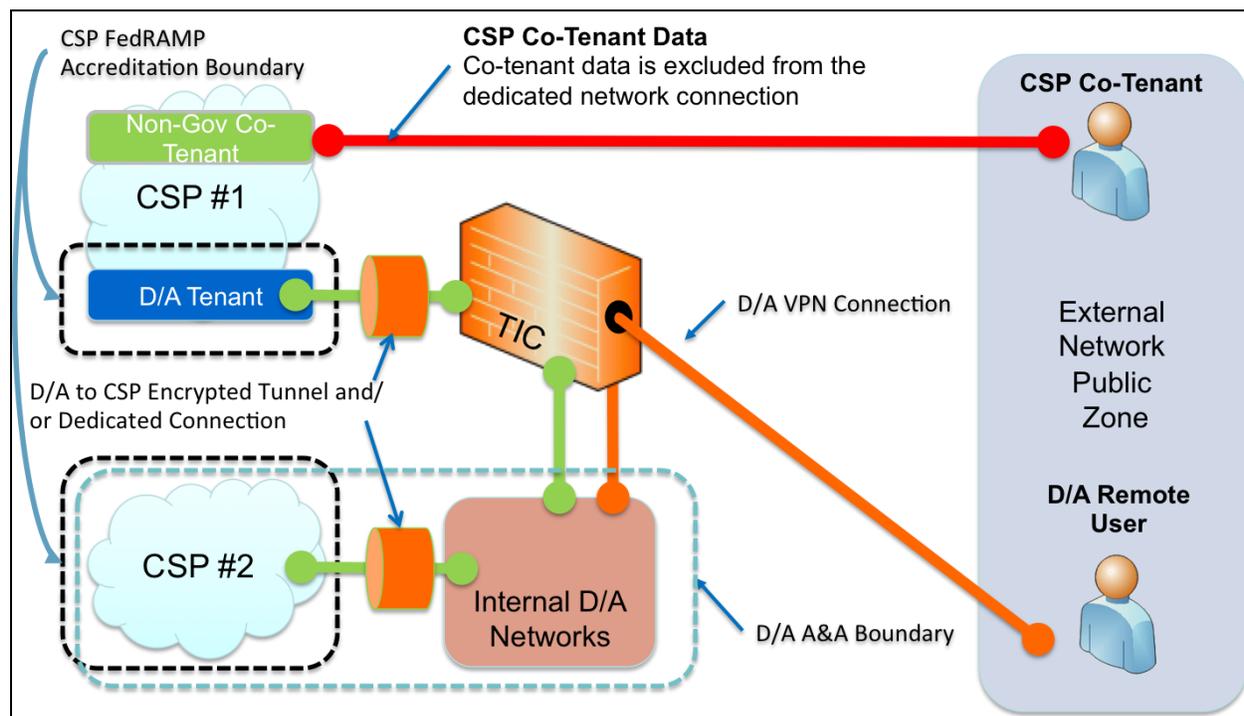**Figure 16: D/A-to-CSP Connectivity Requirements**

Figure 16 illustrates the requirements for traffic to transit the TIC. The TIC 2.0 Reference Architecture states that intra-agency connections are not required to transit a TIC but may do so at the D/A's discretion. Additionally, the TIC access point should support dedicated extranet connections to internal partners. The TIC 2.0 capability TS.RA.03 states

> The TIC access point supports dedicated extranet connections to internal partners (e.g., TIC federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but [is] not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other internal networks.

Therefore, if the CSP is considered an extension of the D/A internal network (the D/A's information at the CSP is included in the D/A's A&A boundary) then the traffic between the D/A's boundary and the CSP is not required to transit a TIC. This scenario is depicted in Figure 16, where the second cloud instance—which is inside the CSP FedRAMP Accreditation boundary—and the D/A network are both included inside the D/A's A&A boundary.

The TIC access point should also support dedicated external connections to external partners. The TIC 2.0 capability TS.RA.02 states

The TIC access point supports dedicated external connections to external partners (e.g., non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but [is] not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks.

Therefore, if the CSP is considered an external network to the D/A (the D/A's information at the CSP is not included in the D/A's A&A), then the traffic between the D/A's boundary and the CSP must transit a TIC. This scenario is illustrated in Figure 16, where the first cloud instance is inside the FedRAMP Accreditation boundary but outside the D/A's A&A boundary.

The flow of data in Figure 16 can be summarized as follows:
- Authorized D/A remote user -> TIC -> encrypted tunnel -> access to CSP #1
- Authorized D/A remote user -> TIC -> Internal D/A network -> encrypted tunnel -> access to CSP #2
- Internal D/A user -> TIC -> encrypted tunnel -> access CSP #1
- Internal D/A user -> encrypted tunnel -> direct access to CSP #2

Use Case 4: Clarification of CSP Data Segmentation Requirements

Another issue for D/As is the provisioning and segmentation of data between the D/A infrastructure and the CSP, specifically in identifying data paths between the D/A and the CSP based on their proximity to non-government CSP co-tenants. As identified in the *Guide to Understanding FedRAMP,* [5] conditions A, B, and C (illustrated in Figure 17) must be satisfied by the CSP and the consumer's architecture.

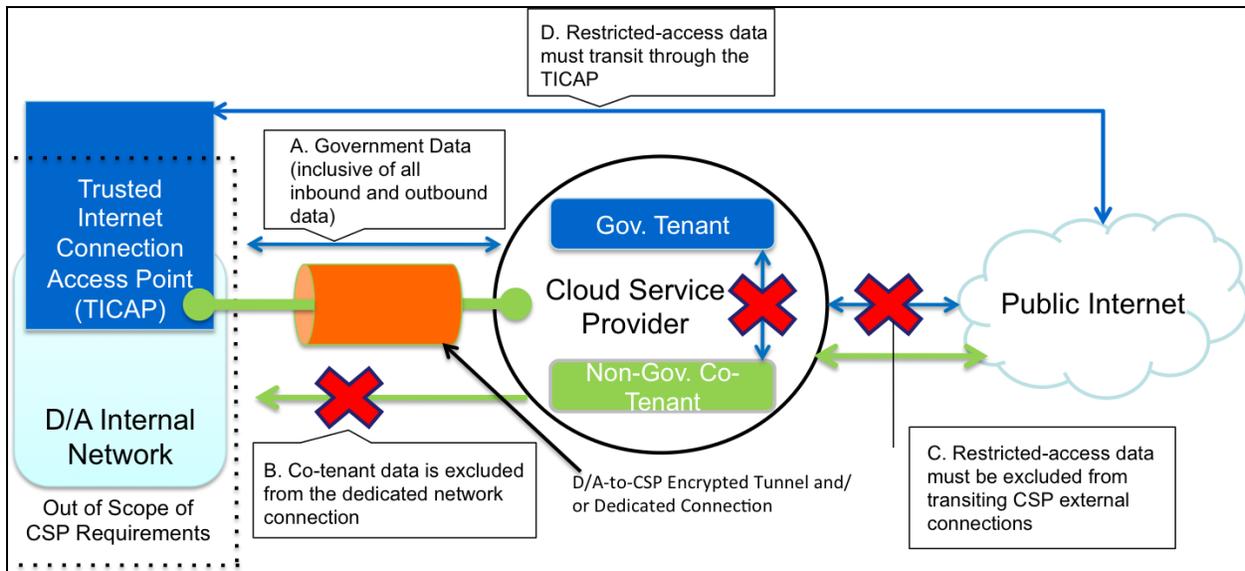**Figure 17: CSP Data Segmentation Requirements**

Figure 17 shows the data segmentation requirements for D/As using cloud services located at a CSP. The CSP depicted in the center of the figure shows government and non-government tenants. There is no logical data service connection between these tenants. The D/A communicates with the D/A-contracted services at the CSP via a secure, dedicated connection, which is inclusive of all inbound and outbound data to and from the service (condition "A" in the figure). Condition B shows that co-tenant data is excluded from traversing this dedicated connection between the D/A and the CSP. Condition C shows that data intended solely for government use can be excluded from being routed through external (non-dedicated) network connections. Condition D shows that all restricted-access data must travel through the TICAP to or from the CSP. As previously noted, the *Guide to Understanding FedRAMP* requires that conditions A, B, and C must be satisfied by the CSP and the consumer's architecture.

---

[5] http://www.gsa.gov/portal/mediaId/170599/fileName/Guide_to_Understanding_FedRAMP_042213 as of 16 September 2013

LEGISLATION

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

National Security Presidential Directive (NSPD) 54, *Cyber Security and Monitoring*, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, *Computer Network Monitoring and Cyber-security*, 8 January, 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, 2 August 2005.

Office of Management and Budget (OMB) Memorandum *M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, 11 January 2007.

Office of Management and Budget (OMB) Memorandum M-08-05, *The Trusted Internet Connection initiative (TIC)*, November 2007.

National Security Telecommunications and Information Systems Security Committee NTTISSP 101, *National Policy on Securing Voice Communications,* 14 September 1999.

Federal Chief Information Officer Memorandum, *Transition to IPv6*, 28 September 2010.

Intelligence Community Directive Number 705, *Sensitive Compartmented Information Facilities*, 26 May 2010. Supersedes DCID 6/9.

STANDARDS

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

General Services Administration (GSA), Public Buildings Service (PBS), *Facilities Standards (P100)*, 2009.

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Module*, 3 December 2002.

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2006.

IEEE 802.1X: IEEE Standard for port-based Network Access Control (PNAC).

GUIDELINES

NIST's Information Technology Laboratory, ITL Security Bulletins, *An Introduction to Secure Telephone Terminals - ITL Security Bulletin*, March 1992.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

National Institute of Standards and Technology Special Publication 800-78-2, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-81, Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, August 2009.

National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

Office of Management and Budget Memoranda, M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, 4 April 2008.

Office of Management and Budget Memoranda, M-08-26, *Transition from FTS 2001 to NETWORX*, 28 August, 2008.

Office of Management and Budget Memoranda, M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, 20 September 2008.

Office of Management and Budget Memoranda, M-09-32 *Update on the Trusted Internet Connections Initiative*, 17 September 2009.

Office of Management and Budget Memoranda, M-11-11 *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, 3 February 2011.*

SANS Institute - Combining IDPS and Vulnerability Management