Managed Trusted Internet Protocol Service (MTIPS)

The EIS Managed Trusted Internet Protocol Service (MTIPS) allows agencies to logically and physically connect to external connections or the public Internet in a way that aligns with the security compliance requirements of the agency and OMB's Trusted Internet Connection (TIC) initiative (M-08-05).

This service enables an agency to fully comply with TIC directives from the Office of Management and Budget (OMB)[1], and the U.S. Department of Homeland Security (DHS)[2]. (See Figure 1 below for an illustration of the service, and its elements.)

MTIPS is composed of the network infrastructure to transport IP traffic between the agency Enterprise WAN and the TIC Portal; together they create an agency TIC Trusted Domain (DMZ) for IP traffic. In today's environment, the agency perimeter boundary is dynamic and morphing to include virtual instances. Hence, MTIPS provides the transport that serves as a "collection" network for TIC physical or virtual Portal connectivity insulating an agency's internal network from the Internet and other external networks.

The TIC Portal provides both physical and virtual security services to multiple government agencies, as well as allowing for specific controls based on an agency's coordination with DHS, GSA and the EIS contractor, when necessary. The contractor provides virtual TIC capabilities upon request for agencies with resources hosted outside their physical boundaries.

[1] Office of Management and Budget. November 20, 2007. "M-08-05: Implementation of Trusted Internet Connections (TIC)."

[2] U.S. Department of Homeland Security. April 21, 2016. "Trusted Internet Connections."

MTIPS is part of a larger, strategic initiative to improve the federal government's security posture and prevent cyberattacks by supporting the following Trusted Internet Connection Strategic goals:

- Reduce and consolidate external access points across the federal enterprise.
- Manage the security requirements for the TIC network and security operations center (NOC/SOC).
- Establish a compliance program to monitor Departments and Agency adherence to Federal Regulations.

According to EIS contract Section C.1.8.8 National Policy Requirements, the five service offerings listed below require using an externally routed DHS National Cyber Protection System (NCPS) (operationally referred to as EINSTEIN) Enclave.

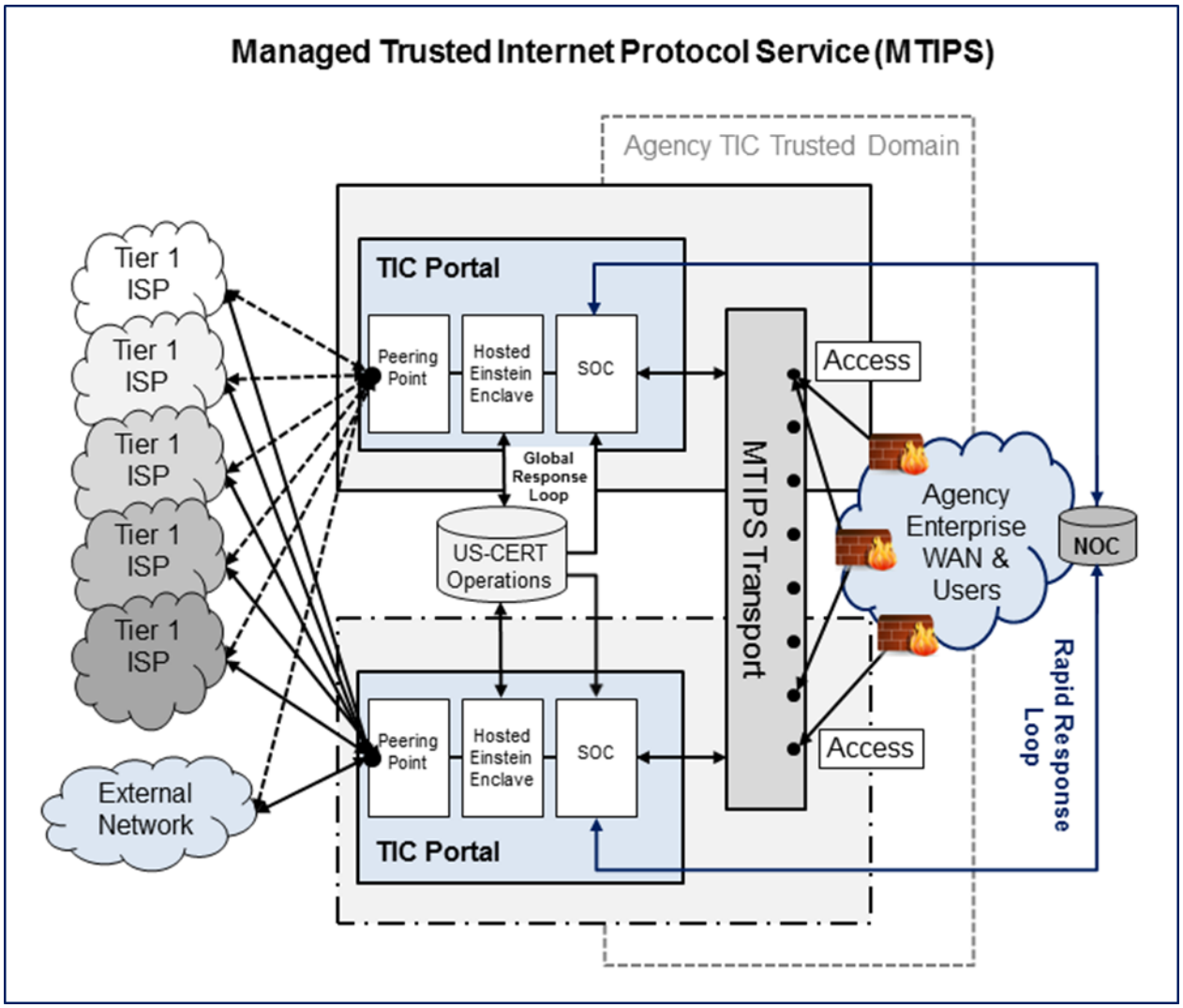
- Virtual Private Network Service
- Ethernet Transport Service
- Private Line Service
- Internet Protocol Service
- Cloud services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)

Category: Managed Services

Complementary Services Needed: In order to use MTIPS, the agency would need EIS Access Arrangements or equivalent.

Definitions: Please see EIS contract Section J.12 Glossary of Terms for clarification of technical terms and acronyms.

Figure 1— The diagram below illustrates how data is collected from the agency WAN by the MTIPS transport network, and then directed to the TIC, which includes the Security Operations Center (SOC) and the Einstein Enclave.



1. Four Important MTIPS Factors Customers Must Understand

There are four key factors that form the technical, security and legal foundations for the deployment of an agency's MTIPS solution. An agency must know and understand these factors, and must complete the required tasks before the contractor deploys the agency's MTIPS solution. Each factor is listed and explained below.

1.1 Capabilities for Cloud Services

MTIPS can support agencies using externally hosted cloud services such as IaaS, PaaS, and SaaS. If an agency needs such TIC support for cloud services, it must state the requirement in its MTIPS task order and follow the appropriate Federal Government IT Security Policies.

1.2 Roles and Responsibilities of the Agency, DHS, GSA, and MTIPS Contractor

The following roles and responsibilities must be clearly understood, and all required tasks completed before deployment of an agency's MTIPS solution.

- **Agency (Client)**
  - Signs a Memorandum of Agreement (MOA) and executes a Service Level Agreement (SLA) with DHS (see Section 1.3 below for details)
  - Reviews and accepts GSA Security Assessment
  - Identifies and assesses the NIST 800-53 Controls associated with MTIPS connectivity (see Table 1 below for listing of Controls)
  - Issues agency Authorization to Operate (ATO)
- **DHS**
  - Completes TIC certification process
  - Operates the National Cybersecurity Protection System (NCPS), also known as EINSTEIN
  - Ensures MOA with agency is in place before connection is activated.
- **GSA**
  - Performs system security assessments for MTIPS (see Section 1.4 below)
  - Issues Provisional Authorization to Operate (PATO)
  - Continuously monitors system
  - Makes security assessment documents available to agency
- **MTIPS Contractor**
  - Performs authenticated scans at least monthly or quarterly
  - Provides MTIPS Plan of Action and Milestones (POA&Ms), with remediation, to GSA monthly or quarterly if necessary (dependent upon existence of any high/critical vulnerabilities)
  - Updates system security documentation at least annually or when any changes to system occur

Table 1—NIST Special Publication 800-53 Revision 4 Customer Responsible Controls

Control Identifier	*Control Title*
AC-4	Information Flow Enforcement
CA-3	Information System Connections
CA-5	Plan of Action and Milestones
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-8	Information System Component Inventory
IR-6	Incident Reporting
PL-2	System Security Plan
RA-2	Security Categorization
RA-3	Risk Assessment
SA-11	Developer Security Testing and Evaluation
SC-5	Denial of Service Protection
SC-7	Boundary Protection

For detailed information on Customer Responsible Controls, see: NIST Special Publication 800-53 R4: Security and Privacy Controls for Federal Information Systems and Organizations.

1.3 DHS Memorandum of Agreement

The agency needs to enter into a formal agreement with DHS relating to the deployment of EINSTEIN, a system that is a vital part of the MTIPS service. Hence, in order to fully implement and begin using MTIPS, the agency Chief Information Officer (CIO) must sign a Memorandum of Agreement (MOA) and execute a Service Level Agreement with DHS.

The MOA facilitates TIC preparations and due diligence for utilizing EINSTEIN. The MOA also authorizes in-line traffic inspection and modification, and such activities that may include the interception, modification, use, and disclosure of agency traffic.

1.4 GSA and Agency's Shared Security Responsibility

GSA and the customer agency share responsibility in ensuring the agency's MTIPS solution meets federal security standards.

GSA, for its part, performs the system security assessment of a contractor's MTIPS system, evaluating the solution up to the edge routers for both the agency and Internet sides. Once satisfied that the MTIPS solution meets federal security standards, GSA issues a Provisional Authorization to Operate (PATO). GSA also makes the assessment documents available to its customer agencies to help them save time and money on their own internal security analysis.

The customer agency is responsible for conducting an assessment to ensure that all of its connections to MTIPS are compliant with the NIST 800-53 R4 High impact security controls shown in Table 1 above. (These controls are known as “Customer Responsible Controls.”) The agency CIO reviews the resulting assessment package, and signs the Authorization to Operate (ATO) once all security requirements have been met.

The agency's ATO must be in place before its MTIPS solution is deployed.

2. Important MTIPS Requirements

2.1 Contractor Requirements

The MTIPS contractor is required to have fully operational TIC, compliant with the OMB TIC directives and with ATO approval from the GSA. The MTIPS contractor is required to identify and route government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities.

The MTIPS contractor provides and supports two (2) components associated with the MTIPS service:

- TIC Portal (TIC Access Points)—(These must be closely monitored by an integral MTIPS Security Operations Center [SOC] to protect agency IP traffic.)
- Transport Collection and Distribution (MTIPS Transport)—(This serves as a "collection" network for TIC physical or virtual portal connectivity insulating an agency's internal network from the Internet and other external networks.)

2.2 Security Requirements

The MTIPS contractor must meet MTIPS-specific security requirements as defined in the System Security Plan (see EIS contract Section C.2.8.4.5.4 System Security Plan [SSP]) at a NIST 800-53 High impact level and must support government security and authorization efforts, including those efforts to verify that these standards are being met. For more detail, refer to the following sections in the EIS contract for MTIPS security requirements:

- C.2.8.4.5.1 General Security Compliance Requirements
- C.2.8.4.5.2 Security Compliance Requirements
- C.2.8.4.5.3 Security Assessment and Authorization (Security A&A)
- C.2.8.4.5.4 System Security Plan (SSP)
- C.2.8.4.5.5 Additional Security Requirements
- C.2.8.4.5.5.1 Personnel Background Investigation Requirements

3. Key Technical Specifications

NOTE: This portion of the service guide has been abridged due to space considerations. For full technical details on MTIPS, please refer to EIS contract Section C.2.8.4 Managed Trusted Internet Protocol Service and to Section C.2.8.4.1.4 Technical Capabilities.

Table 2—MTIPS Technical Capabilities

Capability	*Description*
TIC Portal Capabilities	(1) Provides TIC Portal Access to External Networks including the Internet, and meets the following requirements when establishing interconnecting relationships: • Capability for the TIC Portal connection to the Internet via Tier 1 Internet Service Providers (ISPs). • Allocation of enough interconnection bandwidth to accommodate increasing agency demands. • Capability for alternate and diverse Routing (multiple, physically diverse connectivity to interconnection points). • Inter-carrier Routing Requirements. • Supports Internet Protocol version 6 (IPv6) and is also backward compatible with IPV4 or both IPv4 and IPv6 (i.e. dual-stack). (2) EINSTEIN Protection. (3) TIC Portal Security Operations Center (SOC). (4) ICD 705 Sensitive Compartmented Information Facility (SCIF). (5) Content Filtering/Inspection of Encrypted Traffic with documented procedures. (6) Asymmetric Routing. (7) Federal Video Relay Service (FedVRS) Support. (8) E-Mail Forgery Protection. (9) Support signing procedures for outgoing email messages. **(NOTE: May not be available from all contractors.)** (10) Domain Name System (DNS) and DNS Security Extensions (DNSSEC). (11) Uninterrupted Operations. (12) Internet Protocol Version 6 (IPv6). (13) Data Loss/Leak Prevention.

Table 3—MTIPS Transport Collection and Distribution Capabilities

Capability	*Description*
Transport Collection and Distribution Capabilities	(1) Allows agency's Internet bound traffic to reach the Internet via one of the two TIC Portals. (2) Creation of an agency Trusted Domain (DMZ) to ensure that an agency's traffic is protected and physically isolated when transported to the portal and the public Internet. a. The DMZ includes the access portion of the service as well as the MTIPS transport. b. The contractor ensures that the traffic is not sniffable and ports cannot be spoofed. (3) Routes Inter-agency traffic through the TIC Portal, which inspects the traffic if the connection is classified as an external connection.

Table 4—MTIPS Features

Feature	*Description*
Encrypted Traffic	(1) The TIC Portal monitors, scans and filters the incoming and outgoing encrypted traffic traversing MTIPS (e.g., email, authorized/known bad mail, FTP, and web traffic) which is proxied/non-proxied based on URL or IP address. (2) The TIC portal also analyzes all encrypted traffic for suspicious patterns that might indicate malicious activity and keeps logs of at least the source, destination and size of the encrypted connections for further analysis.
Agency Security Policy Enforcement	(1) Supports the ordering agency's security policy to ensure security regulations compliance. (2) Supports agency's operational models and specific security rules. (3) Supports adjustments to the agency's security strategy based on threats identified by the TIC Portal SOC.
Forensic Analysis	(1) Supports full, real-time, header and payload, raw packet capture of selected agency's traffic flows. (2) Supports subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). (3) Supports engineering parameters applied to the traffic capture such as, but not limited to, packet capture rate and data retention period (e.g., 5% of the agency's traffic traversing the TIC Portal for a period of 60 days).
Custom Reports	The contractor provides reports as required by the ordering agency, including ad-hoc reports.
Agency NOC/SOC Console	The contractor provides additional features and functions (or dashboard customization) customized to agency's specifications not covered by the Web portal which is included in the basic MTIPS service.
Custom Security Assessment and Authorization Support (formerly known as Certification & Accreditation [C&A])	Agencies opting for security controls more stringent than the NIST High-Impact Baseline can negotiate agency-unique requirements directly with the contractor.

Feature	*Description*
External Network Connection	(1) The contractor enables the agency to connect to external IP networks at their physical locations. (2) The traffic exchanged will be IP traffic only and compliant to TIC portal's interconnecting requirements. (3) The TIC portal 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. (4) TIC Portal support includes, but is not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. (5) The following baseline capabilities are supported for external dedicated VPN and private connections implemented using communication services offered through this contract, i.e., private lines or other dedicated connections SONETS, E-LINE, VPNS, etc. at the TIC portal: a. The connection terminates at an appropriate point so that traffic can be routed through the EINSTEIN Enclave to allow traffic to/from the external connections to be inspected. The EINSTEIN Enclave and the security stack at the portals are the public-facing side of the TIC Zone. The incoming traffic from the external network will be inspected within the EINSTEIN Enclave and the security stack before reaching the internal network. b. The connection terminates in front of the full suite of TIC sensors/capabilities to allow traffic to/from external connections to be inspected. c. When connecting over the public networks, including the Internet, the VPN connections are encrypted, compliant with NIST FIPS 140-2. d. Connections terminated prior to routing through the EINSTEIN Enclave may use split tunneling. If required by the agency, the MTIPS contractor will configure telecommunications service priority (TSP) for external connections, including to the Internet, to provide for priority restoration of telecommunication services.

Feature	*Description*
Encrypted DMZ	(1) Supports encryption from the agency's service delivery point (SDP) at the edge of the agency's WAN to the MTIPS Portal (FIPS 140-2 compliant). (2) Contractor provides encryption devices and manages the devices.
Remote Access	(1) The MTIPS portal supports remote access for teleworkers connecting from home or satellite offices and mobile, on-the-go workers. Teleworkers and mobile workers are a subscriber agency's authorized staffs that connect via ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. (2) For permanent VPN connections for branch offices or business partners use Feature # 7 (External Network Connection) or Feature # 10 (Extranet Connections) as appropriate. NOTE: For more details on the baseline capabilities supported for telework/remote access at the MTIPS portal, and the support provided to satisfy the requirements of OMB M-06-16, "Protection of Sensitive Agency Information", please refer to EIS contract Section C.2.8.4.2 MTIPS Feature # 9 Remote Access, sub-items (a) through (i).
Extranet Connections	(1) The TIC portal 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. (2) TIC portal support for extranet connections includes, but is not limited to, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by communication services offered through this contract. NOTE: For more details on the baseline capability supported for extranet dedicated VPN and private line connections at the TIC Portal refer to EIS contract Section C.2.8.4.2 MTIPS Feature # 10 Extranet Connections, sub-items (a) through (e).

Feature	*Description*
Inventory/Mapping Service	(1) The agency may request the MTIPS contractor to keep an inventory or a complete map of all networks connected to the MTIPS portal. (2) The MTIPS contractor maintains a complete map, or other inventory, of all subscriber agencies' networks connected to the TIC access portal. (3) The MTIPS contractor validates the inventory through the use of network mapping devices. (4) Static translation tables and appropriate points of contact are provided to US-CERT on a quarterly basis, to allow in-depth incident analysis.

4. Pricing Basics for MTIPS

Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide to gain an understanding of EIS pricing fundamentals.

4.1 Access Arrangements

Appropriate access arrangements must be selected for each endpoint. Please visit the EIS Resources Listing and locate the Access Arrangements Guide for more detailed information.

4.2 Service Related Equipment (SRE)

- SRE must be chosen based on equipment required at each location. NOTE: SRE uses catalog-based pricing.
- Request that contractor provide pricing for any SRE that would be required, in addition to the agency's existing infrastructure, to deliver the service.
- Please visit the EIS Resources Listing and locate the Service Related Equipment Service Guide for more detailed information.

4.3 MTIPS Price Components

The price structure for MTIPS consists of the components shown in Table 5 below.

Table 5—MTIPS Pricing Components

Component	*Charging Unit*
MTIPS Port: Monthly Recurring Charge (MRC)	Port (includes TIC Portal Capabilities and Transport Collection and Distribution Capabilities)
Features: MRC & Non Recurring Charge (NRC)	Charging unit varies per feature, but would be one of the following: • Per Proposal • Per Report • Per Node • Per Connection • Per Seat • Per Network • Per ICB (i.e. Encrypted Traffic, Agency Security Policy Enforcement, Forensic Analysis, etc.)

Figure 2 below shows how the pricing components in Table 5 are combined to produce the total cost for the service.

Figure 2—This figure shows how the various pricing components in Table 5 would be combined to calculate the total MTIPS charge. NOTE: One or more of these components may not be needed to price a particular service package.

The charges for the different components in *Figure 2* are calculated using details provided in the pricing tables in EIS contract Section B.2.8.4 Managed Trusted Internet Protocol Service. (Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide for instructions on using the pricing tables to compute the cost of a service.)

NOTE:

(1) A contractor may offer a custom variation of the service to meet an agency's unique requirements. Such a customization would be identified with a Task Order Unique CLIN (TUC), and would include charges that would have to be added to the components in Figure 2 to determine the total cost of the service.

(2) If the contractor provides any optional MTIPS security functions, the contractor prices those security functions using the corresponding Managed Security Service prices explained in EIS contract Section B.2.8.5 Managed Security Service.

4.4 MTIPS Pricing Examples

Example: MTIPS with 10Gbps Ethernet Access and Remote Access (100 Seats),

Service CLINs

- Choose CLIN MT00060 "MTIPS - Ethernet – 10 Gbps" (see EIS contract table B.2.8.4.4.2— MTIPS Port Pricing Instructions Table).

- Choose CLIN MT91018 "Remote Access (CONUS and OCONUS, 51 – 100 seats)" (see EIS contract table B.2.8.4.5.2— MTIPS Feature Pricing Instructions Table).

5. References and Other Sources of Information

- For more technical details and information on MTIPS, please refer to EIS contract Section C.2.8.4; for pricing details, Section B.2.8.4.
- For more information on service-related items, please see:
    - EIS contract Section B.2.10 Service Related Equipment
    - EIS contract Section B.2.11 Service Related Labor
- Please refer to a contractor's individual EIS contract for specifics on the contractor's MTIPS offerings.
- For additional EIS information and tools, visit the EIS Resources Listing.
- For guidance on transitioning to EIS, please visit EIS Transition Training where you'll find several brief video training modules.