C.2.4.1.5 Managed Trusted Internet Protocol Service (MTIPS)

The Managed Trusted Internet Protocol Service (MTIPS) allows Agencies to physically and logically connect to the public Internet or other external connections, as required by the Agency, in full compliance with the Office of Management and Budget's (OMB) Trusted Internet Connections (TIC) initiative (M-08-05), announced in November 2007. MTIPS facilitates the reduction of the number of Internet connections in Government networks and provides standard security services to all Government users.

MTIPS solutions offered by Networx contractors shall be subject to periodic DHS compliance assessment modeled after the DoD's Computer Network Defense Service Provider (CNDSP). See the report "Trusted Internet Connections (TIC) Initiative, Statement of Capability Evaluation Report," Prepared by United States – Computer Emergency Readiness Team (US-CERT) / Information Systems Security Line of Business (ISS LOB), June 4th 2008.

MTIPS is comprised of the network infrastructure to transport Internet Protocol traffic between the Agency Enterprise WAN and the Trusted Internet Connection (TIC) Portal; together they create an Agency TIC Trusted Domain (DMZ) for Internet Protocol traffic. The architectural framework of MTIPS is illustrated in Figure C.2.4.1.5-1.

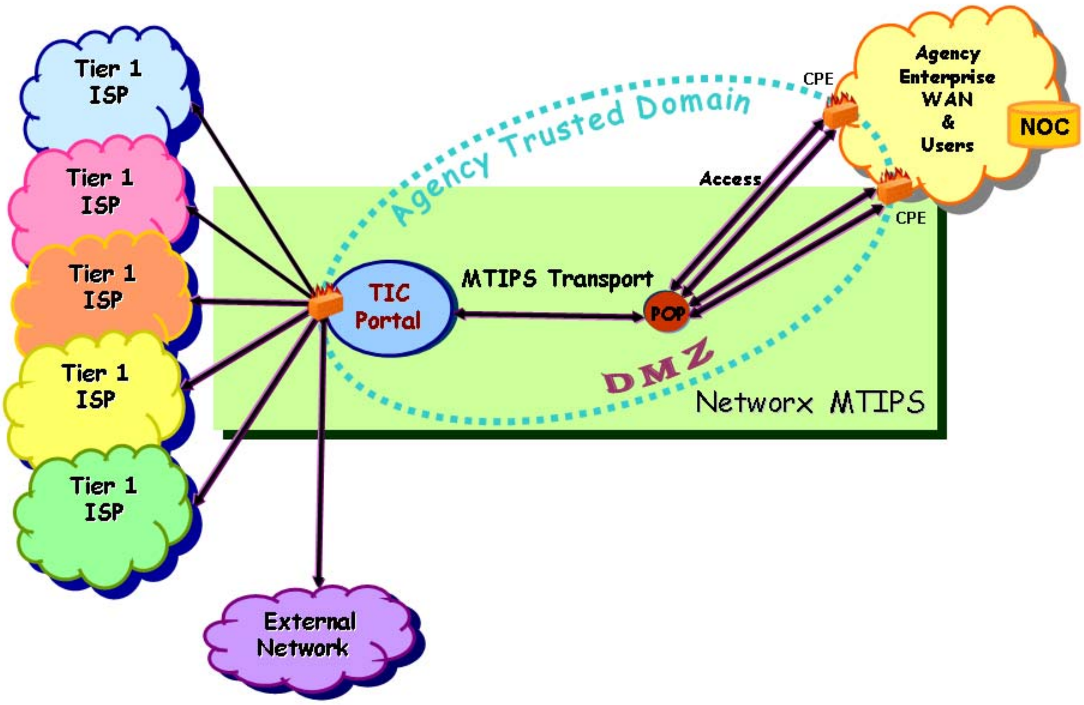

Figure C.2.4.1.5-1 Networx MTIPS Notional Architecture

MTIPS enables the Government to react more effectively to cyber security attacks thus reducing malicious penetrations and theft of critical data. Exchange of information through the TIC Portal is closely monitored by an integral MTIPS Security Operations Center (SOC) to protect Agency IP traffic.

The MTIPS provided transport shall serve as a “collection” network for TIC Portal connectivity insulating an Agency’s internal network from the Internet and other external networks.

[redacted]

C.2.4.1.5.1 Service Description

[redacted]

C.2.4.1.5.1.1 Functional Definition

The MTIPS generic functional model depicted in [redacted] subsumes the following set of functions and sub functions:

(1) TIC Portal

a. Access to the Internet.

b. Hosted EINSTEIN Enclave.

c. Security Operations Center (SOC).

d. [redacted]

(2) Transport Collection and Distribution (MTIPS Transport).

[redacted]

Figure C.2.4.1.5- 2 MTIPS Context Architecture

The traffic collection and distribution supports the transport of Government-only IP traffic between Agency Enterprise WANs and TIC Portals utilizing the secure functionality of the SOC. The TIC Portal SOC monitoring and management systems shall be dedicated to the management and monitoring of the subscribing Agencies hosted by the contractor's portal and shall be isolated from commercial customers.

[redacted]

The contractor shall meet DHS' TIC compliance verification requirements before providing MTIPS service delivery to an Agency. This process can be initiated by the contractor after certification activities have occurred on the specific vendors implemented MTIPS architecture, policies, and procedures. Compliance can be completed before the Agency DAA C&A processes. DHS will conduct periodic TIC compliance reviews.

C.2.4.1.5.1.2 Standards

MTIPS shall comply with the following standards, as applicable, and when commercially available. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions of the listed standards.

1. Applicable Internet Engineering Task Force (IETF) RFCs.
2. T1.276-2003 American National Standard for Telecommunications — Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.
3. IP/MPLS Forum.
4. IEEE
    a. 802.1Q
    b. 802.1P
    c. 802.3AD
5. Metro Ethernet Forum (MEF).
6. The PCI Data Security Standard (PCI DSS).
7. All new versions, amendments, and modifications to the above documents and standards when offered commercially.
8. MTIPS providers shall comply with current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security, including those listed below. Contractors shall comply with new document versions, amendments, and modifications. Those most notable include minimum expectations for MTIPS specified security services identified in this SOW. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions.
9. E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA)).
10. NIST Federal Information Processing Standards Publication (FIPS) PUB 140-2 — Security Requirements for Cryptographic Modules.
11. NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems.

12. United States Computer Emergency Readiness Team (US CERT) reporting requirements. (http://www.us-cert.gov/federal/reportingRequirements.html)
13. The Health Insurance Portability & Accountability Act of 1996 (HIPAA) Standards for the Security of Electronic Health Information.
14. The Sarbanes-Oxley Act of 2002.
15. The Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, November 12, 1999 (GLBA).
16. The PCI Data Security Standard (PCI DSS).
17. [redacted]
18. Standards included in Networx Contract Section C.2.4.3.1.2, Collocated Hosting Service (CHS).
19. Standards included in Networx Contract Section C.2.7.3.1.2, Network Based IP Virtual Private Network Service (NBIP-VPNS).
20. Standards included in Networx Contract Section C.2.10.1.1.2, Managed Firewall Service (MFS).
21. Standards included in Networx Contract Section C.2.10.2.1.2, Intrusion Detection and Prevention Service (IDPS).
22. Standards included in Networx Contract Section C.2.10.4.1.2, Anti-Virus Management Service (AVMS).
23. Department of Homeland Security Management Directive Number 11042, DHS MD11042, 2005.
24. Electronic Code of Federal Regulation, Title 49, PART 1520--Protection Of Sensitive Security Information
25. IETF RFC 1757 — Remote Network Monitoring Management Information Base.
26. NIST suite of documents for conducting C&A.
    a. SP 800-18 Rev 1 — Guide for Developing Security Plans for Federal Information Systems.
    b. SP 800-30 — Risk Management Guide for Information Technology Systems.
    c. SP 800-34 — Contingency Planning Guide for Information Technology Systems.
    d. SP 800-37 — Guide for the Security Certification and Accreditation of Federal Information Systems.
    e. SP 800-53 Rev 2 — Recommended Security Controls for Federal Information Systems.

  f. Annex 3 to SP 800-53 Rev 2 — High Impact Baseline.
  g. SP 800-53 A — Guide for Assessing the Security Controls in Federal Information Systems.
  h. SP 800-59 — Guideline for Identifying an Information System as a National Security System.
  i. SP 800-60 — Guide for Mapping Types of Information and Information Systems to Security Categories.
  j. SP 800-64 Rev 1 — Security Considerations in the Information System Development Life Cycle.
  k. SP 800-84 — Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.

27. Designation and Sharing of Controlled Unclassified Information (CUI), http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html
28. All commercially available standards for any applicable underlying access and transport services.
29. OMB Memo M-05-22 — Transition Planning for Internet Protocol Version 6 (IPv6).

.

C.2.4.1.5.1.3 Connectivity

The MTIPS provider shall connect and interoperate with:

1. The Public Internet — MTIPS shall enable the subscribing Agency's users to connect to the Internet through the TIC Portal.
2. [redacted]
3. [redacted]
4. Other Agency IP Networks. See Requirement C.2.4.1.5.2.1 (7).

C.2.4.1.5.1.4 MTIPS Technical Capabilities

C.2.4.1.5.1.4.1 TIC Portal Capabilities

The following TIC Portal capabilities are mandatory, unless marked optional:

1. **TIC Portal Access to the Internet** — In order to ensure that Agencies are able to exchange traffic with the Internet and external networks at all times the TIC Portal shall comply with the following requirements when establishing interconnecting relationships:
    a. The TIC Portals shall connect to the Internet via Tier 1 Internet Service Providers (ISPs).
    b. The contractor shall budget enough interconnection bandwidth to accommodate increasing Agency's demands.
    c. Alternate Routing — The contractor's TIC Portal shall provide multiple, physically diverse connectivity to interconnection points.
        i. The TIC Portal shall enable alternate routing functions to keep the portals operating at all times.
        ii. [redacted]
        iii. [redacted]
        iv. [redacted]
    d. The contractor shall establish and provide interconnection points in CONUS and shall support OCONUS and Non-Domestic traffic.
    e. Private interconnection agreements shall be established to connect the TIC Portal to the Internet by one or both of the following means:
        i. Direct Circuit Interconnection, where the two parties share point-to-point circuits (i.e., neutral locations).
        ii. Exchanged-Based Interconnection Model, that takes place in a neutral exchange site. At the TIC Portal all government traffic shall be separated from commercial traffic by dedicated routers/switches connecting the TIC Portal to public Internet facing routers. This will ensure security for the government traffic.

f. Inter-carrier Routing Requirements — The ISPs and external networks converging to a portal shall run BGP (eBGP, BGP4, etc.) or one of the options for inter-AS connectivity as specified by the IETF.

2. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. **TIC Portal Security Operations Center (SOC)** — The TIC Portal SOC is the set of tools, appliances and processes that collect, reduce, normalize, correlate, fuse, and manage event data from a variety of devices that support the MTIPS operations. For the SOC, these devices include firewalls, Network Intrusion Detection Devices (NIDS), Host-based IDS (HIDS), and other platforms that may collect TIC Portal-relevant event data. The SOC tools also provide reports customized to Agency's requirements [Refer to Section C.2.4.1.5.2.1 — MTIPS Features] but as a minimum shall support TIC Portal authorities / analysts by identifying security events of interest that may be negatively affecting the TIC Portal environment. [redacted]

[redacted]

Figure C.2.4.1.5- 3 The TIC Portal Security Operations Center Architecture

The primary goal of the SOC is to provide analysis/correlation and management structure to mitigate the threat presented by external attacks. The contractor shall provide the following security functions:

a. Support to all SOC functions. The contractor shall be responsible for monitoring, incident response, vulnerability management, vulnerability assessment, incident reporting, engineering support, and TIC Portal SOC standard security policy enforcement at the hosting facility. The contractor shall describe clearly the building blocks of the proposed security solution and their internal components. The following items shall be included:

   i. Architectural diagram and its description.

   ii. TIC Portal physical locations appropriately labeled.

   iii. Consistency on the labeling of the architectural building blocks and the proposal's text.

   iv. Clear relationship between the solution's building blocks and their internal components.

   v. [redacted]

vi. [redacted]

vii. Functional relationship between the SOC and the NOC.

viii. Redundancy of the security stack at each TIC Portal.

ix. Storage network or systems, and their physical location.

b. [redacted]

c. All systems accessible from the Internet shall reside in the Agency's Trusted Domain.

d. All inbound and outbound connections shall be set to a default "deny" policy.

e. The basic SOC shall protect Controlled Unclassified Information (CUI) data.

f. The basic SOC shall provide event validation to determine if alerts/threats/events generated by different sources [sensors, SOC infrastructure] after being correlated in the appropriate context are relevant to the Agency's business to be escalated and examined by the security authorities.

g. The SOC shall support escalation functions.

h. The SOC shall be the central coordination point of contact (POC) for computer security incidents across the SOC for the subscribing Agency.

i. The SOC architecture shall limit outbound connections so that only needed services are allowed. The contractor shall keep an inventory of such services that shall be verified daily.

j. [redacted]

k. The SOC shall provide centralized, secured, and unified management of security events in order to protect the integrity of the US Government data and infrastructure.

l. [redacted]

m. [redacted]

n. All the devices involved in the SOC implementation shall be synchronized via Network Time Protocol (NTP) adhering to

Universal Standard Time (UST) and clearly designating time zone in time stamps to ensure consistency.

o. [redacted]

p. The SOC architecture previously depicted in Figure C.2.4.1.5-3, shall comprise the following building blocks at a minimum:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

q. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

r. The TIC Portal components shall function on hardened and patched platforms in compliance with the applicable NIST standards.

s. The SOC shall provide alert and health status of MTIPS components.

t. The SOC shall be able to accommodate network and system event data without degradation of performance.

u. The contractor shall build two instances of the TIC Portal SOCs that are manned with qualified personal 24x7 and [redacted] different physically diverse locations. [redacted]

4. [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

C.2.4.1.5.1.4.2 MTIPS Transport Collection and Distribution Capabilities

The following MTIPS capabilities are mandatory unless marked optional:

1. [redacted]
2. The contractor shall support failover mechanisms that will reroute Agency's traffic [redacted]
3. The contractor shall support link (backbone) aggregation of the diverse access speeds between the subscribing Agency's SDP and the TIC Portal.
4. The contractor shall provide interworking services at the POP for Agency locations to transparently access MTIPS using the following services:
    a. The contractor's ATM networks
    b. The contractor's FR networks
    c. The contractor's Ethernet networks (optional)
    d. The contractor's NBIP-VPN networks
5. [redacted]
6. [redacted] -
7. [redacted]

    [redacted]

    [redacted]

8. [redacted]

9. The firewall(s) supported shall be compliant to the TIC Portal SOC standard security policy, as described in Section C.2.4.1.5.1.4 (3).

10. Inter-Agency traffic shall be routed through and inspected by the TIC Portal.

11. [redacted]

12. [redacted]

    [redacted]

    [redacted]

        [redacted]

        [redacted]

13. The contractor shall provide subscribing Agencies with a web-based administrative tool to view the following:

    a. Operational state.

    b. Order status.

    c. Other transport parameters associated with each MTIPS.

C.2.4.1.5.1.5 MTIPS Basic Service Summary

1. The contractor shall provide a summary of all the functions and capabilities included in the MTIPS basic service offering.

2. [redacted]

    [redacted]

    [redacted]

        [redacted]

        [redacted]

[redacted]

[redacted]

[redacted]

C.2.4.1.5.2 Features

The MTIPS features delineated in Section C.2.4.1.5.2.1 are mandatory unless marked optional.

C.2.4.1.5.2.1 MTIPS Features

ID	Name of	Description
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ID Number	Name of Feature	Description
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ID Number	Name of Feature	Description
6	Custom Certification and Accreditation (C&A) Support	1. [redacted] 2. The contractor shall provide additional support to the Agency in the C&A process for systems and services provided under the contract in accordance with the following prescribed activities: a. OMB Circular A-130 Appendix III — Management of Federal Information Resources. b. NIACAP (NSTISSI 1000) — National Information Assurance Certification and Accreditation Process. c. NIST SP 800-37 — Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems. d. [redacted] e. Agency specific requirements for Certification and Accreditation. 3. The contractor shall ensure that the C&A deliverables comply with all applicable federal laws, regulations, policies, guidelines, and standards.
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

C.2.4.1.5.3 Interfaces

The contractor shall support the User-to-Network interfaces (UNIs) defined in Section C.2.4.1.5.3.1 for the provisioning of MTIPS.

C.2.4.1.5.3.1 User-to-Network Interface for MTIPS

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1	Asynchronous Transfer Mode (ATM)	1. T1 2. T3 3. E1 4. E3 5. OC-3c 6. OC-12c	IP/PPP over ATMS
2	Cable High Speed Access (Optional)	320 Kbps up to 10 Mbps	IP/PPP
3	Ethernet	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional)	IP/PPP over Ethernet
4	Frame Relay (FR)	1. 56 Kbps with 32 Kbps CIR 2. Fractional T1 1. 128 Kbps with 64 Kbps CIR 2. 256 Kbps with 128 Kbps CIR 3. 384 Kbps with 128 Kbps CIR 4. 512 Kbps with 256 Kbps CIR 5. 768 Kbps with 384 Kbps CIR 3. T1 1. 1.536 Mbps with 768 Kbps CIR 2. 1.536 Mbps	IP/PPP over FRS

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
		with 1024 Kbps CIR 4. Fractional T3 1. 3 Mbps 2. 6 Mbps 3. 12 Mbps 4. 24 Mbps 5. 45 Mbps 5. T3 6. E1 7. E3	
5	IP over SONET	1. 0C-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET
6	Electrical Interfaces for Dedicated Wireline Access	1. DS0 2. Fractional T1 3. T1 4. Fractional T3 5. T3 6. E1 7. E3	IP/PPP
7	Broadband Access (Optional)	xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	IP/PPP
8	Satellite Access (Optional)	See Networx Contract Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	

C.2.4.1.5.4 MTIPS Performance Metrics

The performance levels and AQL of KPIs for MTIPS in Sections C.2.4.1.5.4.1 through C.2.4.1.5.4.3 are mandatory unless marked optional.

C.2.4.1.5.4.1 Performance Metrics for TIC Portal

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(TIC Portal)	[redacted]	[redacted]	[redacted]	[redacted]
Grade of Service (Failover Time)	[redacted]	[redacted]	[redacted]	[redacted]
Grade of Service (Monitoring and Correlation)	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	
Grade of Service (Configuration/Rule Change)	[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]	
EN (Firewall Security Event Notification)	[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]	
		[redacted]	[redacted]	
EN (Intrusion Detection/Protection Security Event Notification)	[redacted]	[redacted]	[redacted]	
		[redacted]	[redacted]	
Grade of Service (Virus Updates and Bug Fixes)	[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]	

Notes:

1. The TIC Portal availability is calculated as a percentage of the total reporting interval time that all the TIC Portal components are operationally available to the Agency. Availability is computed by the standard formula:

$$Availability(TICPortal) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Failover Time for the TIC Portal is the time that it takes to switch from one TIC Portal instance to another provided by the same contractor.
3. Grade of Service (Monitoring and Correlation) — [redacted]
4. The GOS (Configuration/Rule Change) value represents the elapsed time between the configuration/change request and the change completion. The value is measured by logs/reporting. Changes are initiated and prioritized by the Agency, or may be implemented in response to an event. Changes initiated by the contractor require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
5. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the Agency. Events are categorized as follows:
   a. Low — Events in the Low category have a negligible impact on service. They include incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
   b. Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.
   c. High — Events in the High category represent violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, which should be immediately reported via email, pager, or telephone, as specified by the Agency.
6. Grade of Service (Virus Updates and Bug Fixes) represents the time between the release of the virus updates and bug fixes (patches), and their deployment. This indicator ensures automatic and timely delivery of updates/bug fixes.

C.2.4.1.5.4.2 Reserved

C.2.4.1.5.4.3 Performance Metrics for MTIPS Transport Collection and Distribution

For MTIPS Transport Collection and Distribution, the nomenclatures of "*end-to-end*" and *"Networx core"* refer to the connectivity from the Agency's SDP to the access point of connection to the TIC Portal.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(Port)	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	
Latency (CONUS)	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	
GOS(Data Delivery Rate)	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	
Time to Restore	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	
EN(Security Incident Reporting)	[redacted]	[redacted]	[redacted]	[redacted]

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100 \,.$$

   For *critical user type*, the contractor would provide essentially 100% uptime for customer's Internet connection with high availability equipment, redundancy, automatic restoration, and reconfiguration.

2. Latency is the average one-way time for IP packets to travel over the Networx core network. The Backbone Latency metric does not apply for DSL, Cable High Speed, and Satellite access methods.

3. Network packet delivery is a measure of IP packets successfully sent and received over the Networx core network.

4. See Networx Contract Section C.3.3.1.2.4 for the definitions and measurement guidelines.

5. [redacted]

C.2.4.1.5.5 MTIPS Network Operations and Management

C.2.4.1.5.5.1 Network Management

The contractor shall provide Network Management. See Networx Contract Section C.3.3.1 for the Network Management requirements.

C.2.4.1.5.5.2 Security Management

The contractor shall provide Security Management. See Networx Contract Section C.3.3.2 for the Security Management requirements.

The contractor shall support the following operational functions applicable to the contractor's networks and equipment, in addition to the functions specified in Section C.3 of the Networx contracts:

1. Remote management of all contractor's network equipment and servers shall be carried through an encrypted connection (e.g., SSH, HTTPS, etc).
2. Management of all contractor's network equipment and servers shall require strong authentication (e.g., one-time password, cryptographic key exchange, etc.) instead of relying on static userID and password, even if the userID and password are encrypted.
3. [redacted]
4. The contractor shall create a connection control program where machines that will be connected to new systems shall be fingerprinted, and base-lined. This meta-data shall be archived and the systems shall be audited weekly to maintain the baseline. Included with authorization are the name, telephone number, and email of the system administrator responsible for controlling that machine. The database of system administrators shall be verified at least once a month.
5. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C.2.4.1.5.5.2.3 Roles and Responsibilities

The roles and responsibilities of the subscribing Agency and the contractor for the basic MTIPS operations are described in Table C.2.4.1.5- 1 below. The contractor shall agree with the subscribing Agency on specific requirements to support an Agency's mission.

Table C.2.4.1.5- 1 Subscribing Agency & Contractor Roles for MTIPS Security Operations

ID Number	TIC SOC Security Support Services O&M Functions	Subscribing Agency Role	Contractor Role
1	Security Device Monitoring	1. Receive alerts from distributed devices 2. Monitor devices	1. Provide devices' alerts and system reporting 2. Monitor devices.
2	Security Device Administration & Management	1. Validate alerts 2. Determine response	Provide initial alerts' analysis
3	Security Engineering	Review for implementation and support	Design for implementation and support
4	Audit Log Management	Acceptance and oversight	Acceptance and oversight
5	Transition and Implementation	Acceptance and oversight	Acceptance and oversight
6	Access Controls (security devices)	Grant access based on verification	Implement and monitor access controls
7	Firewall Management	Oversight, review and approval	Manage all firewall rules and configurations
8	Network Intrusion Security Event Detection / Analysis / Prevention	Global oversight	1. Monitor 2. Initial analysis 3. Provide reports on anomalous network events
9	Network Anti-Virus Management	Oversight	1. Manage scanning devices 2. Monitor incoming traffic
10	Incident Response and Management	Oversight and engineering support	Proactive & Reactive engineering support
11	Vulnerability Assessment and Management	Compliance tracking and oversight	Conduct assessment in accordance with schedule
12	Change and Configuration Management	Initiate and approve changes	Initiate and implement changes

ID Number	TIC SOC Security Support Services O&M Functions	Subscribing Agency Role	Contractor Role
13	Security Reporting	Review and oversight	Produce status & performance reports in accordance with schedule
14	Security Policy Enforcement and Review	Create policy guidance and review	1. Enforce policy guidance 2. Provide recommendations

C.2.4.1.5.6 Disaster Recovery

The contractor shall provide Disaster Recovery. See Networx Contract Section C.3.3.3 for the Disaster Recovery requirements.

C.2.4.1.5.7 Service Level Agreements

The Internet Protocol Service (IPS) is offered by the Networx Contracts as unprotected IPS as required in Section C.2.4.1 and as Managed Transport IPS (MTIPS) as described in Section C.2.4.1.5. Agencies have the ability to select how to access the Internet.

The Networx Contract in Section J.13 defines the required Service Level Agreements (SLAs) that Contractors must meet. A Service Level Agreement (SLA) is an agreement between the General Services Administration (GSA) and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s).

Therefore, the contractors supporting MTIPS shall comply with the following:

1. Guidelines on the Networx SLAs included in Section J.13.1 of the Networx Contract.
2. SLA Measurement Guidelines provided in Networx Contract Section J.13.2 SLA Measurement Guidelines
3. SLA Performance Objectives for MTIPS as included in Section J.13.3.9.1.
    a. Service-Independent Performance Objectives — The contractor shall meet the service-independent SLAs in Networx Contract Section J.13.3 SLA Performance Objectives.
4. Credit Arrangements — The contractor shall meet the requirements in Networx Contract Section J.13.4 Credit Arrangements.

C.2.4.1.5.8 MTIPS FISMA Certification & Accreditation (C&A)

C.2.4.1.5.8.1 MTIPS FISMA C&A Scope

1. The Government designates each TIC Access Portal Security Operations Center (SOC) as a federally-controlled information system that is contractor owned-and-operated on behalf of subscribing agencies. Accordingly, the contractor shall fully conform & comply with FISMA requirements as implemented by OMB and NIST.
2. In addition, Homeland Security Presidential Directive 12 (HSPD-12) applies to each contractor SOC. The contractor shall comply with HSPD-12 as implemented by OMB Memorandum-05-24 (M-05-24), “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” as well as Memorandum-07-06 (M-07-06), “Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials.”
3. The Government defines each TIC Portal Security Operations Center (SOC) to be a FIPS 199 “High-Impact System.” The SOC security accreditation boundary consists of the hardware components, software components, firmware components, and system interconnections that constitute the TIC Portal SOC. [redacted]
4. Table C.2.4.1.5-2 presents an overview of the MTIPS security domains and clearly differentiates the FISMA C&A of the SOC from the other MTIPS components.

[redacted]

Component	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SOC	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
Hosted EINSTEIN Enclave	[redacted]	[redacted]	[redacted]	[redacted]	
Internet Access	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
MTIPS Transport	[redacted]	[redacted]			
Access to Agency Enterprise WAN	[redacted]	[redacted]			

C.2.4.1.5.8.2 MTIPS FISMA Certification & Accreditation (C&A) – Stipulated Requirements

The MTIPS C&A requirements each require a stipulated response from the contractor affirming the contractor's commitment to fully comply with all OMB and NIST guidelines for C&A at the [redacted]. The Government requests no narrative responses to Section C.2.4.1.5.8.2 stipulated requirements.

C.2.4.1.5.8.2.1 General Requirements

1. The Contractor shall employ the [redacted] security controls as defined by [redacted] to determine the minimum security baseline.
2. The Contractor shall execute the C&A process in full compliance with SP 800-37 including all referenced standards and guidelines. In all cases, the referenced document is defined to be the latest approved release.

Figure 2.4.1.5-4 illustrates the specific activities in the NIST Risk Management Framework and the information security standards and guidance documents associated with each activity[1].

Figure 2.4.1.5-5 provides a high-level view of the security certification and accreditation process including the tasks associated with each phase in the process[2].

[1] Reference: NIST SP 800-53, Rev 2, pg 16.

[2] Reference: NIST SP 800-37, pg 25.

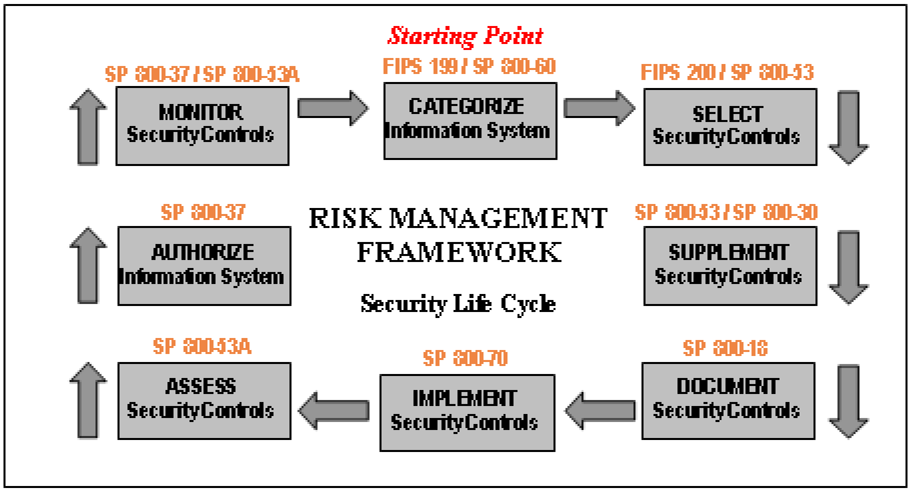

Figure 2.4.1.5-4 NIST Risk Management Framework

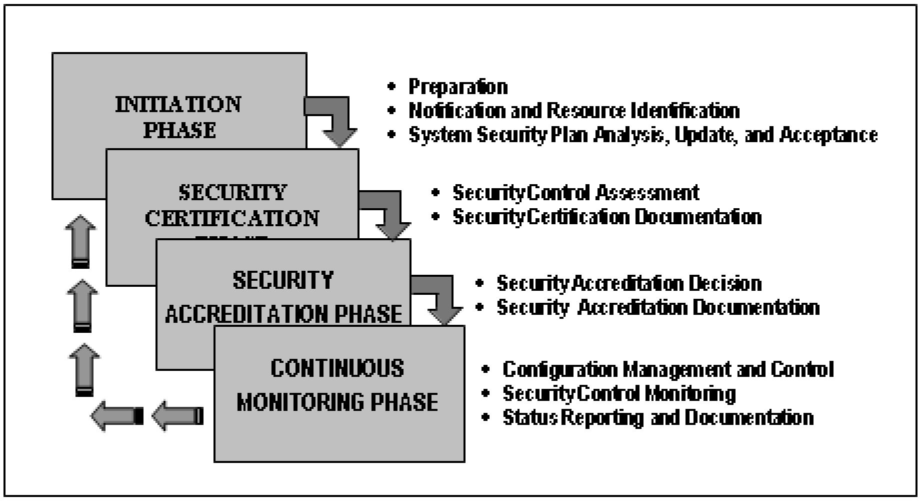
INITIATION PHASE
• Preparation
• Notification and Resource Identification
• System Security Plan Analysis, Update, and Acceptance
SECURITY CERTIFICATION
• Security Control Assessment
• Security Certification Documentation
SECURITY ACCREDITATION PHASE
• Security Accreditation Decision
• Security Accreditation Documentation
CONTINUOUS MONITORING PHASE
• Configuration Management and Control
• Security Control Monitoring
• Status Reporting and Documentation

Figure 2.4.1.5-5. Security Certification and Accreditation Process

A summary table of all security certification and accreditation tasks and subtasks and the individuals responsible for accomplishing those tasks and subtasks is provided in Table C.2.4.1.5-2[3].

3. Contractor is designated the “Information System Owner” role and shall complete each task & sub-task that is assigned to the Information System Owner Role.

4. Contractor shall support each task & sub-task that is assigned to the Authorizing Official and/or Senior Agency Information Security Officer role.

[3] Reference: NIST SP 800-37, Appendix D, pg 59.

5. Contractor shall acquire the services of an independent third-party Certification Agent (CA) that will conduct each C&A task/subtask that is assigned to the CA role.
6. Contractors shall provide each subscribing agency with complete, accurate, and trustworthy information on the security status of each Security Operations Center (SOC) in order for Agency officials to make timely, credible, risk-based decisions on whether to authorize agency operation of contractor's SOC.
7. Contractors shall develop the information and supporting evidence needed for security accreditation during a detailed security review of an information system, typically referred to as security certification.
8. Contractors shall directly manage the CA's contract; shall be accountable for establishing, maintaining, and demonstrating the CA's independence; and shall ensure that the sub-contact scope and resources are adequate.

C.2.4.1.5.8.2.2 Minimum C&A Requirements for Basic MTIPS Service

For each SOC, contractor's CA shall provide each subscribing agency with the following minimum information and supporting evidence to support Agency accreditation decisions:

1. The Contractor shall develop and maintain a SOC System Security Plan (SSP) IAW NIST SP 800-18. The SSP shall be submitted with the draft certification package for a full C&A and updated as required but not less than annually.
2. The contractor shall develop & maintain a SOC Assessment Test Procedures (ATP) IAW NIST SP 800-53 and SP 800-53A. The ATP shall be submitted with the C&A certification package and updated as required but not less than annually.
3. The contractor shall develop and maintain a SOC Risk/Security Assessment Report IAW NIST SP 800-53A. The ATP shall be updated as required but not less than annually.
4. The contractor shall develop and maintain a SOC Plan of Actions & Milestones IAW OMB M-02-01 and annual reporting Instructions (e.g., M-08-09). The POA&M shall be updated as required but not less than quarterly.
5. The contractor shall develop and maintain a SOC Configuration Management (CM) Plan in contractor format. The CM Plan shall be updated as required but not less than annually.
6. The contractor shall develop and maintain a SOC Contingency Plan (CP) IAW NIST SP 800-34. The CP shall be updated as required but not less than annually.
7. The contractor shall conduct a Contingency Plan Test IAW NIST SP 800-34 not less than annually. The contractor shall submit the results of the Contingency Plan Test IAW NIST SP 800-34.

8. The contractor shall conduct security control assessment & test and submit vulnerability scanner reports and script-generated hardening data on not less than a quarterly basis. As a minimum, the contractor shall submit the scanner & script reports to provide a formal body of evidence in support of the quarterly POA&M submittal.
9. The GSA Networx Program Management Office (PMO) will serve as Government Program Manager for C&A of the basic MTIPS service. Accordingly, GSA will participate throughout the C&A life cycle and will accept each SOC's certification documentation set on behalf of all potential Agency subscribers to the basic MTIPS service. The GSA Senior Program Manager will issue a Government-wide Certification Memorandum in support of subscribing Agencies and will manage the Plan of Action & Milestones (POA&Ms) for the basic MTIPS SOC C&A.
10. The contractor shall conduct a security control self assessment in support of the annual OMB FISMA Self Assessment. This self-assessment shall review the SOC security control baseline, affirm that each control is properly implemented at the [redacted] and is functioning as intended; and document any/all controls for which an enhancement is planned.

C.2.4.1.5.8.2.3 Custom C&A Support for Agency-Unique Requirements

1. Contractor shall provide Custom C&A Support by Feature ID No. 6, Figure 2.4.1.5.2.1 MTIPS Features. Custom support may address agency-unique requirements for the Initial C&A, Continuous Monitoring, and/or OSS Changes and Three-Year FISMA Recertification. Negotiated scope of work shall be incremental using the minimum C&A Support baseline of the basic MTIPS service.

C.2.4.1.5.8.2.4 Release of Contractor C&A Information to Subscribing Agencies

1. Contractor shall directly manage the release of all security certification documentation to subscribing agencies IAW with contractor's information security requirements.
2. Contractor shall execute required Non-Disclosure Agreements with Agency representatives as required. Prior coordination with or approvals from the Networx Program Management Office is not required.
3. Contractor shall maintain an audit log of all releases of certification & accreditation documentation.
4. Contractor shall provide audit reports to the Program Management Office upon request and reports any security breaches.
5. Contractors shall develop security certification documentation in accordance with NIST guidelines. Security certification documentation that is provided as

part of the basic MTIPS service need not respond to any Agency-specific documentation formats or agency specific standards.

Table C.2.4.1.5-2 Summary of FISMA C&A Phases and Responsibilities

PHASES, TASKS, AND SUBTASKS	RESPONSIBILITY
INITIATION PHASE	
Task 1: Preparation	
Subtask 1.1: Information System Description	Information System Owner
Subtask 1.2: Security Categorization	Information System Owner
Subtask 1.3: Threat Identification	Information System Owner
Subtask 1.4: Vulnerability Identification	Information System Owner
Subtask 1.5: Security Control Identification	Information System Owner
Subtask 1.6: Initial Risk Determination	Information System Owner
Task 2: Notification and Resource Identification	
Subtask 2.1: Notification	Information System Owner
Subtask 2.2: Planning and Resources	Authorizing Official Sr. Agency Information Security Officer Information System Owner Certification Agent
Task 3: System Security Plan Analysis, Update, and Acceptance	
Subtask 3.1: Security Categorization Review	Authorizing Official Sr. Agency Information Security Officer Certification Agent
Subtask 3.2: System Security Plan Analysis	Authorizing Official Sr. Agency Information Security Officer Certification Agent
Subtask 3.3: System Security Plan Update	Information System Owner
Subtask 3.4: System Security Plan Acceptance	Authorizing Official Sr. Agency Information Security Officer
SECURITY CERTIFICATION PHASE	
Task 4: Security Control Assessment	
Subtask 4.1: Documentation & Supporting Materials	Information System Owner Certification Agent
Subtask 4.2: Methods and Procedures	Certification Agent
Subtask 4.3: Security Assessment	Certification Agent
Subtask 4.4: Security Assessment Report	Certification Agent
Task 5: Security Certification Documentation	
Subtask 5.1: Findings and Recommendations	Certification Agent
Subtask 5.2: System Security Plan Update	Information System Owner
Subtask 5.3: Plan of Action & Milestones Preparation	Information System Owner
Subtask 5.4: Accreditation Package Assembly	Information System Owner
SECURITY ACCREDITATION PHASE	
Task 6: Security Accreditation Decision	
Subtask 6.1: Final Risk Determination	Authorizing Official
Subtask 6.2: Risk Acceptability	Authorizing Official
Task 7: Security Accreditation Documentation	
Subtask 7.1: Security Accreditation Package Transmission	Authorizing Official
Subtask 7.2: System Security Plan Update	Information System Owner
CONTINUOUS MONITORING PHASE	
Task 8: Configuration Management and Control	
Subtask 8.1: Documentation of Info. System Changes	Information System Owner
Subtask 8.2: Security Impact Analysis	Information System Owner
Task 9: Security Control Monitoring	
Subtask 9.1: Security Control Selection	Information System Owner
Subtask 9.2: Selected Security Control Assessment	Information System Owner
Task 10: Status Reporting and Documentation	
Subtask 10.1: System Security Plan Update	Information System Owner
Subtask 10.2: Plan of Action and Milestones Update	Information System Owner
Subtask 10.3: Status Reporting	Information System Owner

C.2.4.1.5.9 Supply Chain Risk Management (SCRM) Plan

Managed Trusted Internet Protocol Service (MTIPS) shall include a Contractor Supply Chain Risk Management (SCRM) Plan to address counterfeit and illegally modified products.

The MTIPS supply chain consists of organizations, people, activities, information, resources, and also the information and communication technology (ICT) equipment, subcomponents and software. The products are installed into the MTIPS configuration, from the contractor, system integrators, ICT re-sellers, and ICT and component OEMs. “Genuine Information and Communications Technology (ICT)” are ICT equipment, components and software that are as represented by their suppliers, whether named brand products or commodity products specified only by performance characteristics.

The contractor shall develop a SCRM Plan to reduce supply chain risks to performance and security of the contractor’s MTIPS throughout the contractor’s Multi-Agency Transport Internet Connection Access Provider (TICAP) solution life cycle.

C.2.4.1.5.9.1 SCRM Plan Requirements

The SCRM Plan shall provide sufficient detail for the Government to determine the contractor reasonably understands the MTIPS Supply Chain. The contractor shall ensure that Genuine ICT will be employed in the MTIPS, and shall manage the risk that counterfeit or illegally modified products will be employed within the MTIPS. The SCRM Plan shall describe the processes and practices the contractor shall employ to ensure that Genuine ICT is employed in the contractor’s MTIPS. As a result, a body of evidence will be generated through SCRM Plan execution. The body of evidence will provide the Government assurance that Genuine ICT is employed in the contractor’s Multi-Agency Transport Internet Connection Access Provider (TICAP) solution.

The technical proposal for a SCRM Plan shall address, at a minimum, how the contractor:

1. Ensures within its processes that requirements for Genuine ICT are levied upon its direct suppliers, whether systems integrator, reseller or OEM. The requirements for assurance and supporting evidences shall include:
    a. That system integrators perform all steps to ensure contractor’s SCRM plan will be performed for ICT in delivered configuration
    b. That the equipment resellers from whom the contractor purchases ICT for use within the MTIPS have valid licenses for OEM equipment and software

    c. That the ICT OEM is exercising quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product
    d. Ensures traceability of assurance and evidence of genuineness of ICT back to the licensed product and component OEMs.

2. Ensures that products and components are not repaired and shipped as new products and components provided to the Government.
3. Ensures the MTIPS will be monitored for counterfeit throughout the life cycle to include maintenance and repair.
4. Ensures independent verification and validation of assurances and supporting evidence, as required.