AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 of 20

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00146	See Block 16B	PR201707210009	

6. ISSUED BY CODE

General Services Administration/FAS/ITC
Office of Acquisition Operations, Interagency Contracts
1800 F Street, NW
Washington DC 20405

7. ADMINISTERED BY *(If other than Item 6)* CODE

8. NAME AND ADDRESS OF CONTRACTOR

Defined Technologies, LLC
8330 Boone Blvd., Suite 600a
Vienna, VA 22182

CODE FACILITY CODE

(☐)	9A. AMENDMENT OF SOLICITATION NO.
	9B. DATED ***(SEE ITEM 11)***
X	10A. MODIFICATION OF CONTRACT/ORDER NO. GS00Q17NSD3008
	10B. DATED ***(SEE ITEM 13)*** 7/31/2017

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is ☐ extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning ___ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATA SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(☐)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Mutual Agreement of Both Parties (FAR 43.103(a)(3))
	OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor _ is not, X is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

SEE CONTINUATION PAGES

Except at provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
Anthony R. Jimenez Executive Director	Joseph Brozi Contracting Officer

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
Anthony Jimenez Digitally signed by Anthony Jimenez DN: cn=Anthony Jimenez, o=Defined Technologies, LLC, ou=Executive Director, email=TJimenez@DefTech.com, c=US Date: 2021.02.25 16:15:53 -05'00' *(Signature of person authorized to sign)*	25 Feb 2021	JOSEPH BROZI Digitally signed by JOSEPH BROZI Date: 2021.02.25 17:05:08 -05'00' *(Signature of Contracting Officer)*	

1. The purpose of this modification is to:
    a. Add Broadband Internet Service (BIS) to the contract.
    b. Add the Managed Security Services (MSS) Trusted Internet Connections Service (TICS) to the contract.
    c. Add references to FIPS 140-3 where FIPS 140-2 is referenced throughout Section C.
    d. Adjust or remove Interfaces limits within the VPNS, ETS, IPS, SDWANS and AA services.
    e. Update Figure 1 within C.2.8.4.1.1.1 MTIPS Context Architecture to match the EIS service guide.
    f. Update SDWANS to remove IPSec tunnel and specific UNI requirements,

2. The contract is modified as follows:

TABLE OF CONTENTS: Section pages renumbered.

Section B:

1. Section B.1.2.1.1 Pricing Identification Structure is changed to add Broadband Internet Service to the Data Service Area.

Service Area	Service Name	Mandatory/ Optional (M/O)	Service ID	Service CLIN Prefix	Section C Reference	Section B Reference	CBSA Based Service*
Data Service	Broadband Internet Service	O	BIS	BI	C.2.1.8	B.2.1.8	Yes (One-sided)

2. Section B.2.1.7.3.1 IPS Port Prices Table is changed to update the following footnote for consistency throughout Section B: "** Country/Jurisdiction IDs are provided in Section B.4.2.1"

3. Section B.2.1.8 Broadband Internet Service (BIS) is added to the contract.

B.2.1.8 Broadband Internet Service (BIS)

The technical requirements for Broadband Internet Service (BIS) are defined in Section C.2.1.8.

B.2.1.8.1 BIS Price Structure

The price structure for domestic and non-domestic BIS includes the following elements:

1. NRC
2. MRC
3. Feature Charges

B.2.1.8.2 BIS Access

All BIS ports shall include embedded access; the access prices shall be included in the BIS port NRC and MRC.

The access component shall equal or exceed the download bandwidth of the port with which it is embedded.

B.2.1.8.3 BIS Port Prices

Table **Error! Reference source not found.** provides the format for pricing BIS ports. Table **Error! Reference source not found.** provides the pricing mechanisms and charging units.

BIS port CLINs shall be priced as ICB. All ICB case descriptions shall include the BIS access download and minimum upload bandwidths, port speed, and service location.

B.2.1.8.3.1 BIS Port Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.8.3.2 BIS Port Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
BI10001	NRC	BIS – Port with Embedded Access	Port	ICB
BI10002	MRC	BIS – Port with Embedded Access	Port	ICB

B.2.1.8.4 BIS Feature Prices

BIS feature CLINs shall be priced as ICB. Table B.2.1.8.4.1 provides the format for pricing the features supported by BIS. Table **Error! Reference source not found.** provides the pricing mechanisms and charging units.

B.2.1.8.4.1 BIS Feature Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.8.4.2 BIS Feature Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
BI90001	MRC	BIS Enhanced Class of Service (CoS)	Port	ICB, Optional
BI90002	MRC	Static IP Address	Address Block	ICB, Optional

B.2.1.8.5 BIS Task Order Unique CLINs

Table **Error! Reference source not found.** provides the format for pricing the TUCs supported by BIS. Table **Error! Reference source not found.** provides pricing instructions. TUCs shall be used as defined in Section **Error! Reference source not found.**.

B.2.1.8.5.1 BIS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.8.5.2 BIS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
BI99990	BI99991	BI99992	BIS Task Order Unique	ICB	ICB

---

4. Section B.2.8.5 Managed Security Service is changed to add the following item: "4. Trusted Internet Connections Service"

5. Section B.2.8.5.4 Managed Security Service Category Reference Table is changed to add the following item:

Category	Category Description
4	Trusted Internet Connections Service (TICS)

Section C:

6. Section C.1.8.1 Organization of EIS Services is changed to add the following services:
- "Broadband Internet Service" under Data Service
- "Software Defined Wide Area Network Service" under Managed Services

7. Section C.1.8.7.1 System Security Compliance Requirements is changed to add:
- "• FIPS PUB 140-3, "Security Requirements for Cryptographic Modules." Dated March 2019."

8. Section C.1.8.7.6 Additional Security Requirements is changed to add the following to table under ID number 1 within the Description: "& 140-3"

9. Section C.1.8.8 National Policy Requirements is changed to replace number 2 with the following: "2. OMB Memorandum M-21-07 directs that agencies must transition from IPv4 agency infrastructures to IPv6 agency infrastructures (network backbones). For

agencies with an IPv6 network (and those implementing IPv6 networks) the contractor solution must maintain functionality and shall comply with relevant policies and standards defined by OMB and NIST SP 500-267. All systems, software, and equipment supporting the agency network and its services shall handle IPv6 in an equivalent or more efficient method than IPv4 capabilities, performance, and security. No systems, software, or equipment shall be deployed on the network that does not meet this requirement. Additionally, all network management shall be enabled using IPv6."

10. Section C.1.8.8 National Policy Requirements is changed to remove an extra space at the start of number 3.

11. Section C.2.1.1.2 Features is changed to add the following under ID Number 3 Description: "/3" and remove ", 197"

12. Section C.2.1.1.3 Interfaces are changed as follows:

- Network-Side Interface limit updates
    - 1 – Add "or higher"
    - 4 – delete previous text and replace it with: "xDSL access at 1.5 Mbps download and above, and 384 Kbps and above upload"
    - 5 - delete previous text and replace it with: "25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)"
    - 6 - 2. LTE - add "and future evolutions"

13. Section C.2.1.2.1 Service Description is changed to add "or higher" to the following sentence in the second paragraph: "Ethernet Transport Service (ETS) allows agencies to interconnect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 **or higher** Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN) regardless of the geographical location of their sites."

14. Section C.2.1.2.1.2 Standards was updated to reflect the updated MEF standards listed in the section.

- 1. Updated MEF CE 2.0 to 3.0
- 1b. Updated CE 2.0 to 3.0 and MEF CE 2.0 to 3.0
- 1c. Updated MEF 6.1 to 6.3 and added the 6.3 "Subscriber Ethernet" title addition
- 1c Updated MEF 10.2 to 10.4 and added the 10.4 "Subscriber Ethernet Service Attributes" title addition while removing the previous title for 10.2 "CE Service Attributes".
- 1c Updated MEF 23.1 to 23.2 and added the 23.2 title to "Carrier Ethernet Class of Service - Phase 3" addition
- 1c Updated MEF 26.1 to 26.2 and added the 26.2 "and Operator Service Attributes" title addition
- 1d updated CE 2.0 to 3.0
- 1d updated the following MEF standards – MEF 6.1 to 6.3, MEF 10.2 to 10.4, MEF 23.1 to 23.2, MEF 10.2 to 10.4 (again), MEF 26.1 to 26.2, MEF 7.1 to 7.3, and MEF 30 to 30.1

15. Section C.2.1.2.1.4 Technical Capabilities is changed to remove "– up to 40 Gbps" limits from the following:

    25. The contractor shall support the following Virtual Connection sizes:
    a) For point-to-point Ethernet connections

b) For multi-point-to-multi-point connections

16. Section C.2.1.7 Internet Protocol Service is changed from “TCP/IP” to “IP.”

17. Section C.2.1.7.3 Interfaces - Network-Side Interface descriptions are changed to remove the limits as follows:
    a. 1 - Replace text with "25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)"
    b. 2 - Add text "and above" after 2. 10 GbE
    c. 5 - Replace text with: "xDSL access at 1.5 download and above, and 384 Kbps upload and above"
    d. 6 - Remove "to 150 Mbps" and add "and above"
    e. 7 - Add "and future evolutions" after 1. LTE

18. Section C.2.1.8 Broadband Internet Service (BIS) is added to the contract.

C.2.1.8 Broadband Internet Service

The government uses Broadband Internet Service (BIS) to support a wide range of connectivity requirements. BIS will use the IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

Use cases for BIS include supporting SD-WAN service as an underlay, potential direct connections to Cloud Service Providers, low cost network connectivity to Agency networks, Wi-Fi backhaul for public facing agencies customers and guests, and services for geographic areas where other network transport services are limited or non-existent.

C.2.1.8.1 Service Description

Broadband Internet Service provides high-speed Internet access that is always on. Broadband Internet Service includes several high-speed transmission technologies such as those listed in Section C.2.1.8.3.

C.2.1.8.1.1 Functional Description

BIS provides transport of Internet Protocol (IP) packets.

C.2.1.8.1.2 Standards

BIS shall comply with Federal Standards listed in Section C.1.8 as they apply to the service.

C.2.1.8.1.3 Connectivity

BIS shall connect:

1. Government locations, including mobile and remote users, (i.e., SDP devices such as customer routers, switches, and firewalls) to the Internet.
2. A wide range of equipment (such as notebook PCs, Mobile devices, etc.) via appropriate combinations of EIS services to the Internet.
3. Government locations to other networks, including those of other EIS contractors.
4. Non-Government locations, including Partners, Local Exchange Carriers (LECs), Collaborators (educational activities such as Universities).

C.2.1.8.1.4 Technical Capabilities

The following BIS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section **Error! Reference source not found.**.
2. All BIS port access components shall equal or exceed the download bandwidth of the port with which it is embedded.
3. The contractor shall include appropriate embedded asymmetric or symmetric access services (such as high speed access over copper or fiber optic cable, DSL, wireless or satellite) to connect customer SDPs to the contractor's BIS as part of the service. Separately priced Access Arrangements are not required for BIS.
4. The contractor shall not impose a limit or throttle on the data downloaded or uploaded during the billing period.
5. The contractor's network shall have:
    a) Established public peering arrangements from the contractor's network to the Internet.
    b) Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.
    c) Support for the government-assigned and InterNIC-registered IP addresses and domain names.
    d) Primary and Secondary Domain Name Service (DNS) to provide an authoritative name server for the customer.
    e) Albility to designate dynamic or fixed IP addresses for customer equipment.

C.2.1.8.2 Features

The listed BIS features are optional.

ID Number	Name of Feature	Description
1	BIS Enhanced Class of Service (CoS) (Optional)	The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. Some providers of BIS may not be able to provide CoS as part of the standard BIS service without additional SRE. The Classes of Service or prioritization levels may be categorized as shown in the examples below: 1. Enhanced ─ for business-critical traffic such as transactions, and SD-WAN control/data plane communications
2	Static IP Address (Optional)	The contractor shall provide static IPv4/IPv6 addresses with the BIS service.

C.2.1.8.3 Interfaces

These UNIs at the SDP for the provisioning of BIS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1	Cable Access	25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)	IPv4/v6
2	Ethernet Interface	10 Mbps and above (sub-interfaces of lesser capacity shall be made available to meet customer requests where feasible)	IPv4/v6 over Ethernet

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
3 (Optional)	DSL Service	xDSL access from 25 Mbps and above download, and from 5 Mbps and above upload	Point-to-Point Protocol, IPv4/v6
4 (Optional)	FTTP	25 Mbps and above	IPv4/v6
5	Fixed Wireless Access	1. LTE 2. 5G and future evolutions 3. 802.11x 4. Satellite (optional)	IPv4/v6

C.2.1.8.4 Performance Metrics

The performance levels (KPIs) for BIS are mandatory and are as follows:

Broadband Internet Service Performance Metrics:

- Availability (Port): Best effort

KPI	Service Level	Performance Standard (Threshold)	How Measured
Time to Restore (TTR)	Without Dispatch	24 hours	See Note 1
	With Dispatch	48 hours	

Notes:

1. See Section G.8.2 for the definitions and measurement guidelines.

---

19. Section C.2.5.1.1.2 Standards is changed to add the following item:
"8. FIPS 140-3, Security Requirements for Cryptographic Modules"

20. Section C.2.6.1.2 Standards is changed to add "/3" to 5. 3G Security b) NIST FIPS Publication 140-2/3

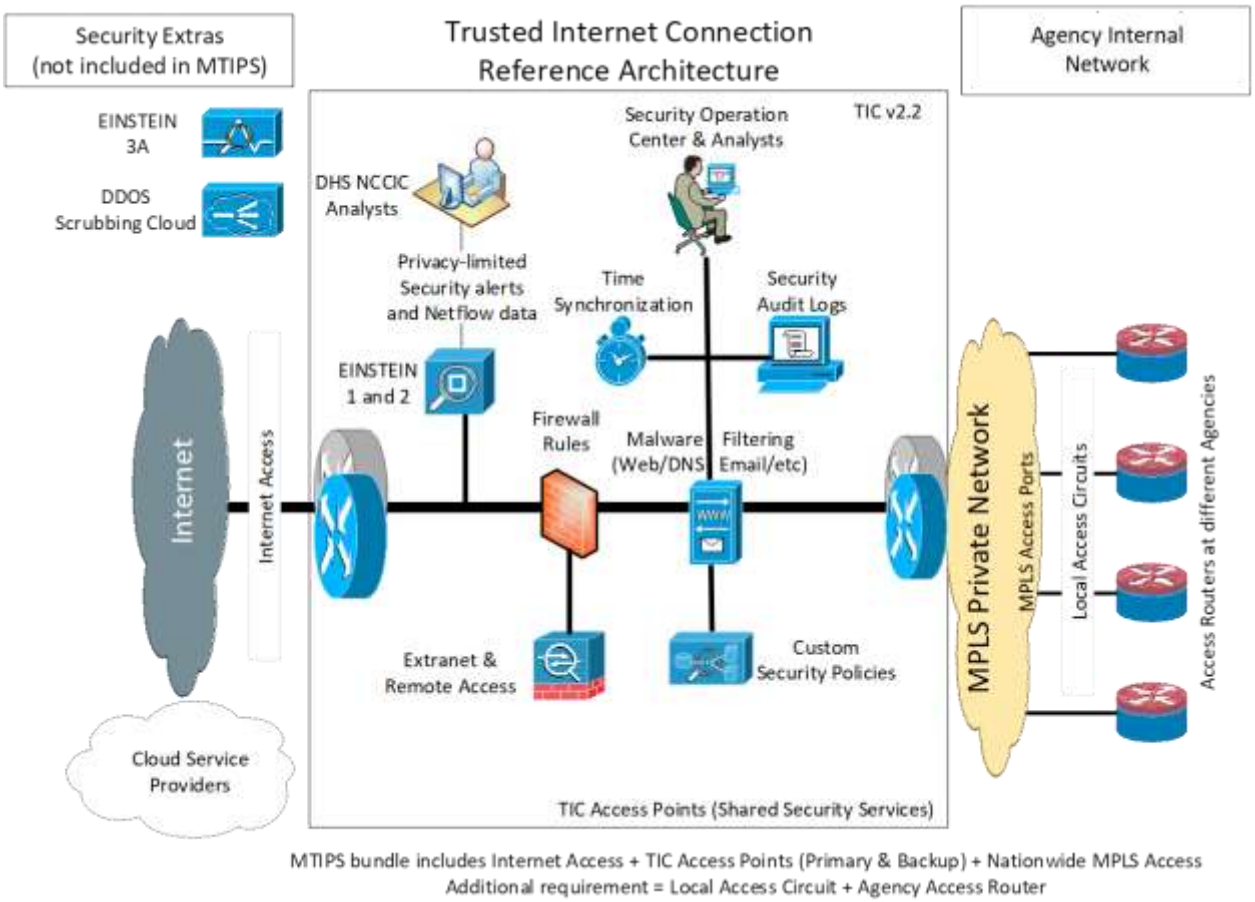
21. Section C.2.8.4.1 Service Description is changed to switch a word in the following sentence from integral to integrated.
"MTIPS enables the government to react more effectively to cyber security attacks thus reducing malicious penetrations and theft of critical data. Exchange of information

through the TIC Portal is closely monitored by an **integrated** MTIPS Security Operations Center (SOC) to protect agency IP traffic."

22. Section C.2.8.4.1.1 Functional Definition is changed to remove the following sentence: "The TIC Portal Security Operations Center Architecture is defined in Figure C.2.8.4.1.1.2."

23. Section C.2.8.4.1.1.1 MTIPS Context Architecture is changed to add the following caption and diagram. The diagram is from the EIS MTIPS Service Guide.

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.*



24. Section C.2.8.4.1.4.1 TIC Portal Capabilities is changed to remove the highlight around "4. Reserved."

25. Section C.2.8.4.2 Features is changed as follows:

- Add "/3" to 7. c) after FIPS 140-2 to highlight that both publications now apply.
- Add "/3" to 8. after FIPS 140-2 to highlight that both publications now apply.
- Add "/3" to 9. c) after FIPS 140-2 to highlight that both publications now apply.

- Add "/3" to 9. i) ii. after FIPS 140-2 to highlight that both publications now apply.
- Add "/3" to 10. c) after FIPS 140-2 to highlight that both publications now apply.
- 10. d) – Update the first sentence regarding split tunneling for Extranet Connections: "d) Split tunneling shall not be allowed unless directed otherwise from the ordering agency. (Agencies may authorize split tunneling in support of branch office and remote user solutions.) Any VPN connection that allows split tunneling is considered an external connection, and must terminate prior to routing through the EINSTEIN Enclave."
- 11. – Update US-CERT to “the CISA Incident Reporting System”

26. Section C.2.8.4.4.2 Performance Metrics for MTIPS Transport Collection and Distribution Note #4 was changed to update DHS US-CERT to "the CISA Incident Reporting System"

27. Section C.2.8.4.5.1 General Security Compliance Requirements is changed to add "• FIPS PUB 140-3, “Security Requirements for Cryptographic Modules”"

28. Section C.2.8.4.5.5 Additional Security Requirements is changed to add "/3" after FIPS 140-2 to highlight that both publications now apply

---

Changes to C.2.8.5 Managed Security Service to add the Trusted Internet Connections Service

29. Section C.2.8.5.1.1 Functional Definition is changed to add "4. Trusted Internet Connections Service"

Trusted Internet Connections Service (TICS) provides a networking and cybersecurity solution meeting the guidance provided by OMB and the Cybersecurity and Infrastructure Agency (CISA) for the TIC program. The OMB M-19-26 memorandum supersedes previous TIC guidance and provides an enhanced approach for implementing the TIC initiative while providing agencies with increased flexibility to use modern connectivity and data security capabilities. The memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats. As a result agencies have been given more autonomy to decide how they can provide their workforce access to applications, data, and Internet access within their enterprises regardless of location. Although TICS solutions are to remain coordinated with the CISA NCPS and CDM programs, neither GSA nor CISA will be issuing formal authorization stating a TICS solution is compliant with OMB M-19-26 and the CISA TIC program office guidance. TICS solutions leveraged by an agency are to follow and comply with the customer agency specific Assessment and Authorization (A&A) processes while adhering to the CISA program guidance and other required National Policy Requirements in C.1.8.8.

CISA has issued Trusted Internet Connections 3.0 guidance to include a Program Guidebook, Reference Architecture, Security Capabilities Catalog, a Use Case Handbook, and an Overlay Handbook. The guidance and use case documents are living documents and will evolve as the related landscape changes.

The MSS TIC Service within the EIS contract relies on the CISA TIC program guidance documents. TICS solutions under this service shall adhere to the CISA guidance.

MSS TICS Solutions for the Cloud, Agency Branch Office, and Remote Users Initial Common TIC Use Cases listed in OMB M-19-26 may be constructed in a number of ways under EIS. Leveraging the SDWANS, MSS, MNS, SaaS, BIS, and other EIS services while following the CISA TIC guidance will produce a safe, flexible, and repeatable TICS solution for the agency which address the TIC 3.0 Security objectives listed below.

For the TIC 3.0 Traditional TIC use case, MTIPS based on the previous TIC 2.2 guidance may be proposed in combination with other Managed Security Services (MSS), Software as a Service (SaaS), Managed Network Services (MNS), or other EIS services to fill in any security capability gaps between a TIC 2.2 and a TIC 3.0 solution.

Objective	**Description**
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures

30. Section C.2.8.5.1.2 Standards is changed as follows:
- Add "3. NIST FIPS PUB 140-3 – Security Requirements for Cryptographic Modules"
- Update 17. “United States Computer Emergency Readiness Team (US-CERT)” to “CISA Incident Reporting System”

31. Section C.2.8.5.1.4.4 Trusted Internet Connections Service (TICS) is added to Section C.

1. The contractor shall provide TICS solutions that adhere to the current DHS CISA Trusted Internet Connections (TIC) guidance.
2. The contractor shall ensure their TICS solutions adhere to the Key Concepts of TIC 3.0 and the Conceptual Implementation of TIC 3.0 listed in the CISA Trusted Internet Connection Reference Architecture (Volume 2) guidance.

3. The contractor shall ensure their TICS solutions contain the required Security Objectives and Security Capabilities listed in the CISA Trusted Internet Connections Security Capabilities Catalog (Volume 3) guidance.

    a. TICS solutions shall include the defined Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.

    b. TICS solutions shall include the defined Policy Enforcement Point Security Capabilities: Network-level capabilities that inform technical implementation for relevant TIC use cases.

4. The contractor shall reference the CISA TIC Use Case Handbook (Volume 4) TIC 3.0 Use Case Structure when designing and providing a TICS solution to the EIS customer. The Use Case Handbook outlines alternative security controls, such as endpoint and user-based policy enforcment point protections, that must be in place for specific instances where traffic is not required to flow through a traditional TIC 2.2 access point (i.e. TICAP or MTIPS).

5. The contractor shall reference the CISA TIC Overlay Handbook (Volume 5) guidance when constructing and proposing TICS solutions for the ordering agency customer. The Overlay Structure is a high level mapping of a contractor's proposed TICS solution to the list of deployable security controls, security capabilities, and best practices within the Security Capabilities Catalog (Volume 3) of the CISA TIC Core Guidance. The Overlay will assist agency customers with identifying any gaps in the proposed TICS solution as it maps to the Security Objectives and Security Capabilities from the CISA TIC Core and Use Case Guidance documentation. Some proposed TICS solutions may not align with all the recommended TIC security capabilities for the intended use case, and agencies may need to obtain additional Managed Security Services from the EIS provider or other third-party providers to secure their environments to the use case specifications and their agency specific requirements.

6. The contractor proposed TICS solutions shall integrate with and support the CISA NCPS and CDM program requirements as required by the agency customer. Consult the NCPS Program and CDM Program references for further details.

32. Section C.2.8.5.2 Features in Section C was added to for the addition of the TICS sub-service.

4. Trusted Internet Connections Service (TICS)

    a) Encrypted Traffic: The TICS solution shall monitor, scan and filter the incoming and outgoing encrypted traffic traversing agency Web Security Capabilities Policy Enforcement Points based on URL or IP address. The TICS solution shall analyze all encrypted traffic that passes through the Web Security Capabilities PEP for suspicious patterns that might indicate malicious activity and shall retain the logs of at least the source, destination and size of the encrypted connections for further analysis. Log retention time frames shall be specified within the agency requirements.

b) Agency Security Policy Enforcement: The contractor shall adhere to and support the ordering agency's security policy to ensure security regulations compliance. The contractor shall support agency's operational models and specific security rules. These shall be negotiated between the agency and the contractor. The contractor shall support adjustments to the agency's security strategy based on threats identified. For example, adjustments to the security policy could be made by the agency's authorities after the SOC identifies changing trends in intrusion behavior.

c) Forensic Analysis: The contractor shall support capturing and logging of traffic flows and shall support subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). The agency shall identify technical requirements such as, but not limited to traffic of interest (relevant traffic to capture/log) and the data retention timelines required.

d) Custom Reports: The contractor shall provide reports as required by the ordering agency, including ad-hoc reports.

e) CISA NCPS Program Protections – At the appropriate TICS Policy Enforcement Points the contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring encrypted connections are applied between agency Service Delivery Points, TICS aggregation points, and Policy Enforcement Points and the required data from the NCPS program is trasmitted to CISA for NCPS program data collection and inspection (i.e. to EINSTEIN, the Cloud Log Aggregation Warehouse (CLAW), etc.).

f) Custom Security Assessment and Authorization (A&A) Support (formerly known as Certification & Accreditation (C&A)): Agencies will specify agency-unique requirements and support required for A&A activities directly with the contractor.

g) External Network Connections: The contractor shall enable the agency to connect to external IP networks. The traffic exchanged shall be compliant with customer agency interconnecting requirements. The TICS solution shall support dedicated external connections to external partners (e.g., cloud service providers, 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, ad-hoc or permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities shall be supported for external dedicated and private connections implemented using communication services offered through this contract, i.e. ETS, IPS, VPNS, BIS, CHS, PLS, SDWANS, etc or other dedicated connections at the TICS solution location(s)::

    1. The connection shall terminate at an appropriate point so that traffic can be routed through the required Policy Enforcement Points to allow traffic to/from the external connections to be inspected. The incoming traffic from the external network shall be inspected within the Policy Enforcement Points before reaching the internal network while ensuring compliance with CISA NCPS program requirements.
    2. When connecting over the public networks including the Internet, the connections shall be encrypted, compliant to NIST FIPS 140-2/3.

3. Connections terminated prior to routing through the Policy Enforcement Point (PEP) may use split tunneling, while ensuring compliance with CISA NCPS requirements.
4. The External Network Connection Feature is subject to performance measures established by EIS depending on the transport service selected for connectivity and included in Sections C and Section J.

h) The contractor shall support FIPS 140-2/3 compliant encryption within their TICS solutions. The contractor shall provide the encryption capability and shall manage the capability where required by the customer.

i) (OPTIONAL) Remote Access: The TICS solution shall support 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 staff that connects through external connections, including the Internet. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities shall be supported for telework/remote access at the TICS solution policy enforcement points:

1. The connection shall terminate at an appropriate point prior to routing through the TICS Policy Enforcement Points (PEPs) so that all outbound traffic to/from the external connections, including the Internet, can be inspected within the TICS Policy Enforcement Points while ensuring compliance with CISA NCPS program requirements.
2. The external or remote connection shall terminate in front of TICS Policy Enforcement Point 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. All external or remote connections shall be NIST FIPS 140-2/3 compliant.
4. The VPN or remote connection shall not be capable of split tunneling (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of the Policy Enforcement Point (PEP) for inspection while also ensuring CISA NCPS program complaince.
5. The contractor shall use multi-factor authentication (see NIST SP 800-46 Rev1).
6. VPN concentrators and Virtual-Desktop/Application Gateways (Remote Access Enclave) shall use hardened appliances and shall be maintained in a separate network security boundary depending on the contractor's implementation.
7. Implementation requirements:
    i. The contractor shall support TLS and/or IPSec VPNs or remote connections to connect to the TICS solutions where applicable. The contractor shall provide the end device client (agent) if required by the agency.
    ii. The contractor shall provide a VPN or remote connection Encryption Algorithm compliant to FIPS 140-2/3.

iii. Multi-factor authentication services shall be supported and issued in accordance to the NIST SP 800-63 Digital Identity Guidelines and agency specific requirements.
iv. The contractor shall also support customized remote access implementations for teleworkers and mobile workers to meet agency-specific requirements.

j) Extranet Connections: The TICS solution shall support dedicated extranet connections to internal partners (e.g., partner 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 connections to other internal networks provided by communication services offered through this contract. The following baseline capabilities shall be supported for extranet dedicated connection, other tunneled traffic, and private line connections:
    1. The connection shall terminate at an appropriate point before routing through the full suite of TICS Policy Enforcement Point (PEP) sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including Internet transport, is inspected within the Policy Enforcement Point while ensuring compliance with CISA NCPS program requirements.
    2. The connection shall terminate in front of the TICS policy enforcement point(s) to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected.
    3. Extranet connections over shared public networks, including the Internet shall be NIST FIPS 140-2/3 compliant.
    4. Split tunneling shall not be allowed, unless there is direction received from the agency customer to support split tunneling.
    5. Implementation requirements:
        i. VPN from the fixed remote location (business partners, remote agency's sites, other agencies' sites, etc.) to the TICS policy enforcement points.
        ii. Multi-Factor Authentication: Passwords, Cryptographic Tokens or PIV shall be supported.
        iii. The contractor shall also support customized remote access implementations for extranet connections to meet agency-specific requirements.

k) Additional EIS services shall be proposed to fill any CISA TIC 3.0 Security Capabilities Catalog (Volume 3) gaps to the customer requirements for a particular agency requested TICS use case. The CISA Overlay Guidance (Volume 5) will aid the contractor in identifying the Security Capabilities Catalog gaps were additional EIS services may be required.

33. Section C.2.8.5.3 Interfaces is changed to add:
    4. BIS as specified in Section C.2.1.8

5. SDWANS as specified in Section C.2.8.10

34. Section C.2.8.5.4.1 Managed Security Service Performance Metrics is updated to add the following:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (Port) for TICS	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS) for TICS	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate) for TICS	Routine	99.95%	≥ 99.95%	See Note 3
	Critical	99.995%	≥ 99.995%	
Event Notification (EN) Security Incident Reporting for TICS	Routine	Near real time	≤ 30 min	See Note 4

Notes:

2. TICS 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. The TICS Port availability metric does not apply for DSL and Cable High Speed (i.e. Broadband Internet Service (BIS)) access methods. Availability is computed by the standard formula:

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

3. Latency is the average one-way time for IP packets to travel over the EIS core network. The Backbone Latency metric does not apply for DSL and Cable High Speed (i.e. Broadband Internet Service (BIS)) access methods.

4. Security incident reporting to the CISA Incident Reporting System must be performed in near real-time, congruent with NIST SP 800-61 Rev 2, not to exceed 30 minutes, from the time of confirmed incident detection.

9. Time to Restore (TTR) for MSS solutions leveraging the Broadband Internet Service (BIS) will default to the BIS TTR Performance Metrics in Section C.2.1.8.4 for the components leveraging BIS.

- Renumbered the Notes: list in Section C.2.8.5.4.1 to accommodate the added Performance Metrics
  - The former Notes: numbered 2. – 5. are now 5. – 8.
- On the last KPI in the table, Time to Restore (TTR), “See Note 9” was added to the How Measured column.

35. Section C.2.8.6.1.2 Standards is changed to add "/3" after 3. FIPS 140-2

36. Section C.2.8.6.1.4.4 Mobile Security is changed to add "/3" in 15. Encrypt the data in transit between the MDM and the device in accordance with FIPS 140-2/3

37. Section C.2.8.9.1.2 Standards is changed to update "US-CERT" to "CISA Incident Reporting System"

38. Section C.2.8.9.1.3 Connectivity is changed to update "DHS US-CERT" to "CISA Incident Reporting System"

39. Section C.2.8.9.1.4 Technical Capabilities is changed to update the following:

- Update the DHS CISA organization in 18. Apply DHS-directed prevention services, as defined and approved by the Cybersecurity and Infrastructure Security Agency's Cybersecurity Division.
- Update the DHS CISA lab in 22. Provide quarantined malware to Participating Agency and to DHS via the CISA Threat Hunting malware lab or other specified DHS entity.

40. Section C.2.8.10 – removed "and commercial broadband Internet" from the end of paragraph 2.

41. Section C.2.8.10.1 Service Description - removed "commercial broadband Internet" and added "BIS".

42. Section C.2.8.10.1.1 Functional Description is changed to update the following:
Update the SDWANS where noted to allow for non-IPSec FIPS 140-2/3 encrypted tunnels rather than requiring IPSec. Added "/3" after FIPS 140-2 to highlight that both publications now apply.

- "1. A secure IP-based virtual overlay network over physical IP networks (underlays) using an encrypted connection, compliant with the FIPS 140-2/3 standard for approved cryptographic modules."
- "3. Quality-of-Service (QoS) assurance of each FIPS 140-2/3 compliant encrypted connection is to be measured in real-time on key parameters (latency, packet loss, and jitter) to ensure that the performance level specified is being achieved."

43. Section C.2.8.10.1.1 Functional Description – Item 2 removed "commercial broadband Internet" and added "BIS".

44. Section C.2.8.10.1.2 Standards:
2. Updated MEF CE 2.0 to 3.0

45. Section C.2.8.10.1.3 Connectivity – Item 2 removed “commercial broadband Internet” and added “BIS”.

46. Section C.2.8.10.1.4 Technical Capabilities is changed as follows:
Update the SDWANS where noted to allow for non-IPSec FIPS 140-2/3 encrypted tunnels rather than requiring IPSec. Added "/3" after FIPS 140-2 to highlight that both publications now apply.

- "2. a. SD-WAN shall provide a secure IP-based virtual overlay network that uses FIPS 140-2/3 compliant encrypted connection through one or more underlay networks. For additional security, the FIPS 140-2/3 compliant encrypted connection shall support Agency-provided end-to-end encrypted traffic."
- "2. c. End-to-end secure FIPS 140-2/3 compliant encrypted connection shall also include Access Arrangements that connect Agency sites (SDPs) to their respective underlay physical network POPs."

47. Section C.2.8.10.1.4 Technical Capabilities – Item #1 and Item 2 B removed "commercial broadband Internet service and" and added "BIS, "

48. Section C.2.8.10.3 Interfaces is changed as follows”

- Update the sentence to state that the following UNIs may be leveraged vs required to connect. Also replace commercial broadband internet with BIS references. Remove the mandatory language and make it all optional.
    - "The following UNIs at the SDP may be leveraged to connect the uCPE (e.g. virtualized edge router) to multiple underlays (e.g. BIS, IPS, VPNS and ETS services) with access arrangements to their respective POPs for the provisioning of SDWANS."
- Update "Network-Side Interface" table descriptions to remove limits
    - 1 – replace text with "25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)"
    - 2 – add text "and above" after 2. 10 GbE. Deleted “(Optional)”
    - 5 – remove limits and replace text as: "xDSL access at 1.5 Mbps download and above, and 384 Kbps upload and above"
    - 6 - remove "to 300" and added "and above"
    - 7 - add "and future evolutions" after 2. 5G

49. Section C.2.8.10.4 Performance Metrics is changed as follows:

- Replace 2. d. to remove Commercial Broadband Internet Performance Metrics and reference the added Broadband Internet Service.
    - "d. For BIS, see Section C.2.1.8.4 BIS Performance Metrics"

50. Section C.2.9.1.4 Technical Capabilities is changed as follows:

- 15. d) add "and above"

- 17. a) 1, 2 and 3. Update “upstream” to “upload” and “downstream” to “download” for consistency across the services in the contract.
- 18. a) 5. add "and above"
- 19. a) update to state "a) Provide data rates of 25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)"
- 20. a) update to state "a) 25 Mbps (download) and 5 Mbps (upload) and above"
- 21. a) update to state "a) Cellular Service - 4G Long Term Evolution (LTE) and future evolutions:
    1. 100 mbps (download), 50 mbps (upload) and above

SECTION G

Tables of Content Updates

51. Section G.4.4, last paragraph, is changed to delete the sentence reading: “The government will accept and process the contractor's disputes.”

52. Section G.8.2.1.1.1 is changed to insert a new row after Internet Protocol Service with the following values:

· Service = Broadband Internet Service

· Service ID = BIS

· Section C Reference = C.2.1.8.4

53. Section G.8.2.1.2.1 to insert a new row after Internet Protocol Service with the following values:

· Service = Broadband Internet Service

· Service ID = BIS

· Section C Reference = C.2.1.8.4

54. Section G.8.2.2.2.1 Services Subject to ICB Provisioning Intervals is changed to insert a new bullet for Broadband Internet Service (BIS) after Internet Protocol Service (IPS).

---

3. The estimated dollar value of the contract remains unchanged.