



governmentattic.org

"Rummaging in the government's attic"

Description of document: Plan for modernization of the General Services Administration (GSA) information Technology Network, 2023

Requested date: 25-July-2023

Release date: 23-August-2023

Posted date: 08-April-2024

Source of document: FOIA Request
U.S. General Services Administration
FOIA Requester Service Center (LG)
1800 F Street, NW, 7308
Washington, DC 20405-0001
Fax: 202-501-2727
[FOIA Public Access Portal](#)
[FOIA.gov](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



August 23, 2023

This letter is in response to your U.S. General Services Administration (GSA) Freedom of Information Act (FOIA) request number GSA-2023-001689 which was perfected on July 25, 2023. You requested a copy of the current (2023) plan for modernization of the GSA IT network which is occurring now (summer 2023).

Enclosed please find the records responsive to your request.

We provided the presentation that describes the current GSA IT Network Modernization efforts. Due to the nature of the request, we referenced work in the Summer of 2023, relating to the Managed Trusted Internet Protocol Services (MTIPS) migration that took place in July 2023.

If you are not satisfied with our response to your request, you may file an administrative appeal online (<https://www.foiaonline.gov/foiaonline/action/public/home>) or in writing to the following address:

U.S. General Services Administration
FOIA Requester Service Center (LG)
1800 F Street, NW
Washington, DC 20405

Your appeal must be postmarked or electronically transmitted within 90 days of the date of the response to your request. In addition, your correspondence must contain a brief statement regarding the basis of your appeal. Please enclose a copy of your initial request and this response letter. Both the appeal letter and envelope or online appeal submission should be prominently marked, "Freedom of Information Act Appeal."

This completes our action on this FOIA request. You may contact the GSA FOIA Public Liaison, David Eby at (202) 213-2745 or by email at david.eby@gsa.gov for any additional assistance and to discuss any aspect of your FOIA request.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, email at ogis@nara.gov; telephone at (202) 741-5770; toll free at (877) 684-6448; or facsimile at (202) 741-5769.

Sincerely,

Amanda Jones

Amanda Jones
FOIA Program Manager
Senior Assistant General Counsel
Office of the General Counsel
General Services Administration

Enclosure(s)

Modernizing GSA's Network

June 2023



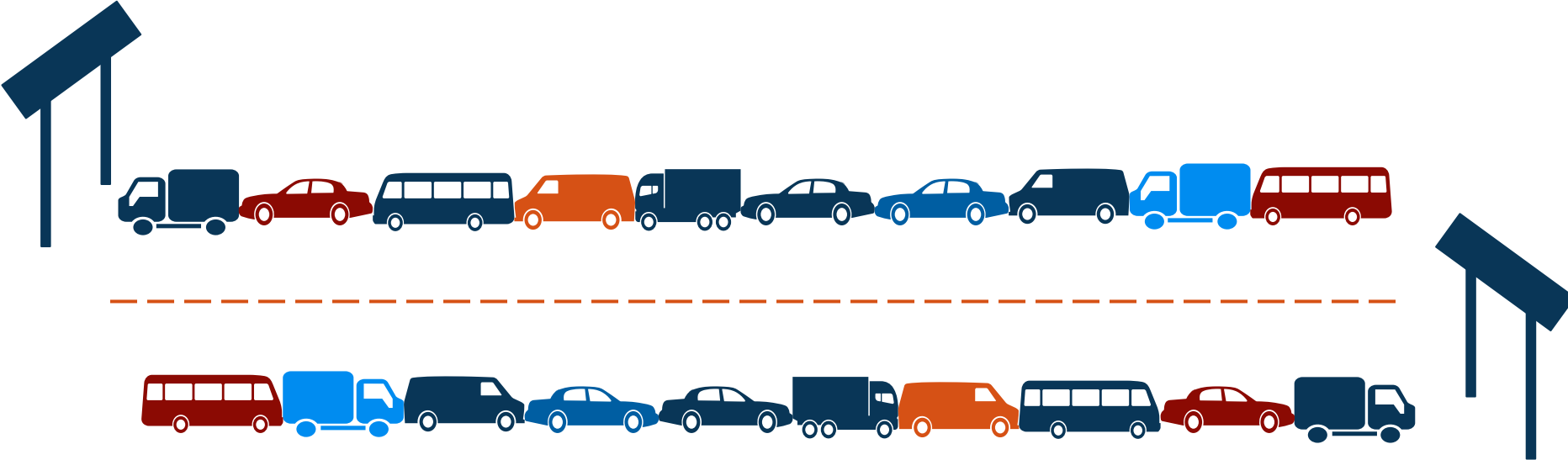
Modernizing GSA's Network

- ★ Moving off legacy infrastructure
- ★ Improving user experience
- ★ Incorporating security best practices

**All without
increasing costs**

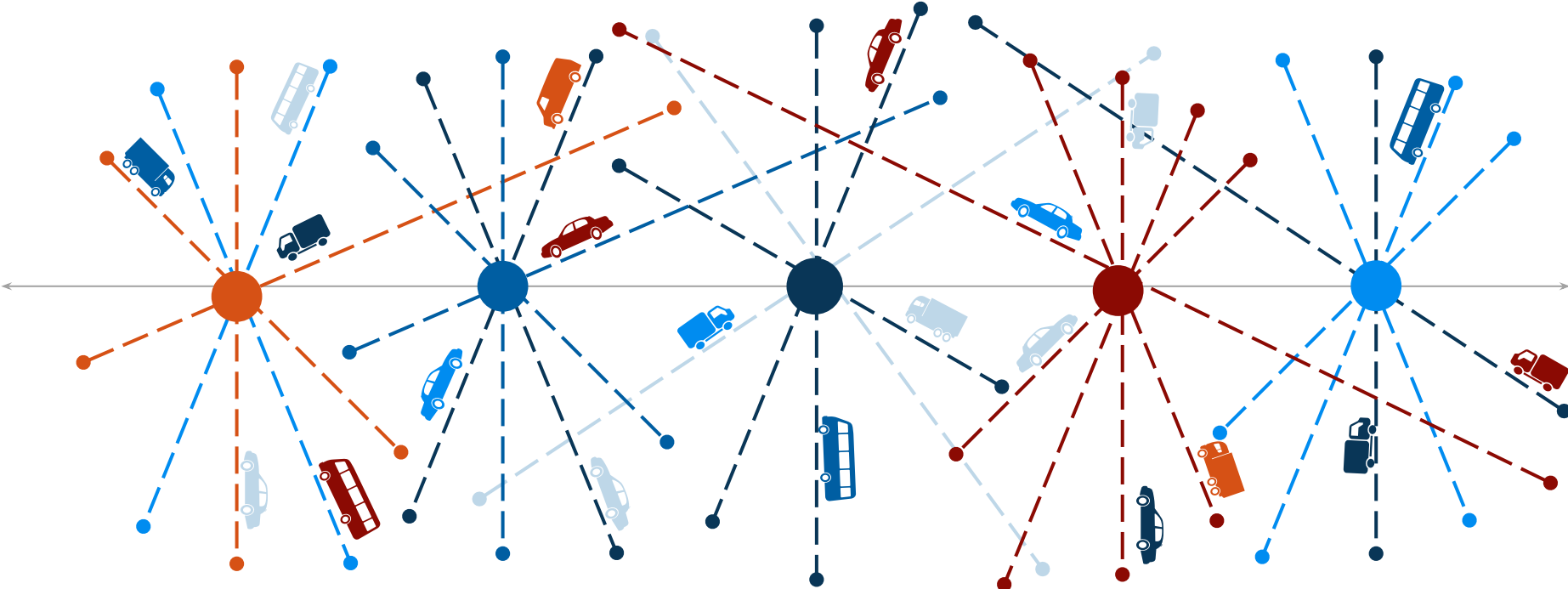
How our network currently works

Similar to a traffic bottleneck, security stack inspects network traffic



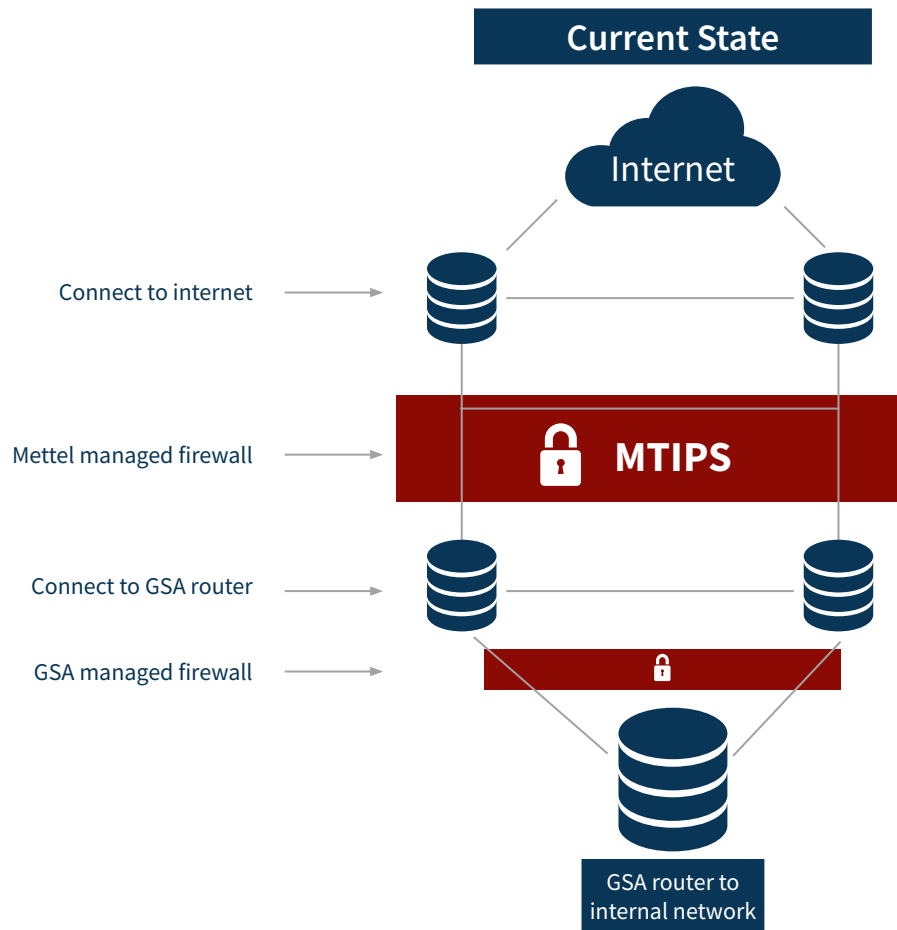
How our network will work

Distributed network allows direct internet access from every GSA site (no bottlenecks!)








Where we are today

- Today, we use a Managed Trusted Internet Protocol Service (**MTIPS**) layer that a user “passes through” to access internet/other IT apps & resources
 - MTIPS is offered through the Enterprise Infrastructure Solutions (EIS) contract
- MTIPS satisfied previous requirements for Trusted Internet Connections (TIC) program (TIC 2.2)






Problem vs. solution

Problems

-  Poor **UX** in field offices, for remote users
-  **Slow access** to internet, business apps
-  **Connectivity** restricted to physical data centers
-  **Costly, duplicative** remote access tech
-  **Old tech, need modernization** to support Zero Trust

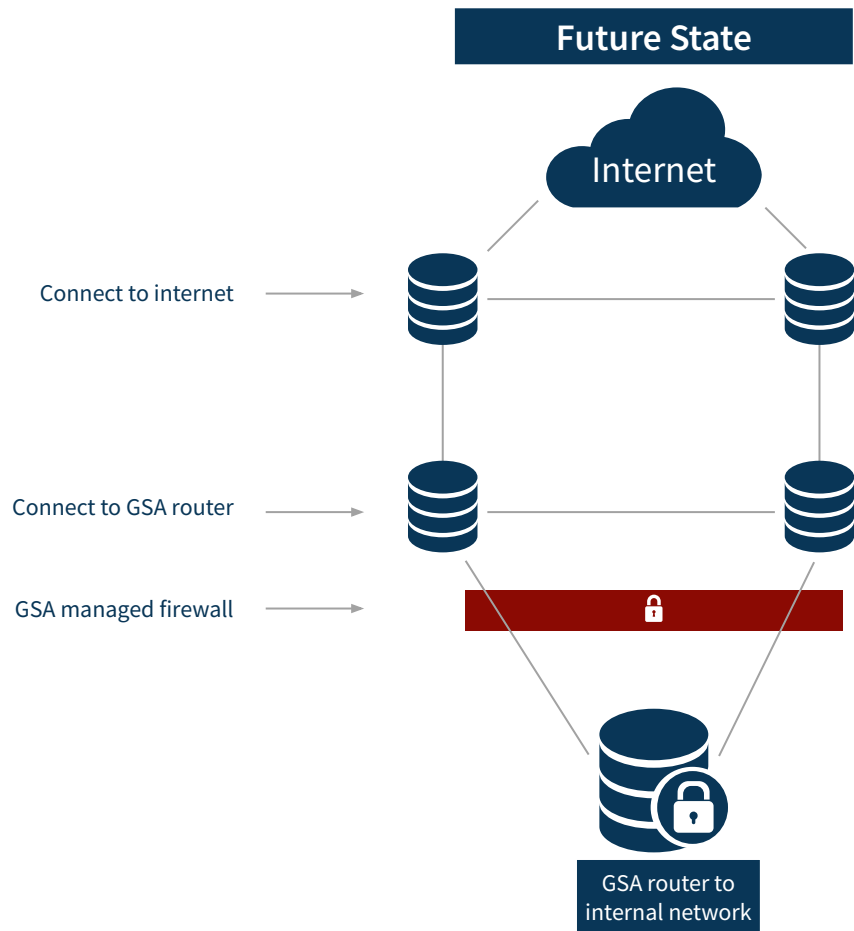
Solution

SECURE ACCESS SERVICE EDGE (SASE)

-  More of GSA infrastructure, business apps, & data **moving to cloud**
-  Employees expect **immediate, uninterrupted access**
-  **SASE** provides an emerging approach for network security

What's changing?

- OMB & CISA came out with **new guidance** ([OMB M-19-26](#), TIC 3.0)
 - Allow agencies to modernize networks & incorporate a **Zero Trust** Architecture
 - Focus on **how data is accessed** rather than focusing on a centralized security perimeter where all access must pass through
- **MTIPS layer will be removed**
 - Security baked in from the start - no longer a layer you “pass through”



Inputs & outputs

Planning the project



PLANNING PHASE

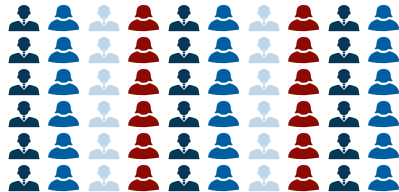
2022 - 2023



MIGRATION

August 2023

18,000 FTE Hours



Delivering customer benefits

\$1.5M



Yearly cost deferral

Applied to TMF payback & Zscaler

Security

Align w/ Zero Trust initiatives

& OMB/CISA guidelines



Fewer Mods

Reduces # of EIS contract modifications

Reuse resources

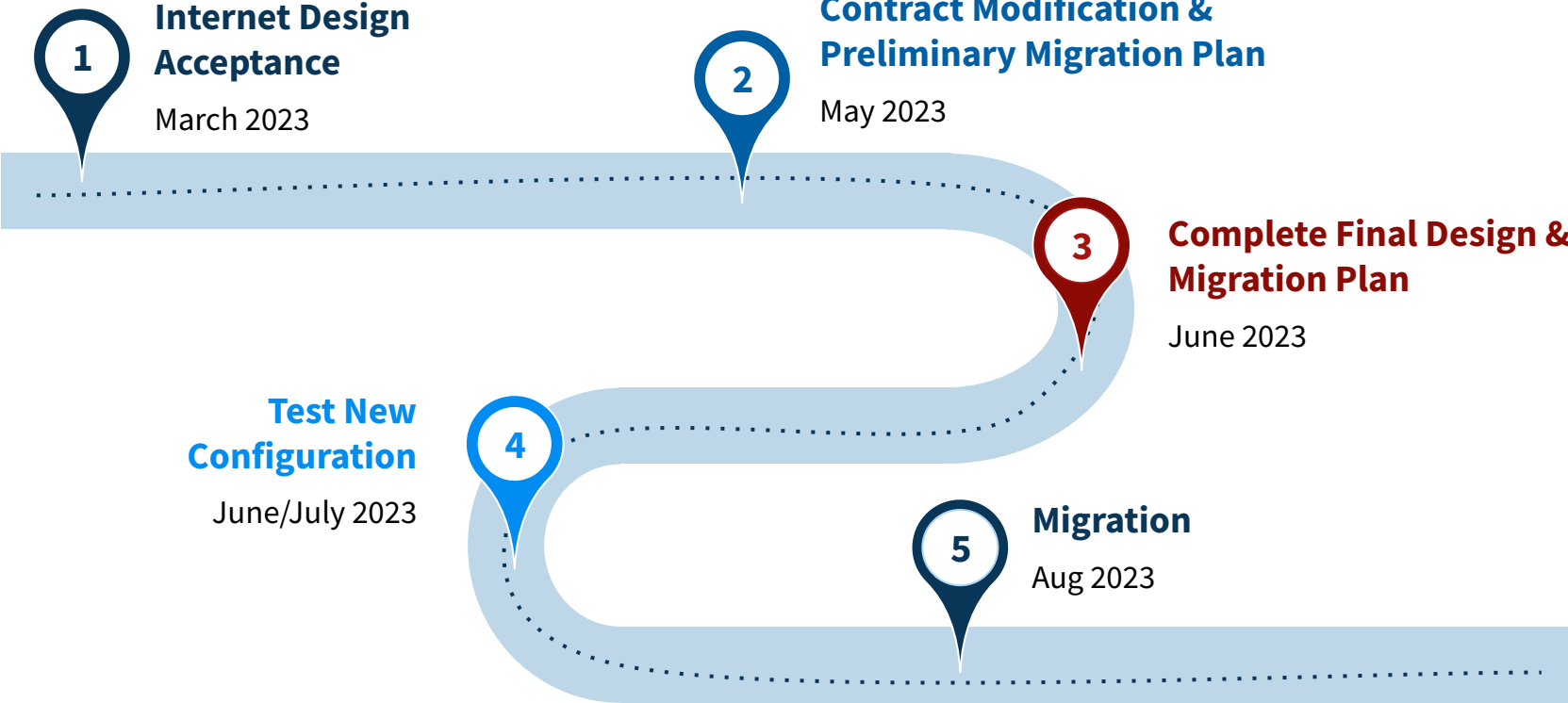
Same hardware & data transmission



Low risk

Safely gain more secure network

Roadmap



To Note

LEADERS

- GSA is **leading the way** in modernizing our network
- GSA will be the **1st agency** to facilitate this change
- Other agencies **asking GSA for advice** on this type of modernization effort



SAFETY FIRST

- Aligning with **Zero Trust** for network technology
- CISA to have **increased monitoring abilities** with Cloud Log Aggregation Warehouse program
- **Zscaler**, other tools protect & monitor GSA's network



SYSTEM OUTAGE

- **System outage** will occur during transition weekend(s)
- GSA apps (HR Links, Pegasys, InSite, ServiceNow, etc.) will be **unavailable**
- Users working **offsite** will still be able to access **Google & cloud resources**



What people are saying

“I have worked for a few government agencies and this VPN [Zscaler] is the **best of any agency** I've worked for. Well done in taking such a fantastic approach to ensuring our jobs can be done as efficiently as possible!”

“ZScaler was a lot easier to use than the normal VPN process. It allows me to be **up and running much quicker.**”

“So much better than the old way of selecting login locations; the amount of **time savings is immeasurable...** this was a seamless and very much time-saving initiative for me!”

Questions?



Backup Slides



Current Status as of 5/1/23

- **DIGIT ROM for MTIPS work has been approved and preliminarily funded (remaining funding has been identified and the funding documents are in the process of being executed)**
- **MetTel is still waiting for the contract mods to be completed, but we do have the preliminary information needed so Alan Suarez can order the new non-MTIPS internet service (SRE {MetTel Required Hardware} orders were placed on 4/26/23)**
- **MetTel will continue their design efforts while we wait for the final contract modifications to be completed**
- **We did confirm that no new circuits will need to be ordered for this service...MetTel will just be adding a new connection between their routers that will bypass the MTIPS infrastructure within the data centers (East and West). Since a new circuit will not be needed, that eliminates the possible circuit availability barriers on delivering this service on time.**
- **Targeting end of July '23 Cutover**

Pros/Cons of New Design



Pros



- ★ ● COSTS!!! (New Internet Connection is significantly less expensive than MTIPS)
- Puts us in line with TIC 3.0/Zero Trust Initiatives
- ★ ● Speed to transition - Less EIS MODs needed
 - Re-Use Same Access Arrangements
 - Re-Use Same transport IPs
 - Re-Use Same SRE/Hardware - Cisco ASR - 1002X
 - Lower environmental impact by reusing existing hardware



Cons



- Added Complexity for METTEL (NAT and other IP Firewall functions moved to ASR {CE Routers})
- Brownfield vs Greenfield Deployment (But GSA will have fallback plan)
- GSA will still have a presence in the Co-Location Facilities (Potential Future Cost savings opportunity)

Cost



Current MTIPS Costs

- **~\$1,963,420 Annually**



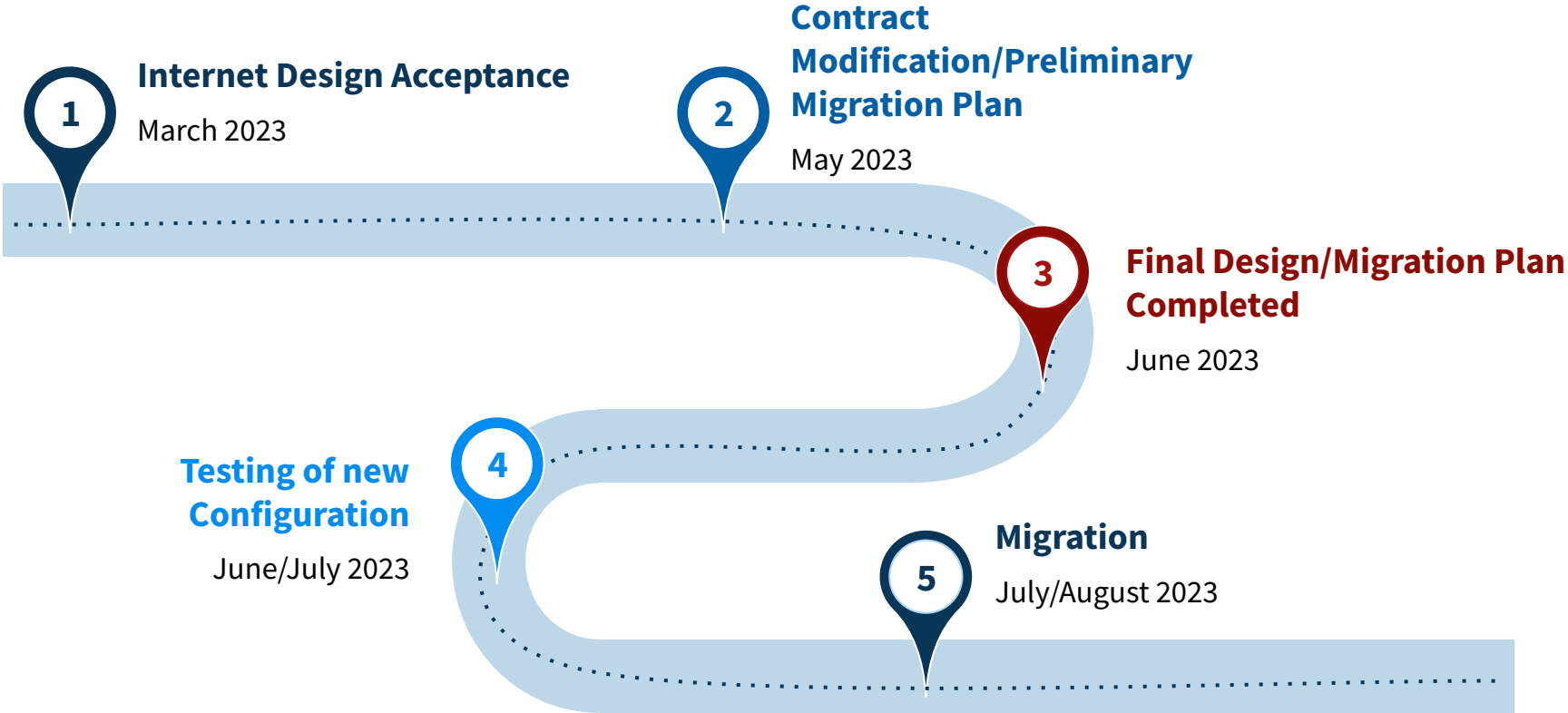
Future Internet Costs

- **~\$222,540 Annually**

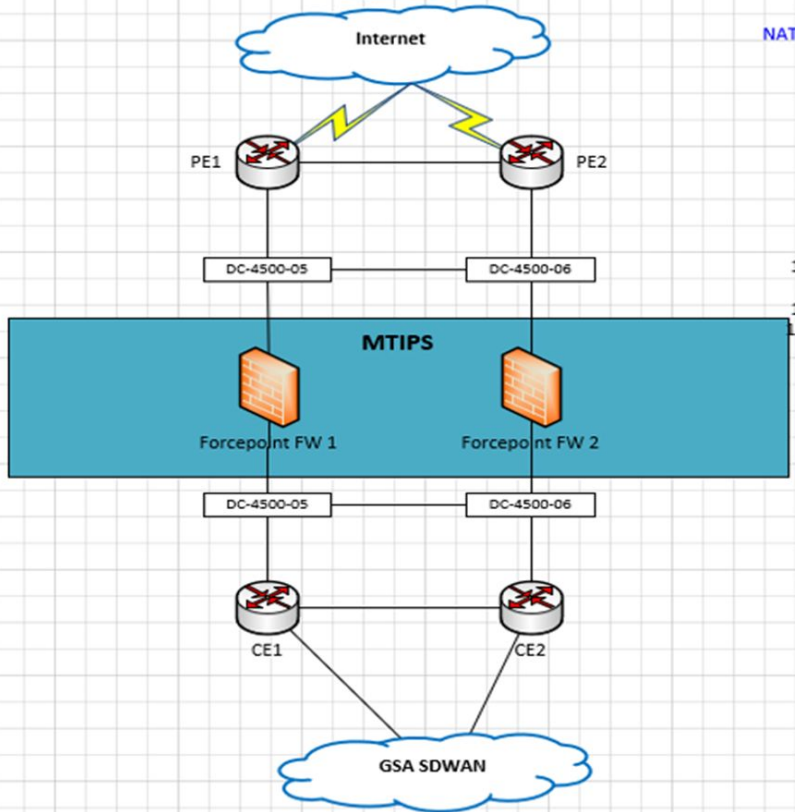
Note: One time payment of \$169,503 for hardware that will be applied to the first payment {this money is available in the current budget}

~\$1.740M Annual Decrease in Cost

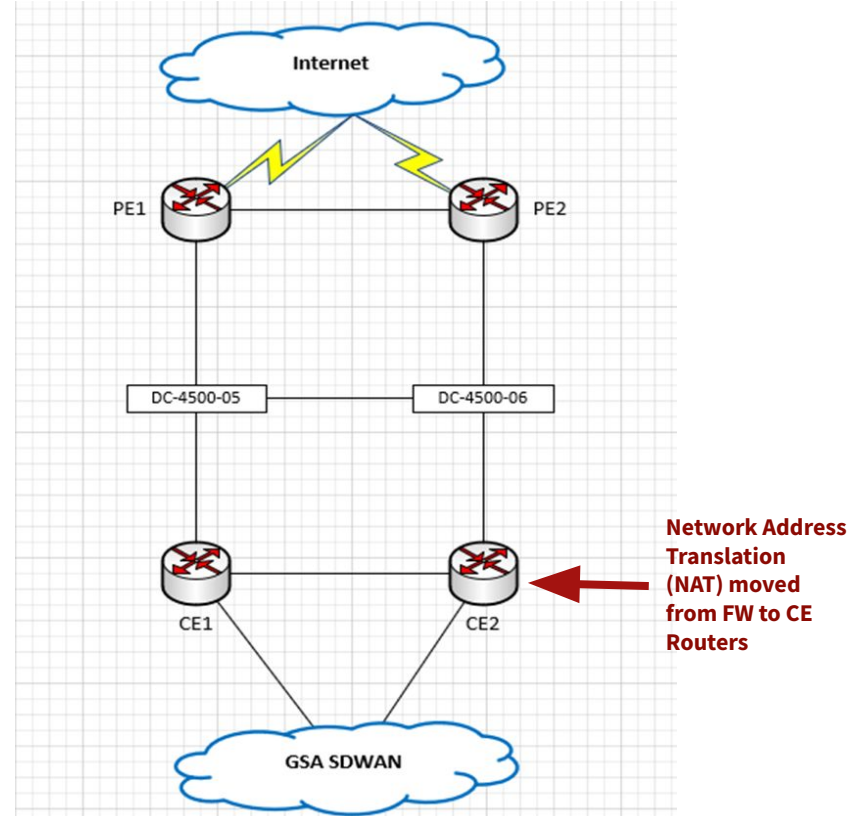
MTIPS Migration Roadmap



Current Design

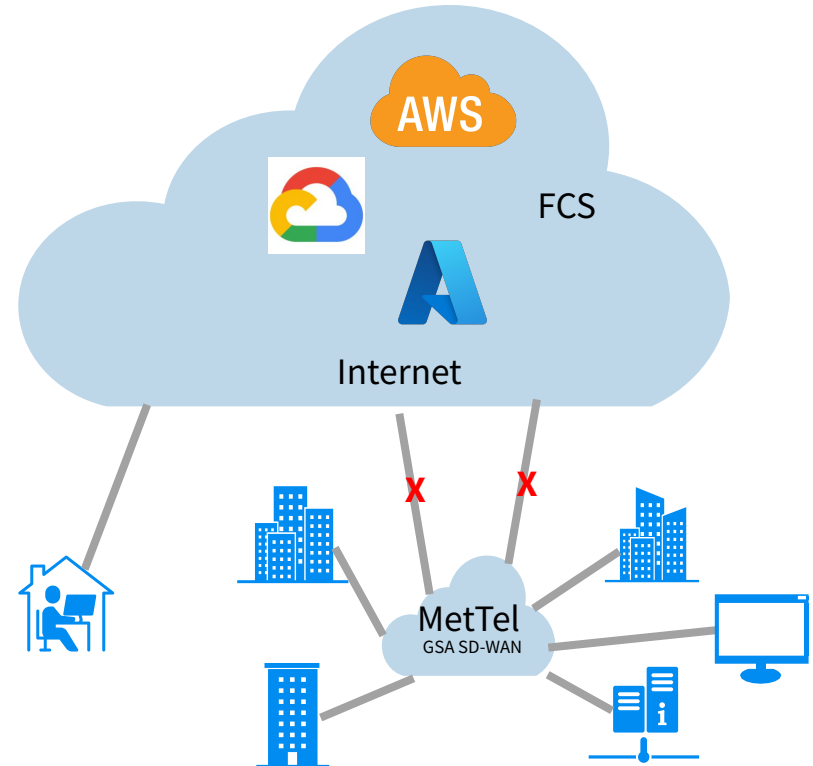


New Design



What We Need Help With????

- **COMMUNICATIONS:** During transition weekend(s), full internet outage should be expected
 - Traffic passing from GSA to the Internet, and from the Internet to GSA will be effected - including user and server traffic
 - Google and cloud traffic from users working off site will not be affected
- **USER COMMUNITY:** Will need to acknowledge that there WILL be an interruption in service during transition weekends
 - All internet facing applications in GSA Datacenters will be effected
- Internal communications within GSA will not be effected



BLUF

- Last met on 7/12/22 detailing our zScaler ZIA and ZPA implementation status and plans, including replacing MTIPS service with no-frills internet connectivity.
- Zscaler Internet Access has now been rolled out to GSA users
- Socialized the action with CISA and CISA TIC leadership and GSA FAS ITC PMO.
 - CISA Feedback:
 - ✓ Have a ISA agreement
 - ✓ CLAW service integration - shipping of Zscaler and Palo Alto firewall logs
 - ✓ Protective DNS integration
 - GSA FAS ITC PMO Feedback:
 - No concerns. Requested to be continually apprised
- Our new TIC 3.0-aligned design is a plus up in security for GSA
- The approach aligns with the CISAs TIC 3.0 Reference Architecture (see ensuing slides for comparative analysis)
- Annual MTIPS savings of \$1.5M will be used for TMF payback and to partial ongoing ZScaler funding.
- MetTel voiced concerns about by-passing MTIPS that we responded to in a memo
- Decision needed to remove MTIPS service provided by MetTel
- Seeking executive decision to disconnect MTIPS in favor of no-frills internet connectivity supported by our security stack on-prem and in the cloud with zScaler.
 - Benefits:
 - ✓ Formalize executive decisioning across GSA and CISA as we will be the first agency to facilitate this change
 - ✓ The decision document with supporting justifications co-signed by GSA and CISA will allay expected questions and concerns from the OIG and/or GAO and Mettel respectively

Replacing MTIPS service with no-frills internet connectivity

(High bandwidth and redundant dedicated internet connections without any added services such as TIC or managed firewalls.)

One of GSA IT's original objectives of the SASE project was to disconnect MTIPS and transition to no-frills internet to:

- Take advantage of CISA's new TIC 3.0 architecture, modernizing TIC capabilities
- Significantly reduce internet connection expenditure and use the recouped funds to pay for SASE

What MTIPS/TIC services does GSA currently leverage?

- CISA IDS traffic monitoring (no SSL decryption); historically service has been of marginal benefit. We do not expect any loss in security utility
 - Given board based implementation of web services encryption traditional TIC offerings have diminished value

GSA previously utilized more MTIPS security services such as perimeter firewall management and perimeter SOC monitoring, however these services were low quality and OCISO assumed the responsibility instead.

Baseline of TIC 2.0 to TIC 3.0

(High bandwidth and redundant dedicated internet connections without any added services such as TIC or managed firewalls.)

How is GSA protected and compliant without MTIPS?

- CISA's TIC 3.0 guidelines permit agencies to implement their own like-for-like TIC solution
- GSA will use a combination of Zscaler, Palo Alto firewalls, the Enterprise Logging Platform (ELP), and the 24x7x365 SOC to align to TIC 3.0 guidelines
- GSA is protected and monitored by multiple layers of security tooling which increase the agency's security posture above and beyond what MTIPS and TIC provide.
- TIC and MTIPS in their current form are outdated, inefficient, and expensive

Mapping of GSA security capabilities to CISA's TIC 3.0 capability guidelines:

Universal Capabilities	✓	Logging, scan tools, SecureAuth..	Resilience PEP Capabilities	✓	Palo Alto, cloud DNS infrastructure
Files PEP Capabilities	✓	Zscaler + Security Agents	DNS PEP Capabilities	✓	Zscaler
Email PEP Capabilities	✓	FireEye ETP	Intrusion Detection PEP Capabilities	✓	Zscaler
Web PEP Capabilities	✓	Zscaler	Enterprise PEP Capabilities	✓	SecOps & 24x7x365 SOC
Networking PEP Capabilities	✓	Zscaler and Palo Alto	Data PEP Capabilities	✓	Encryption + Zscaler DLP

Replacing MTIPS with no-frills internet connectivity...

What does GSA gain by disconnecting MTIPS and replacing it with no-frills internet connectivity?

- GSA will save approximately \$1.5M/yr
- GSA aligns to CISA TIC 3.0 guidelines, modernizing its TIC architecture and likely being one of the first agencies to do so
- GSA will simplify its internet gateway architecture by removing some Mettel MTIPS devices including firewalls.

What does GSA lose?

- CISA will no longer have an intrusion detection system in GSA's internet traffic path.
 - This is mitigated by GSA's integration with the new CISA Cloud Log Aggregation Warehouse (CLAW) program that furthers CISA's visibility into GSA traffic

Leadership Decision to Remove MTIPS

Details of decision:

- Transition to no-frills lower-cost high-speed internet connectivity provided by MetTel by the end of the FY
- Removal of MTIPS firewalls (currently with no rules), replacing the MTIPS security architecture with GSA's TIC 3.0 architecture

Next steps if the decision is made to proceed:

- CISA risk briefing
- Execute GSA/CISA decision memo
- Coordinate and process change management tasks
- Coordinate communications to GSA app teams with the GSA IT Comms team
- Update security documentation to reference the TIC 3.0 architecture