



# Trusted Internet Connection (TIC) & Workplace Modernization



Trusted Internet Connections (TIC) Initiative is to optimize and standardize the security of individual external network connections currently in use by federal agencies, including connections to the Internet. Under the current Network contract, agencies without their own TIC capabilities must procure TIC services by purchasing the costly suite of Managed Trusted Internet Protocol Services (MTIPS).

PSI's TIC services enable the business need and mission all while achieving the tenants of the DHS, GSA, and OMB Modernization efforts: Situational Awareness, Resiliency, and Risk Management. The ability to Protect, Detect, and Respond in a traditional, hybrid, and cloud environment is paramount to protecting federal IT systems.



## Why customers use TIC Modernization

- MTIPS Compliance
- Increased Situational Awareness
- Risk Management

### MTIPS Compliance

- **Azure Cloud will pass DHS MTIPS audit**
- **Azure Cloud will meet FISMA audit**

**Accelerate your agencies compliance**

### Increased Situational Awareness

- **Clear understanding of what is on the Network**
- **Understand what and who is Authorized**
- **Anticipate and respond to threats**

**Fill in architectural gaps with visibility and awareness**

### Risk Management

- **Protect**
- **Detect**
- **Respond**

**Enables you to prioritize assets and protections**

“We’re really pushing to redefine TIC. We’ve had a number of conversations where we said ‘should we even call it TIC anymore’ because it’s going to be so different. We’re making progress towards being unique and different enough that it will support what you’re doing and support future technologies.” – Mark Bunn, Trusted Internet Connections Program Manager, Cybersecurity and Infrastructure Security Agency



# How TIC Modernization works, to achieve business benefits



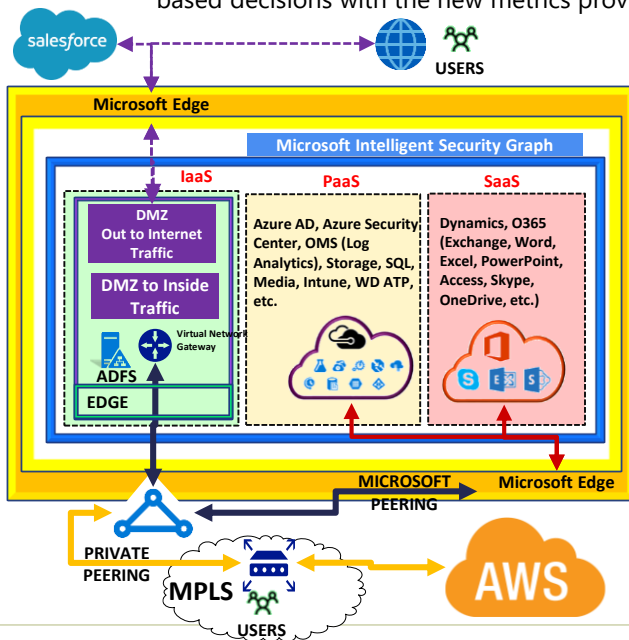
## Reduced Network Latency

- Instant impact to traffic with private network; latency was 175ms to 250ms before and after was 25ms to 75ms at peak time.
- Cost savings of \$6 million a year compared to MTIPS
- Greater network performance reduced user downtime



## Shortened Time to Detect

- Given the greater visibility, Security Analysts were able to greatly reduce noise and respond faster to incidents.
- Time to detect a common malware incident went from 6 days to 3 hours using the native Microsoft tools.
- The CIO and CISO were able to make real time risk based decisions with the new metrics provided.



## Tic Modernization

### Our promise to you

To bring a wealth of knowledge and experience in designing, developing, operating and maintaining small to large-scale high-availability systems in multiple datacenters and cloud environments for our federal and commercial clients.

### An offer to get you started

- See results in days, not months
- Leverage existing tools
- Let PSI give you a demo to see for yourself
- Watch as efficiencies improve, and costs are reduced

## Tangible Benefits / Desired Outcomes

- Utilizing full Microsoft security tools to provide situational awareness of security concerns, giving better and faster insight into security vulnerability trends, customer behaviors.
- Faster access to cloud services to increase customer capacity for compute, storage with tighter integration between front and back end systems.
- Direct connectivity increases bandwidth access to Cloud and Microsoft solutions while reducing the number of hops that could introduce vulnerabilities.

## Practical Solutions, Inc.

PSI has developed a unique strategic approach to resolve the constraints organizations encounter within the Federal Government. Our TIC services enable the business need and mission all while achieving the tenants of the DHS, GSA, and OMB Modernization efforts: Situational Awareness, Resiliency, and Risk Management. The ability to Protect, Detect, and Respond in a traditional, hybrid, and cloud environment is paramount to protecting federal IT systems.