Guidance for Trusted Internet Connection (TIC) Readiness on AWS

February 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

The Trusted Internet Connection (TIC) Initiative[1] is designed to reduce the number of United States Government (USG) network boundary connections, including Internet points of presence (POPs), to optimize federal network services, and improve cyber protection, detection, and response capabilities. In the face of an ever-increasing body of laws and regulations related to information assurance, USG customers wanting to move to the cloud are confronted with security policies, guidelines, and frameworks that assume on-premises infrastructure, and that do not align with cloud design principles. Today, TIC capabilities are not available "in the cloud." This document serves as a guidance for TIC readiness on the Amazon Web Services (AWS) cloud.

Introduction

USG agencies must route connections for the increasing number of mobile users accessing cloud services via smart phones and tablets through their agency network.[2] In alignment with this trend toward mobile use, USG employees and contractors now want the ability to access cloud-based content anytime, anywhere, and with any device. Agencies want to leverage compliant cloud service providers (CSPs) for agile development and rapid delivery of modern, scalable, and cost-optimized applications without compromising on either their information assurance posture or the capabilities of the cloud. In its current form, a TIC-compliant architecture precludes direct access to applications running in the cloud. Users are required to access their compliant CSPs through an agency TIC connection, either a TIC Access Provider (TICAP) or a Managed Trusted IP Service (MTIPS) provider. This architecture often results in application latency and might strain existing government infrastructure. In response to these challenges, the TIC program recently proposed a Draft Federal Risk and Authorization Management Program (FedRAMP)–TIC Overlay[3] that provides a mapping of National Institute of Standards and Technology (NIST) 800-53 security controls to the required TIC capabilities.

Figure 1 below, shows the challenge mobile applications face with the current state of the TIC architecture; it also shows a proposed future state of the architecture contemplated by the Department of Homeland Security (DHS) TIC Program Office and General Services Administration (GSA) FedRAMP Program

Office. This new approach enables direct access to applications running in a compliant CSP. Through a pilot program, DHS and GSA sought to understand whether the objectives of the TIC initiative could be achieved in a cloud environment.

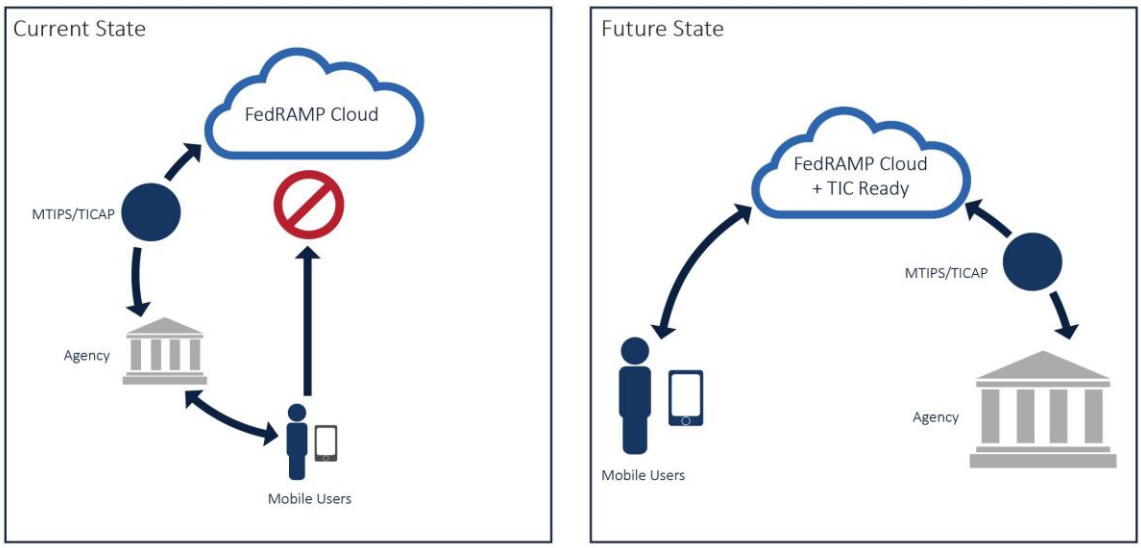

Figure 1: TIC Pilot Objective

FedRAMP-TIC Overlay Pilot

In May of 2015, GSA and DHS invited AWS to participate in a FedRAMP-TIC Overlay pilot. The purpose of the pilot was to determine whether the proposed TIC overlay on the FedRAMP moderate security control baseline was achievable. In collaboration with GSA and DHS, AWS assessed how remote agency users could use the TIC overlay to access cloud-based resources and whether existing AWS capabilities would allow an agency to enforce TIC capabilities.

The scope of the pilot leveraged the existing AWS FedRAMP Moderate authorization. Participants in the pilot included a USG customer, the DHS TIC Program Management Office (PMO), the GSA FedRAMP PMO, and AWS. The alignment to FedRAMP and TIC control objectives was evaluated and administered by an accredited FedRAMP third-party assessment organization (3PAO). Table 1, below, indicates the count of TIC capabilities included in the overlay pilot. Appendix C provides the supporting data for Table 1.

TIC Capabilities Group	Total	Description
Original Capabilities	74	Total TIC v2.0 Reference Architecture Capabilities
Excluded Capabilities	4	TIC Capabilities determined by DHS as excluded from Draft FedRAMP – TIC Overlay. These capabilities are not applicable to FedRAMP Cloud Service Provider environments and are not included in the FedRAMP – TIC Overlay baseline.
Mapped Capabilities	70	Original Capabilities less Excluded Capabilities. These define the baseline FedRAMP – TIC Overlay as defined in the Draft FedRAMP – TIC Overlay Control Mapping.
Deferred Capabilities	13	Mapped Capabilities determined to be specific to the agency (TIC Provider) and removed from the initial scope of the assessment, as directed by DHS TIC and GSA FedRAMP PMO.
Included Capabilities	57	Mapped Capabilities less Deferred Capabilities. These capabilities represent the evaluation target of the pilot.

Table 1: FedRAMP Associated TIC Capabilities Evaluated

The following items were also included in the assessment scope:

- Customer AWS Management Console
- Customer services
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS Identity and Access Management (IAM)
- Customer third-party tools and AWS ecosystem providers used to enforce TIC capabilities
- AWS supporting infrastructure
- Control responsibilities, shown in Table 2

Responsible Party	Total	Description
Customer	16	TIC capabilities determined to be solely the responsibility of the AWS customer
Shared	36	TIC capabilities determined to be a shared responsibility between the customer and AWS
AWS	5	TIC capabilities determined to be solely the responsibility of AWS
TIC Capabilities Evaluated	57	Total number of candidate capabilities evaluated as part of the pilot

Table 2: Control Responsibilities

Pilot Objectives, Process, and Methods

To test the overlay, AWS worked with a FedRAMP-accredited 3PAO and a USG customer to produce results for the following testing objectives:

- Identify whether and how agencies can use TIC overlay controls, via mapping to the FedRAMP Moderate control baseline, to provide remote agency users access to AWS while enforcing TIC compliance.
- Determine whether the required capabilities exist within AWS to implement and enforce TIC compliance.
- Determine the allocation of responsibility for implementing and enforcing TIC compliance.

An initial analysis of the TIC overlay controls by AWS revealed that over 80 percent of the TIC capability requirements map directly to one or more existing FedRAMP Moderate controls satisfied under the current AWS FedRAMP Authority to Operate (ATO). With the control mapping in-hand and in collaboration with our 3PAO, AWS developed a TIC security requirements traceability matrix (SRTM) that included control responsibilities. The results from this exercise, shown in Table 2 above, demonstrated that only 16 TIC capabilities would rest solely with the customer.

Next, our 3PAO proceeded with the following testing process and methods:

- Leveraged previous write-ups, evidence, security documentation, and interviews from the existing AWS FedRAMP Moderate ATO to determine the satisfaction of security controls that were either the responsibility of AWS or a shared responsibility.
- Developed a customer test plan for the controls that were either a customer responsibility or a shared responsibility, using guidance provided by AWS Certified Solutions Architects.
- Tested the covered AWS services (IAM, Amazon EC2, Amazon S3, Amazon EBS, and Amazon VPC) and supporting infrastructure, including features, functionality, and underlying components that assist with enforcing TIC capabilities.
- Tested implementation of shared and customer responsibilities using a Customer Test Plan and a TIC Pilot SRTM.
- Interviewed the USG customer on internal policies, procedures, and security tools used to enforce TIC capabilities as defined by DHS.
- Collected evidence from the customer to complete assessment of the customer and shared responsibility controls.

Pilot Results

After completion of the assessment phase of the pilot, roughly two dozen of the included TIC capabilities required additional discussion with the DHS TIC PMO. The outstanding items were reviewed sequentially, and final dispositions were recorded based on DHS TIC PMO direction. Table 3 below summarizes the results of the pilot assessment and final disposition discussion as synthesized by AWS.

FedRAMP Associated TIC Capabilities Version 2.0 Disposition	Total	Description
Implemented	43	TIC capability determined as satisfied or able to be satisfied on AWS.
Gap	1	TIC capability determined to require further evaluation on AWS by FedRAMP PMO and DHS.

Not Assessed	13	TIC capability determined to be not applicable to a CSP or not included in the customer environment.
FedRAMP-TIC Capabilities Evaluated	57	Total number of candidate capabilities evaluated as part of the pilot.

Table 3: Synthesized FedRAMP- TIC Associated Capability Dispositions

Customer Implementation Guidance

Based on the results of the pilot and lessons learned, AWS is providing guidance on both relevant connection scenarios and the use of AWS capabilities and features that align with the FedRAMP-TIC Overlay work described above. Following the conclusion of the overlay pilot, and pending official guidance from the FedRAMP PMO and TIC PMO, AWS designed the next sections to provide USG agencies and contractors with information to assist in the development of "TIC Ready" architectures on AWS. As additional reference, Appendix A contains a Control Implementation Summary (CIS) showing TIC Capability to FedRAMP Control mappings and includes responsible party information. Appendix B provides per-control guidance for AWS and ecosystem capabilities that enable customer compliance with required TIC capabilities. Finally, Appendix C contains a mapping of TIC Capabilities to their AWS-synthesized dispositions.

Connection Scenarios

In this section, we highlight common connection scenarios that relate to TIC compliance. For each scenario we provide a brief explanation and a high-level architecture diagram.

Public Web and Mobile Applications (Not Included in Pilot)

This use case covers public, unauthenticated web and mobile applications. These applications are accessible via the Internet, typically over HTTPS, by the general public. Users access these web and mobile applications using their choice of web browser and device. They can access these web and mobile applications from their home or any public Wi-Fi networks or via their mobile devices. These applications are deployed in one or more AWS regions. Figure 2 below, illustrates this connection scenario.

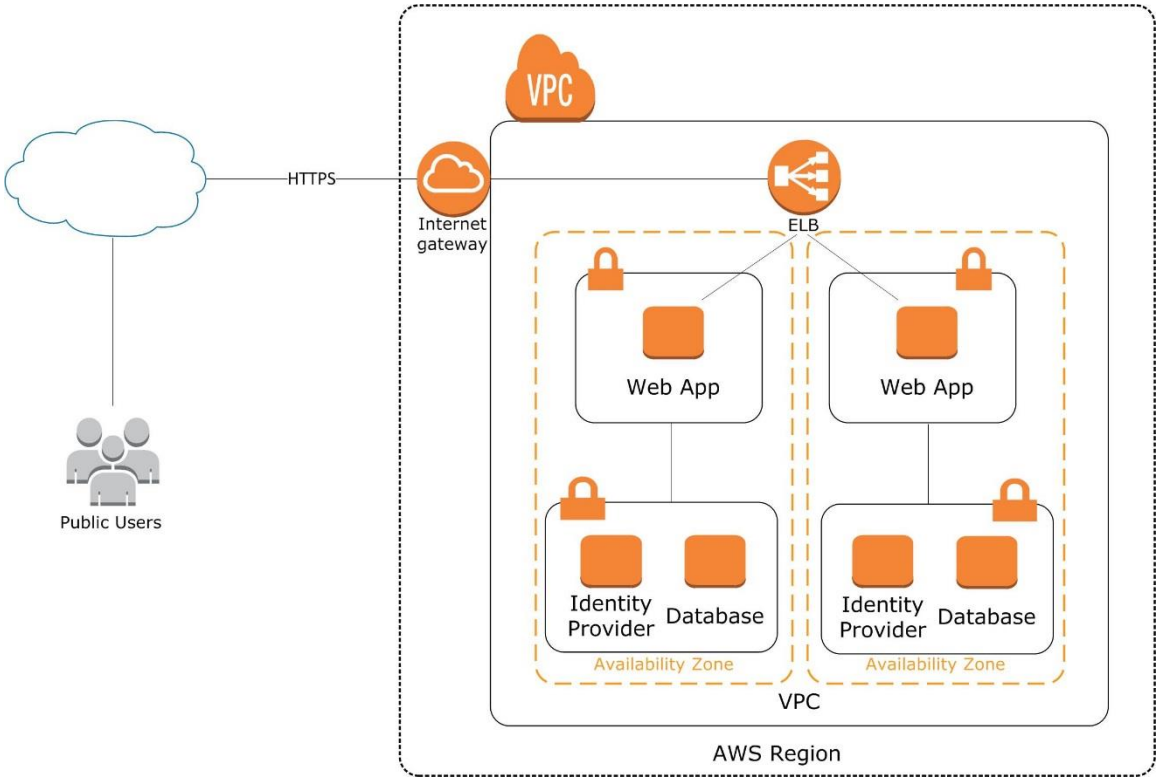

Figure 2: Public Web and Mobile Applications (Unauthenticated)

In this architecture, an Internet Gateway (IGW) provides Internet connectivity to two or more customer-defined public subnets across two or more Availability Zones (Multi-AZ) in the VPC. An Elastic Load Balancing (ELB) load balancer is placed in these public subnets. A web tier is configured within an Auto Scaling group, leveraging the load balancer, to provide a continuously available web front end. The web tier securely communicates with back end resources, such as databases and other persistent storage. The environment is completely contained within the cloud.

Public Web and Mobile Applications Requiring Authentication: "All in" Deployments

This use case covers authenticated web and mobile application used in an "all in cloud" deployment. These applications are accessible via the Internet, typically over HTTPS, by the agency users. They access these web and mobile applications from their home, any public Wi-Fi networks, or agency networks using either personal or agency-issued electronic devices. These applications are deployed in one or more AWS regions. These applications leverage role-based authentication

to arbitrate access to application functionality. The following examples are public websites with authentication requirements:

- System for Award Management (SAM)
- GSA Advantage
- OMB Max Portal
- Cloud-based software as a service (SaaS) offerings (e.g., email)

Figure 3 below illustrates this connection scenario.

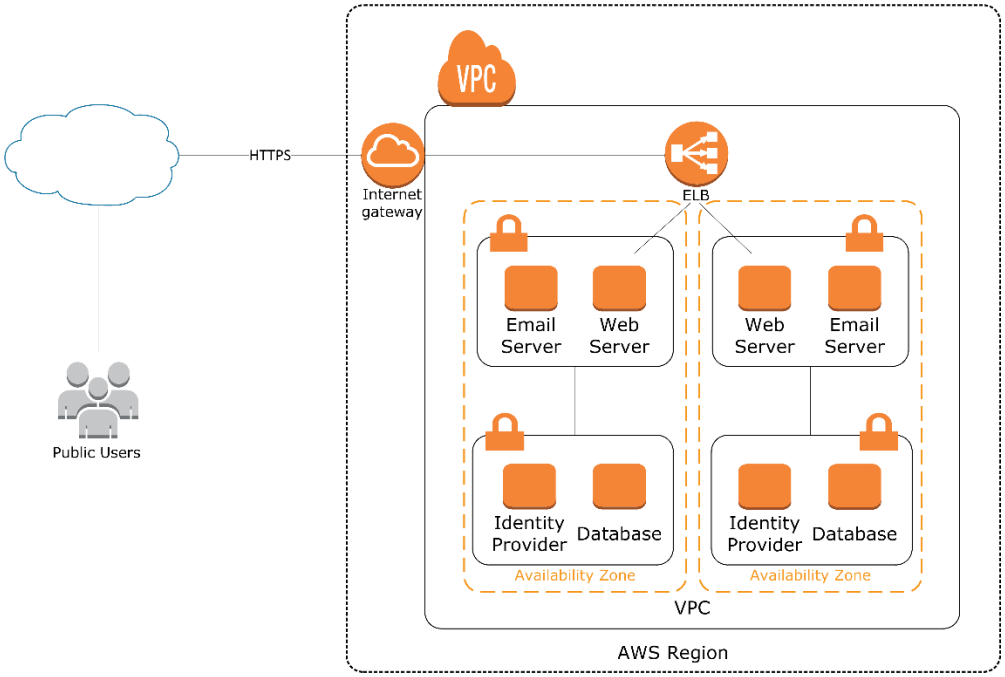

Figure 3: Public Web and Mobile Applications - Authenticated, All In

In this architecture, an IGW provides Internet connectivity to two or more customer-defined public subnets across multiple Availability Zones in the VPC. An ELB load balancer is placed in these public subnets. A web-tier is configured within an Auto Scaling group, leveraging the ELB load balancer to provide a continuously available web front end. This web tier securely communicates with other backend resources, most notably the backend identity store used for role-based authentication. The environment is completely contained within the cloud.

Public Web and Mobile Applications Requiring Authentication: "Hybrid" Deployments

This use case covers authenticated web and mobile application use where a portion of the environment resides within a customer datacenter. These applications are accessible via Internet, typically over HTTPS, by the agency users. They access these web and mobile applications from their home, any public Wi-Fi networks, or agency networks using either personal or agency-issued electronic devices. These applications are deployed in one or more Amazon Web Services (AWS) regions and one or more customer datacenters. These applications leverage role-based authentication to arbitrate access to application functionality.

In the hybrid deployment scenario, a portion of the application architecture, typically the public web presence, resides in the cloud while another portion, typically sensitive data sources, reside in an agency datacenter. This scenario is most commonly seen when an agency wishes to maintain its identity and/or data stores outside of the cloud environment. Connectivity between the in-cloud portions of the application and the controlled, on-premises components is achieved using AWS Direct Connect or VPN service in conjunction with a TICAP or MTIPS provider. In this way, data flow between the customer's in-cloud and

on-premises services are seen by the TIC. Figure 4 below, illustrates this connection scenario.

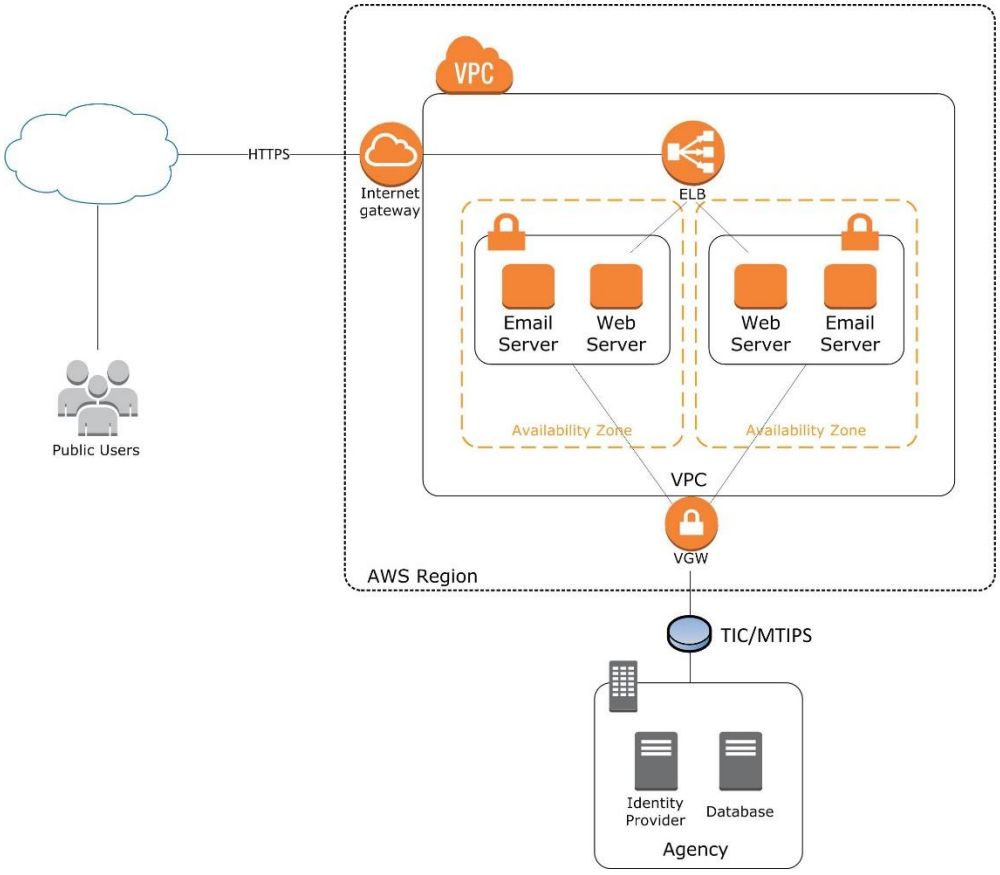

Figure 4: Public Web and Mobile Applications - Authenticated, Hybrid

AWS Capabilities and Features

In order to achieve TIC compliance on AWS, we recommend using the following AWS capabilities and features and following our published best practices to secure the resources.

AWS Identity and Access Management (IAM) is a web service that enables IT organizations to manage multiple users, groups, roles, and permissions for AWS services such as Amazon EC2, Amazon Relational Database Service (RDS) and Amazon VPC. IT can centrally manage AWS Service related resources through IAM policies using security credentials such as Access Keys. These access keys can be applied to users, groups, and roles.

AWS CloudFormation is a web service that uses JSON templates within which customers can describe their IT architecture as code. These templates can then be used to launch or create AWS resources that were defined within the template. This collection of resources is called a *stack*. CloudFormation templates allow agencies to programmatically implement controls for new and existing environments. These controls provide comprehensive rule sets that can be systematically enforced.

AWS CloudTrail provides a log of all requests and a history of AWS API calls for AWS resources. This includes calls made by using the AWS Management Console, AWS SDKs, command-line tools (CLI), and higher-level AWS services. IT can identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, and when the calls were made.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

CloudWatch Logs can be used to monitor your logs for specific phrases, values, or patterns. For example, you could set an alarm on the number of errors that occur in your system logs or view graphs of web request latencies from your application logs. You can view the original log data to see the source of the problem if needed. Log data can be stored and accessed for as long as you need using highly durable, low-cost storage so you don't have to worry about filling up hard drives.

AWS Config is a managed service that provides an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config, IT can discover existing AWS resources, export a complete inventory of AWS resources with all configuration details, and determine how a resource was configured at any point in time. This facilitates

compliance auditing, security analysis, resource change tracking, and troubleshooting. You can use AWS Config Rules to create custom rules used to evaluate controls applied to AWS resources. AWS also provides a list of standard rules that you can evaluate against your AWS resources, such as checking that port 22 is not open in any production security group.

Amazon S3 is storage for the Internet. Amazon S3 is a highly scalable, durable, and available distributed object store designed for mission-critical and primary data storage. Amazon S3 stores objects redundantly on multiple devices across multiple facilities within an AWS region. Amazon S3 is designed to protect data and allow access to it even in the case of a failure of a data center. The versioning feature in Amazon S3 allows the retention of prior versions of objects stored in Amazon S3 and also protects against accidental deletions initiated by staff or software error. Versioning can be enabled on any Amazon S3 bucket.

Amazon EC2 is a web service that provides resizable compute capacity in the cloud; it is essentially server instances used to build and host software systems. Amazon EC2 is designed to make web-scale computing easier for developers and customers to deploy virtual machines on demand. The simple web service interface allows customers to obtain and configure capacity with minimal friction; it provides complete control of their computing resources. Amazon EC2 changes the economics of computing because it allows enterprises to avoid large capital expenditures by paying only for capacity that is actually used.

Amazon VPC enables the creation of a logically separate space within AWS that can house compute resources and storage resources that can be connected to a customer's existing infrastructure through a virtual private network (VPN), AWS Direct Connect, or the Internet. With Amazon VPC, it is possible to extend existing management capabilities and security services such as DNS, LDAP, Active Directory, firewalls, and intrusion detection systems to include private AWS resources, maintaining a consistent means of protecting information whether residing on internal IT resources or on AWS.

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. With Amazon Glacier, customers can reliably store their data for as little as $0.007 per gigabyte per month. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don't have to worry about

capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations

Amazon VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs. Flow logs can help you with a number of tasks; for example, you can troubleshoot why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.

Conclusion

AWS services, features, and our partner ecosystem deliver a suite of capabilities that assist in delivering "TIC Ready" cloud architectures. Through collaboration with a USG customer, the DHS TIC Program Management Office (PMO), the GSA FedRAMP PMO, and our accredited FedRAMP third-party assessment organization (3PAO), AWS has demonstrated how customers might enforce many of the capabilities prescribed by TIC. While the FedRAMP TIC Overlay is being finalized, using the evidence resulting from our TIC Mobile assessment, USG customers can implement the TIC capabilities as part of their virtual perimeter protection solution using functionality provided by AWS, with a clear definition of the customer responsibility for implementation of the additional TIC capabilities.

Contributors

The following individuals and organizations contributed to this document:

- Jennifer Gray, US Public Sector Compliance Architect, AWS Security
- Alan Halachmi, Principal Solutions Architect, Amazon Web Services
- Nandakumar Sreenivasan, Senior Solutions Architect, Amazon Web Services

APPENDIX A:

Control Implementation Summary

TIC v2.0 Associated FedRAMP Security Controls	FedRAMP Control Mapping	RESPONSIBILITY
ID	ID	
TM.AU.01	AC-6 (1)	SHARED
	AC-6 (2)	
	IA-1	
	IA-2	
	IA-2 (1)	
	IA-2 (2)	
	IA-2 (3)	
	IA-2 (8)	
	IA-2 (11)	
	IA-2 (12)	
	IA-3	
	IA-4	
	IA-4 (4)	
	IA-5	
	IA-5 (1)	
	IA-5 (2)	
	IA-5 (3)	
	IA-5 (6)	
	IA-5 (7)	
	IA-5 (11)	
	IA-6	
	IA-7	
	IA-8	
TM.COM.02	AC-8	SHARED
	CA-3	
	PL-4	
TM.DS.01	AU-4	CUSTOMER
TM.DS.02	CP-2	CUSTOMER
	CP-10	
TM.DS.03	AU-1	SHARED
	SI-4	
	N/A	
TM.DS.04	AU-1	SHARED
TM.DS.05	N/A	CUSTOMER
TM.LOG.01	AU-8 (1)	SHARED
TM.LOG.02	AU-3	SHARED
TM.LOG.03	AU-11	SHARED
TM.LOG.04	AU-11	SHARED

TIC v2.0 Associated FedRAMP Security Controls	FedRAMP Control Mapping	RESPONSIBILITY
ID	ID	
TM.PC.06	N/A	SHARED
TM.TC.01	CP-8	AWS
	CP-8 (1)	
	CP-8 (2)	
TM.TC.02	CM-7	SHARED
TM.TC.03	CP-11	SHARED
TM.TC.04	SC-20	CUSTOMER
	SC-21	
	SC-22	
TM.TC.05	IR-8	SHARED
TM.TC.06	IR-1	SHARED
TM.TC.07	CP-2	SHARED
TO.MG.01	CM-8	SHARED
TO.MG.02	CM-3	SHARED
	CM-9	
TO.MG.04	CP-2	SHARED
TO.MG.07	CM-8	SHARED
TO.MG.08	N/A	AWS
TO.MG.09	N/A	AWS
TO.MG.10	N/A	AWS
TO.MG.11	N/A	AWS
TO.MON.02	CA-2	SHARED
TO.MON.03	AU-6 (1)	SHARED
TO.MON.04	AU-1	SHARED
	AU-2	
TO.MON.05	IR-3	CUSTOMER
TO.REP.01	CA-7	SHARED
TO.REP.02	CA-7	SHARED
TO.REP.03	CA-7	SHARED
TO.REP.04	IR-6	SHARED
TO.RES.01	IR-8	SHARED
TO.RES.02	SI-2	SHARED
TO.RES.03	SC-5	SHARED
TS.CF.01	SC-7	SHARED
	SC-7 (8)	
TS.CF.02	SC-7	SHARED
	SC-7 (8)	
TS.CF.03	SC-7	SHARED
	SC-7 (8)	
TS.CF.04	SC-7	CUSTOMER
	SI-3	
	SI-8	

TIC v2.0 Associated FedRAMP Security Controls	FedRAMP Control Mapping	RESPONSIBILITY
ID	ID	
TS.CF.05	SI-4	CUSTOMER
TS.CF.06	SC-8 (1)	CUSTOMER
TS.CF.07	SC-8 (1)	CUSTOMER
TS.CF.08	SI-4	CUSTOMER
TS.CF.09	IA-9	SHARED
TS.CF.10	IA-5	SHARED
TS.CF.13	AU-3 (1)	CUSTOMER
	SC-7	
	SC-20	
	SC-21	
	SC-22	
TS.INS.01	AU-1	CUSTOMER
	AU-6	
	AU-6 (1)	
	SC-7	
TS.PF.01	AC-4	CUSTOMER
	SC-7	
TS.PF.03	SC-7	SHARED
TS.PF.04	SC-7	SHARED
TS.PF.06	AU-3 (1)	SHARED
TS.RA.01	AC-17	CUSTOMER
	AC-17 (2)	
	IA-2 (2)	
	SC-7 (7)	
TS.RA.02	AC-20	CUSTOMER
	CA-3	
	CA-3 (3)	
	CA-3 (5)	
TS.RA.03	AC-20	CUSTOMER

APPENDIX B:

Implementation Guidance

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TM.AU.01	User Authentication	SHARED	Leverage IAM and its multi-factor authentication capabilities.
TM.COM.02	TIC and Customer	SHARED	Leverage IAM Policies to control and to restrict access to AWS resources.
TM.DS.01	Storage Capacity	CUSTOMER	Leverage AWS Marketplace providers for packet capture and analysis. Leverage VPC Flow Logs to capture data flow metadata. Leverage CloudWatch Logs with appropriate log retention for log aggregation. Enable logging with AWS services (e.g., S3 logs, ELB logs).
TM.DS.02	Back up Data	CUSTOMER	Leverage AWS CloudFormation to template the environment. Leverage EC2 AMI Copy, S3 versioning, S3 cross-region replication, S3 MFA delete, and S3 life-cycle policies for backup. Leverage EC2 auto-scaling to recovery from transient hardware failures.
TM.DS.03	Data Ownership	SHARED	Administrative control.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TM.DS.04	Data Attribution & Retrieval	SHARED	Leverage S3 buckets with IAM policies and S3 bucket policies to segregate access to data. Configure services, such as CloudTrail, to log to the appropriate bucket. If needed, leverage S3 Events to initiate data processing workflows. Leverage CloudWatch Logs with IAM policies to consolidate or segregate agency data as required. Implement VPC Flow Logs on all VPCs. Enable CloudTrail logs. Enable AWS Config. Enable ELB logs. Enable S3 logs.
TM.DS.05	DLP	CUSTOMER	Leverage AWS Marketplace providers for DLP technologies. Leverage S3 buckets with versioning enabled and MFA delete. Enable S3 cross-region replication of critical or sensitive data into another AWS account in another region. Leverage Glacier Vault Lock for data retention.
TM.LOG.01	NTP Server	SHARED	Configure approved NTP providers within the customer environment.
TM.LOG.02	Time Stamping	SHARED	Configure approved NTP providers within the customer environment.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TM.LOG.03	Session Traceability	SHARED	Leverage S3 buckets with appropriate lifecycle policies. Configure services, such as CloudTrail, to log to the appropriate bucket. If needed, leverage S3 Events to initiate data processing workflows. Leverage CloudWatch Logs to receive AWS-specific and customer service logs with appropriate retention policies. Configure services, such as VPC Flow Logs, to log to the appropriate Log Stream. Leverage AWS Marketplace offerings for log aggregation and analysis.
TM.LOG.04	Log Retention	SHARED	Leverage S3 lifecycle policies. Leverage Glacier Vault Lock.
TM.PC.06	Geographic Diversity	SHARED	AWS provides geographic diversity within a region. Customers must leverage multiple Availability Zones to achieve this diversity. Customers may also elect to deploy multi-region applications.
TM.TC.01	Route Diversity	AWS	AWS provides route diversity intra-region, inter-region, and for Internet access.
TM.TC.02	Least Functionality	SHARED	Leverage IAM Policies to restrict access to AWS resources. Leverage Network Access Control Lists (NACLs) for course-grained, stateless packet filtering. Leverage Security Groups (SGs) for fine-grained, stateful flow filtering. Consider a separation of duties approach for management of NACLs and SGs.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TM.TC.03	IPv6	SHARED	Contact AWS Sales Representative regarding current IPv6 offerings.
TM.TC.04	DNS Authoritative Servers	CUSTOMER	Leverage customer-managed DNS systems.
TM.TC.05	Response Authority	SHARED	Leverage AWS access and flow control capabilities, including IAM, Network Access Control Lists, and Security Groups. Leverage AWS Marketplace providers.
TM.TC.06	TIC Staffing	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g., OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TM.TC.07	Response Access	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g. OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies. Leverage AWS CloudFormation to template the environment. Leverage EC2 AMI Copy, S3 versioning, S3 cross-region replication, S3 MFA delete, and S3 life-cycle policies for backup. Leverage EC2 Auto Scaling to recovery from transient hardware failures.
TO.MG.01	System Inventory	SHARED	Leverage AWS Config. Leverage resource-level tags.
TO.MG.02	Change & Configuration Management	SHARED	AWS maintains a formalized change and configuration management system. Customers are responsible for these processes within their AWS environment.
TO.MG.04	Contingency Planning	SHARED	Leverage AWS CloudFormation to template the environment. Leverage EC2 AMI Copy, S3 versioning, S3 cross-region replication, S3 MFA delete, and S3 life-cycle policies for backup. Leverage EC2 Auto Scaling to recovery from transient hardware failures. Plan for alternate region recovery.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TO.MG.07	Network Inventory	SHARED	Leverage AWS Config. Leverage resource-level tags.
TO.MG.08	Service Level Agreement	AWS	AWS provides service level information through published artifacts, including the AWS website.
TO.MG.09	Tailored Service Level Agreement	AWS	AWS provides elasticity natively as a cloud service provider. AWS services can expand/contract based on customer configuration and demand.
TO.MG.10	Tailored Security Policies	AWS	AWS allows customers to customize their cloud environment, including security policies.
TO.MG.11	Tailored Communications	AWS	AWS provides services and features that enable customers to tailor communication processes. AWS develops new capabilities based on customer demand.
TO.MON.02	Vulnerability Scanning	SHARED	Leverage pre-authorized products from the AWS Marketplace and/or submit request to AWS for customer-executed vulnerability scans.
TO.MON.03	Audit Access	SHARED	Leverage IAM to control and to restrict access to AWS resources.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TO.MON.04	Log Sharing	SHARED	Leverage S3 buckets with IAM policies and S3 bucket policies to segregate access to data. Configure services, such as CloudTrail, to log to the appropriate bucket. If needed, leverage S3 Events to initiate data processing workflows. Leverage CloudWatch Logs with IAM policies to consolidate or segregate agency data as required. Implement VPC Flow Logs on all VPCs. Enable CloudTrail logs. Enable AWS Config. Enable ELB logs. Enable S3 logs.
TO.MON.05	Operational Exercises	CUSTOMER	Customer Responsibility. Contact your AWS Sales Representative regarding Security Incident Response Simulation (SIRS) Game Day offering.
TO.REP.01	Customer Service Metrics	SHARED	AWS maintains customer service metrics. Customers must provide customer service for their application. Customer secures an AWS Support plan and designates an account point of contact such that AWS customer service may engage as required.
TO.REP.02	Operational Metrics	SHARED	AWS maintains operational metrics. Customers must provide operational metrics for their application.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TO.REP.03	Customer Notification	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g., OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies. Customers provide like capabilities for users of applications they operate on AWS.
TO.REP.04	Incident Reporting	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g. OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies. Customers provide like capabilities for users of applications they operate on AWS.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TO.RES.01	Response Timeframe	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g., OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies. Customers provide their own incident response plan.
TO.RES.02	Response Guidance	SHARED	AWS provides network and security operations continuously. Leverage AWS log sources (e.g., S3 logs, ELB logs, VPC Flow Logs, CloudTrail, Config, etc.) and customer-specific logs (e.g., OS logs, application logs, etc.) to assess network and security operation. Customer designates security points of contact within a customer account such that AWS may communicate detected anomalies. Customers provide their own incident response plan.
TO.RES.03	Denial of Service Response	SHARED	Leverage Anti-DDoS design patterns described in AWS whitepapers. Leverage Elastic Load Balancing. Leverage Auto Scaling. Leverage Network Access Controls Lists. Leverage Security Groups. Leverage AWS Marketplace providers for appropriate tools.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TS.CF.01	Application Layer Filtering	SHARED	Leverage AWS Marketplace providers for appropriate tools.
TS.CF.02	Web Session Filtering	SHARED	Leverage AWS Marketplace providers for appropriate tools.
TS.CF.03	Web Firewall	SHARED	Leverage AWS Marketplace providers for appropriate tools.
TS.CF.04	Mail Filtering	CUSTOMER	Customer responsibility.
TS.CF.05	Agency Specific Mail Filters	CUSTOMER	Customer responsibility.
TS.CF.06	Mail Forgery Detection	CUSTOMER	Customer responsibility.
TS.CF.07	Digitally Signing Mail	CUSTOMER	Customer responsibility.
TS.CF.08	Mail Quarantine	CUSTOMER	Customer responsibility.
TS.CF.09	Crypto-graphically authenticated protocols	SHARED	AWS Direct Connect requires customer use of BGP MD5 authentication.
TS.CF.10	Reduce the use of clear-text management protocols	SHARED	Leverage IAM aws:SecureTransport Policy Condition.
TS.CF.13	DNS Filtering	CUSTOMER	Customer responsibility.
TS.INS.01	NCPS	CUSTOMER	Customer responsibility.
TS.PF.01	Secure all TIC traffic	CUSTOMER	Customer responsibility
TS.PF.03	Stateless Filtering	SHARED	Leverage Network Access Control Lists.
TS.PF.04	Stateful Filtering	SHARED	Leverage Security Groups. Leverage AWS Marketplace providers.
TS.PF.06	Asymmetric Routing	SHARED	Implement symmetric routing in to or out from AWS.
TS.RA.01	Agency-User Remote Access	CUSTOMER	Customer responsibility. Leverage Customer Gateway, VPN, and Virtual Private Gateway to connect a VPC with a site-to-site VPN.

TIC v2.0 Associated FedRAMP Security Controls		RESPONSIBILITY	AWS Feature Mapping
TS.RA.02	External Dedicated Access	CUSTOMER	Customer responsibility.
TS.RA.03	Extranet Dedicated Access	CUSTOMER	Customer responsibility.

APPENDIX C:

Mapped FedRAMP TIC Capabilities Matrix

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
TM.AU.01	User Authentication	TIC systems and components comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access to TIC access point devices requires multi-factor authentication (OMB M-11-11).	INCLUDED	IMPLEMENTED
TM.COM.01	TIC and US-CERT (TS/SCI)	The TICAP has a minimum of three qualified people with TOP SECRET/SCI clearance available within 2 hours, 24x7x365, with authority to report, acknowledge and initiate action based on TOP SECRET/SCI-level information, including tear line information, with US-CERT. Authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access to an ICD 705-accredited Sensitive Compartment Information Facility (SCIF) including	EXCLUDED	N/A

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		the following TOP SECRET/SCI communications channels: - Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI, and - Secure FAX machine. Typically personnel with appropriate clearances to handled classified information will include at least the Senior NOC/SOC manager, Chief Information Security Officer (CISO), and Chief Information Officer (CIO), and other personnel as determined by the agency. The SCIF may be shared with another agency and should be within 30 minutes of the TIC management location, during normal conditions, in order for authorized personnel to exchange classified information, evaluate the recommendations, initiate the response and report operational status with US-CERT within two hours of the notification.		
TM.COM.02	TIC and Customer	The Multi-Service TICAP secures and authenticates the administrative communications (i.e., customer service) between the TICAP operator and each TICAP client.	INCLUDED	IMPLEMENTED
TM.COM.03	TIC and US-CERT (SECRET)	The TICAP has a minimum of one qualified person with SECRET or higher clearance immediately available on each shift, 24x7x365, with authority to report, acknowledge and initiate action based on SECRET-level information; including tear-line information, with US-CERT. Authorized personnel with SECRET	EXCLUDED	N/A

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		clearances or higher have 24x7x365 immediate access at the TIC management location (NOC/SOC) to the following SECRET communications channels: - Secure telephone (STE/STU) and card authorized for SECRET or higher, - Secure FAX machine, - SECRET-level email account able to exchange messages with the Homeland Secure Data Network (HSDN), and - Access to the US-CERT SECRET website. Additionally, authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access within 2 hours of notification to an ICD 705 accredited Sensitive Compartment Information Facility (SCIF) including the following TOP SECRET/SCI communications channels: - Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI, - Secure FAX machine, - TOP SECRET/SCI-level email account able to exchange messages with the Joint Worldwide Intelligence Communications System (JWICS), and - Access to the US-CERT TOP SECRET website.		
TM.DS.01	Storage Capacity	Each TIC access point must be able to perform real-time header and content capture of all inbound and outbound traffic for administrative, legal, audit or other operational purposes. The TICAP has storage capacity to retain at least 24 hours of data generated at full TIC operating capacity. The TICAP	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		is able to selectively filter and store a subset of inbound and outbound traffic.		
TM.DS.02	Back up Data	In the event of a TICAP system failure or compromise, the TICAP has the capability to restore operations to a previous clean state. Backups of configurations and data are maintained off-site in accordance with the TICAP continuity of operations plan.	INCLUDED	IMPLEMENTED
TM.DS.03	Data Ownership	The Multi-Service TICAP documents in the agreement with the customer agency that the customer agency retains ownership of its data collected by the TICAP.	INCLUDED	IMPLEMENTED
TM.DS.04	Data Attribution & Retrieval	The Multi-Service TICAP identifies and can retrieve each customer agency's data for the customer agency, without divulging any other agency's data.	INCLUDED	IMPLEMENTED
TM.DS.05	DLP	The TICAP has a Data Loss Prevention program and follows a documented procedure for Data Loss Prevention.	INCLUDED	IMPLEMENTED
TM.LOG.01	NTP Server	Each TIC access point has a Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC). The primary synchronization method is an out-of-band NIST/USNO national reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock. See the TIC Reference Architecture, Appendix F for additional information.	INCLUDED	IMPLEMENTED
TM.LOG.02	Time Stamping	All TIC access point event recording clocks are synchronized to within 3 seconds relative to Coordinated	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		Universal Time (UTC). All TICAP log timestamps include the date and time, with at least to-the-second granularity. Log timestamps that do not use Coordinated Universal Time (UTC) include a clearly marked time zone designation. The intent is to facilitate incident analysis between TICAPs and TIC networks and devices.		
TM.LOG.03	Session Traceability	The TICAP provides online access to at least 7 days of session traceability and audit ability by capturing and storing logs / files from installed TIC equipment including, but not limited to firewalls, routers, servers and other designated devices. The TICAP maintains the logs needed to establish an audit trail of administrator, user and transaction activity and sufficient to reconstruct security-relevant events occurring on, performed by and passing through TIC systems and components. Note: This capability is intended for immediate, online access in order to trace session connections and analyze security-relevant events. In addition, TM.LOG.04 requires retaining logs for an additional period of time either online or offline.	INCLUDED	IMPLEMENTED
TM.LOG.04	Log Retention	The TICAP follows a documented procedure for log retention and disposal, including, but not limited to, administrative logs, session connection logs and application transaction logs. Record retention and disposal schedules are in accordance with the National Archives and Records Administration existing General Records Schedules, in particular Schedule 12, “Communications	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		Records" and Schedule 20, "Electronic Records;" or NARA approved agency-specific schedule. Note: This capability is intended for the management and operation of the TICAP itself, and does not require the TICAP infer or implement retention policies based on the content of TICAP client communications. The originator and recipient of communications through a TICAP remain responsible for their own retention and disposal policies.		
TM.PC.01	TIC Facility	The TIC access points comply with NIST SP 800-53 physical security controls for high impact systems (FIPS 199).	DEFERRED	N/A
TM.PC.02	NOC/SOC Facilities	The TIC management locations, such as a Network Operations Center (NOC) and a Security Operations Center (SOC), comply with NIST SP 800-53 physical security controls for medium impact systems (FIPS 199).	DEFERRED	N/A
TM.PC.03	SCIF Facilities	The TICAP maintains access to an accredited Sensitive Compartment Information Facility (SCIF) that complies with ICD 705, "Sensitive Compartmented Information Facilities."	EXCLUDED	N/A
TM.PC.04	Dedicated TIC Spaces	The TIC access points and TIC management functions, such as NOC/SOC, are located in spaces dedicated for exclusive use or support of the U.S. Government. The space is secured by physical access controls to ensure that TIC systems and components are accessible only by authorized personnel. Examples of dedicated spaces include, but are not	DEFERRED	N/A

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		limited to, secured racks, cages, rooms, and buildings.		
TM.PC.05	Facility Resiliency	The TIC access point is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: - Electrical systems meet or exceed the building, operating and maintenance standards as specified by the GSA Public Buildings Service Standards, PBS-100. - TIC systems and components are connected to uninterruptable power in order to maintain mission and business-essential functions including, but not limited to, TIC systems, support systems and powered telecommunications facilities, including at the DEMARC or MPOE. - Uninterruptable power systems, HVAC and lighting are connected to an on-site, automatic, standby/emergency generator capable of operating continuously (without refueling) for at least 24 hours.	DEFERRED	N/A
TM.PC.06	Geographic Diversity	The Multi-Service TICAP has geographic separation between its TIC access points, with at least 10 miles separation recommended. It is also recommended that single-agency TICAPs have geographic separation between their TIC access points.	INCLUDED	IMPLEMENTED
TM.TC.01	Route Diversity	The TIC access point follows the National Communications System (NCS) recommendations for Route Diversity, including at least two physically separate points of entry at the TIC access point and physically	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		separate cabling paths to an external telecommunications provider or Internet provider facility.		
TM.TC.02	Least Functionality	TIC systems and components in the TIC access point are configured according to the principal of "least functionality," in that they provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services.	INCLUDED	IMPLEMENTED
TM.TC.03	IPv6	All TIC systems and components of the TIC access point support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22 and Federal CIO memorandum “Transition to IPv6.” - The TICAP supports both IPv4 and IPv6 addresses and can transit both native IPv4 and native IPv6 traffic (i.e. dual-stack) between external connections and agency internal networks. The TICAP may also support other IPv6 transit methods such as tunneling or translation. - The TICAP ensures that TIC access point systems implement IPv6 capabilities (native, tunneling or translation), without compromising IPv4 capabilities or security. IPv6 security capabilities should achieve at least functional parity with IPv4 security capabilities.	INCLUDED	GAP
TM.TC.04	DNS Authoritative Servers	The TIC access point supports hosted DNS services, including DNSSEC, for TICAP client domains. The TICAP configures DNS services in accordance with, but not limited to, the following recommendations from NIST	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		SP 800-81 Rev 1: 1. The TICAP deploys separate authoritative name servers from caching (also known as resolving/recursive) name servers or an alternative architecture preventing cache poisoning. 2. The TICAP implements DNSSEC by meeting NIST SP 800-81 Rev 1 for key generation, key storage, key publishing, zone signing and signature verification.		
TM.TC.05	Response Authority	The TICAP maintains normal delegations and devolution of authority to ensure essential incident response performance to a no-notice event. This includes, but is not limited to, terminating, limiting or modifying access to external connections, including to the Internet, based on documented criteria, including when advised by US-CERT.	INCLUDED	IMPLEMENTED
TM.TC.06	TIC Staffing	The TIC management location, such as a Network Operations Center (NOC) and/or Security Operations Center (SOC), is staffed 24x7. On-scene personnel are qualified and authorized to initiate appropriate technical responses, including when external access is disrupted.	INCLUDED	IMPLEMENTED
TM.TC.07	Response Access	TICAP Operations personnel have 24x7 physical or remote access to TIC management systems which control the TIC access point devices. Using this access, TICAP operations personnel can terminate, troubleshoot or repair external connections, including to the Internet, as required.	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
TO.MG.01	System Inventory	The TICAP develops, documents, and maintains a current inventory of all TIC information systems and components, including relevant ownership information.	INCLUDED	IMPLEMENTED
TO.MG.02	Change & Configuration Management	The TICAP follows a formal configuration management and change management process to maintain a proper baseline.	INCLUDED	IMPLEMENTED
TO.MG.03	Change Communication	The TICAP communicates all changes approved through the formal configuration management and change management processes to customers, as defined in SLAs or other authoritative documents.	DEFERRED	N/A
TO.MG.04	Contingency Planning	The TICAP maintains an Information Systems Contingency Plan (ISCP) that provides procedures for the assessment and recovery of TIC systems and components following a disruption. The contingency plan should be structured and implemented in accordance with NIST SP 800-34 Rev 1.	INCLUDED	IMPLEMENTED
TO.MG.05	TSP	The TICAP has telecommunications service priority (TSP) configured for external connections, including to the Internet, to provide for priority restoration of telecommunication services.	DEFERRED	N/A
TO.MG.06	Maintenance Scheduling	The TICAP employs a formal technical review process to schedule, conduct, document and communicate maintenance and repairs. The TICAP maintains maintenance records for TIC systems and components. The intent of this capability is to minimize	DEFERRED	N/A

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		downtime and operational impact of scheduled maintenance and outages.		
TO.MG.07	Network Inventory	The TICAP maintains a complete map, or other inventory, of all customer agency networks connected to the TIC access point. The TICAP validates the inventory through the use of network mapping devices. Static translation tables and appropriate points of contact are provided to US-CERT on a quarterly basis, to allow in-depth incident analysis.	INCLUDED	IMPLEMENTED
TO.MG.08	Service Level Agreement	The Multi-Service TICAP provides each customer with a detailed Service Level Agreement.	INCLUDED	NOT ASSESSED
TO.MG.09	Tailored Service Level Agreement	The Multi-Service TICAP provides an exception request process for individual customers.	INCLUDED	NOT ASSESSED
TO.MG.10	Tailored Security Policies	The Multi-Service TICAP accommodates individual customer agencies' security policies and corresponding security controls, as negotiated with the customer.	INCLUDED	NOT ASSESSED
TO.MG.11	Tailored Communications	The Multi-Service TICAP accommodates tailored communications processes to meet individual customer requirements.	INCLUDED	NOT ASSESSED
TO.MON.01	Situational Awareness	The TICAP maintains situational awareness of the TIC and its supported networks as needed to support customer security requirements. Situational awareness can be achieved by correlating data from multiple sources, multiple vendors, and multiple types of data by using, for example, Security Incident & Event Management (SIEM) tools.	DEFERRED	N/A

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
TO.MON.02	Vulnerability Scanning	At a minimum, the TICAP annually conducts and documents a security review of the TIC access point and undertakes the necessary actions to mitigate risk to an acceptable level (FISMA, FIPS 199 and FIPS 200). Vulnerability scanning of the TIC architecture is a component of the security review.	INCLUDED	IMPLEMENTED
TO.MON.03	Audit Access	The TICAP provides access for government authorized auditing of the TIC access point, including all TIC systems and components. Authorized assessment teams are provided access to previous audit results of TIC systems and components, including but not limited to, C&A and ICD documentation.	INCLUDED	IMPLEMENTED
TO.MON.04	Log Sharing	The TICAP monitors and logs all network services where possible, including but not limited to, DNS, DHCP, system and network devices, web servers, Active Directory, Firewalls, NTP, and other Information Assurance devices/tools. These logs can be made available to US-CERT on request.	INCLUDED	IMPLEMENTED
TO.MON.05	Operational Exercises	The TIC Access Provider participates in operational exercises that assess the security posture of the TIC. The lessons learned from operational exercises are incorporated into network defenses and operational procedures for both the TICAP and its customers.	INCLUDED	IMPLEMENTED
TO.REP.01	Customer Service Metrics	The TICAP collects customer service metrics about the TIC access point, and reports them to its customers,	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		DHS, and/or OMB as required. Examples of customer service metrics include, but are not limited to, performance within SLA provisions, issue identification, issue resolution, customer satisfaction, and quality of service.		
TO.REP.02	Operational Metrics	The TICAP collects operational metrics about the TIC access point, and reports them to its customers, DHS, and/or OMB as requested. Examples of operational metrics include, but are not limited to, performance within SLA provisions, network activity data (including normal and peak usage), and improvement to customer security posture.	INCLUDED	IMPLEMENTED
TO.REP.03	Customer Notification	The Multi-Service TICAP reports threats, alerts, and computer security-related incidents and suspicious activities that affect a subscribing agency to the subscribing agency.	INCLUDED	IMPLEMENTED
TO.REP.04	Incident Reporting	The TICAP reports incidents to US-CERT in accordance with federal laws, regulations and guidance.	INCLUDED	IMPLEMENTED
TO.RES.01	Response Timeframe	The TICAP has a documented and operational incident response plan in place that defines actions to be taken during a declared incident. In the event of a declared incident or notification from US-CERT, TICAP operations personnel immediately activate incident response plan(s). TICAP operations personnel report operational status to US-CERT within two hours and continue to report based on US-CERT direction.	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
TO.RES.02	Response Guidance	TIC operations personnel acknowledge, implement, and document tactical threat and vulnerability mitigation guidance provided by US-CERT.	INCLUDED	IMPLEMENTED
TO.RES.03	Denial of Service Response	The TICAP manages filters, excess capacity, bandwidth or other redundancy to limit the effects of information flooding types of denial of service attacks on the organization's internal networks and TICAP services. The TICAP has agreements with external network operators to reduce the susceptibility and respond to information flooding types of denial of service attacks. The Multi-Service TICAP mitigates the impact on non-targeted TICAP clients from a DOS attack on a particular TICAP client. This may included diverting information flooding types of denial of service attacks targeting a particular TICAP client in order to maintain service to other TICAP clients.	INCLUDED	IMPLEMENTED
TS.CF.01	Application Layer Filtering	The TIC access point uses a combination of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means to implement inbound and outbound application layer filtering. The TICAP will develop and implement a risk-based policy on filtering or proxying new protocols.	INCLUDED	IMPLEMENTED
TS.CF.02	Web Session Filtering	The TIC access point filters outbound web sessions from TICAP clients based on, but not limited to: web content, active content, destination URL pattern, and IP address. Web	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		filters have the capability of blocking malware, fake software updates, fake antivirus offers, phishing offers and botnets/keyloggers calling home.		
TS.CF.03	Web Firewall	The TIC access point filters inbound web sessions to web servers at the HTTP/HTTPS/SOAP/XML-RPC/Web Service application layers from, but not limited to, cross site scripting (XSS), SQL injection flaws, session tampering, buffer overflows and malicious web crawlers.	INCLUDED	IMPLEMENTED
TS.CF.04	Mail Filtering	The TIC access point performs malware scanning, filters content, and blocks spam-sending servers as specified by NIST 800-45, "Guidelines for Electronic Mail Security," for inbound and outbound mail. These TIC access point protections are in addition to malware scanning and content filtering performed by the agency's mail servers and end user's host systems. The TICAP takes agency specified actions for potentially malicious or undesirable mail, including at least the following actions: block messages, tag undesirable content, sanitize malicious content, and deliver normally. Multi-Service TICAPs tailor their malware and content filtering services for individual agency mail domains.	INCLUDED	NOT ASSESSED
TS.CF.05	Agency Specific Mail Filters	The TIC access point uses an agency-specified custom-processing list with at least the combinations of senders, recipients, network IP addresses or host names. The agency specified custom-processing list has custom TICAP malware and content filtering	INCLUDED	NOT ASSESSED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		actions. Mail allowed by an agency-specified custom-processing list is still scanned by the TICAP for malware or undesirable content and tagged if found. Multi-Service TICAPs tailor their malware and content filtering services for individual agency mail domains.		
TS.CF.06	Mail Forgery Detection	For email received from other agency mail domains known to have domain-level sender authentication (for example Domain Keys Identified Mail or Sender Policy Framework) the TIC access point includes the results of the domain-level sender forgery analysis when determining potentially suspicious or undesirable email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Scoring criteria for this capability will be aligned with the National Strategy for Trusted Identities in Cyberspace (NSTIC). The TICAP takes agency specific actions for email determined to be suspicious or undesirable.	INCLUDED	NOT ASSESSED
TS.CF.07	Digitally Signing Mail	For email sent to other agency mail domains, the TICAP ensures the messages have been digitally signed at the Domain Level (for example Domain Keys Identified Mail) in order to allow receiving agencies to verify the source and integrity of email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Signing procedures will be in alignment with the National Strategy	INCLUDED	NOT ASSESSED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		for Trusted Identities in Cyberspace, and may occur at the bureau or agency sub-component level instead of the TIC access point.		
TS.CF.08	Mail Quarantine	The TICAP quarantines mail categorized as potentially suspicious while the agency's mail domain reviews and decides what action to take. The agency's mail domain can take at least the following actions: block the message, deliver the message, sanitize malicious content and tag undesirable content. Note: this is intended to be an additional option which agency mail operators can specify with capability TS.CF.04. It does not require agencies to quarantine potentially suspicious mail.	INCLUDED	NOT ASSESSED
TS.CF.09	Crypto-graphically authenticated protocols	The TICAP validates routing protocol information using authenticated protocols. The TICAP configures Border Gateway Protocol (BGP) sessions in accordance with, but not limited to, the following recommendation from NIST SP 800-54: BGP sessions are protected with the MD5 signature option. NIST and DHS are collaborating on additional BGP robustness mechanisms, and plan to publish future deployment recommendations and guidance.	INCLUDED	IMPLEMENTED
TS.CF.10	Reduce the use of clear-text management protocols	The TIC access point limits and documents the use of unauthenticated, clear text protocols for TIC management and will phase out such protocols or enable cryptographic authentication where technically and operationally feasible.	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
TS.CF.11	Encrypted Traffic Inspection	The TICAP has a documented procedure or plan that explains how it inspects and analyzes encrypted traffic. The document includes a description of defensive measures taken to protect TICAP clients from malicious content or unauthorized data exfiltration when traffic is encrypted. The TIC access point analyzes all encrypted traffic for suspicious patterns that might indicate malicious activity and logs at least the source, destination and size of the encrypted connections for further analysis.	DEFERRED	N/A
TS.CF.12	User Authentication	The TICAP has a documented procedure or plan that explains how it inspects and analyzes connections by particular TICAP client end-users or host systems which have custom requirements for malware and content filtering. Connection content is still scanned by the TICAP for malware or undesirable content and logged by the TICAP when found.	DEFERRED	N/A
TS.CF.13	DNS Filtering	The TIC access point filters DNS queries, and performs validation of DNS Security Extensions (DNSSEC) signed domains, for TICAP clients. The TICAP configures DNS resolving/recursive (also known as caching) name servers in accordance with, but not limited to, the following recommendations from NIST SP 800-81 Revision 1 (Draft): 1. The TICAP deploys separate recursive name servers from authoritative name servers to prevent cache poisoning. 2. The TICAP filters DNS queries for known malicious domains.	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		3. The TICAP logs at least the query, answer, and client identifier.		
TS.INS.01	NCPS	The TIC access point participates in the National Cyber Protection System (NCPS, operationally known as Einstein).	INCLUDED	NOT ASSESSED
TS.INS.02	IDS/NIDS	The TIC access point passes all inbound/outbound network traffic through Network Intrusion Detection Systems (NIDS) configured with custom signatures, including signatures for the application layer. This includes, but is not limited to, critical signatures published by US-CERT.	DEFERRED	N/A
TS.PF.01	Secure all TIC traffic	All external connections are routed through a TIC access point, scanned and filtered by TIC systems and components according to the TICAP's documented policy, which includes critical security policies when published by US-CERT. The definition of "external connection" is in accordance with the TIC Reference Architecture, Appendix A (Definition of External Connection).	INCLUDED	IMPLEMENTED
TS.PF.02	Default Deny	By default, the TIC access point blocks network protocols, ports and services. The TIC access point only allows necessary network protocols, ports or services with a documented mission requirement and approval.	DEFERRED	N/A
TS.PF.03	Stateless Filtering	The TIC access point implements stateless blocking of all inbound and outbound connections without being limited by connection state tables of TIC systems and components.	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		Attributes inspected by stateless blocks include, but are not limited to: - Direction (inbound, outbound, interface) - Source and destination IPv4/IPv6 addresses and network masks - Network protocols (TCP, UDP, ICMP, etc.) - Source and destination port numbers (TCP, UDP) - Message codes (ICMP)		
TS.PF.04	Stateful Filtering	By default, the TIC access point blocks unsolicited inbound connections. For authorized outbound connections, the TIC access point implements stateful inspection that tracks the state of all outbound connections and blocks packets that deviate from standard protocol state transitions. Protocols supported by stateful inspection devices include, but are not limited to: - ICMP (errors matched to original protocol header) - TCP (using protocol state transitions) - UDP (using timeouts) - Other Internet protocols (using timeouts) - Stateless network filtering attributes	INCLUDED	IMPLEMENTED
TS.PF.05	Filter by Source Address	The TIC access point only permits outbound connections from previously defined TICAP clients using Egress Source Address Verification. It is recommended that inbound filtering rules block traffic from packet source addresses assigned to internal networks and special use addresses (IPv4-RFC5735, IPv6-RFC5156).	DEFERRED	N/A
TS.PF.06	Asymmetric Routing	The TIC access point stateful inspection devices correctly process traffic returning through asymmetric	INCLUDED	IMPLEMENTED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		routes to a different TIC stateful inspection device; or documents how return traffic is always routed to the same TIC access point stateful inspection device.		
TS.PF.07	FedVRE (H.323)	The TIC access point supports Federal Video Relay Service (FedVRS) for the Deaf (www.gsa.gov/fedrelay) network connections, including but not limited to devices implementing stateful packet filters. Please refer to http://www.fedvrs.us/supports/technical for FedVRS technical requirements. Agencies may document alternative ways to achieve reasonable accommodation for users of FedVRS.	EXCLUDED	N/A
TS.RA.01	Agency-User Remote Access	The TIC access point supports telework/remote access for TICAP client authorized staff and users using ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. This capability is not intended to include permanent VPN connections for remote branch offices or similar locations. In addition to supporting the requirements of OMB M-06-16, “Protection of Sensitive Agency Information," the following baseline capabilities are supported for telework/remote access at the TIC Access Point: 1. The VPN connection terminates behind NCPS and full suite of TIC capabilities which means all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected by NCPS. 2. The VPN connection terminates in front of TICAP-managed security controls including, but not limited to, a	INCLUDED	NOT ASSESSED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected. 3. NIST FIPS 140-2 validated cryptography is used to implement encryption on all VPN connections (see NIST SP 800-46 Rev1). 4. Split tunneling is not allowed (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of NCPS. 5. Multi-factor authentication is used (see NIST SP 800-46 Rev1, OMB M-11-11). 6. VPN concentrators and Virtual-Desktop/Application Gateways use hardened appliances maintained as TICAP network security boundary devices. 7. If telework/remote clients use Government Furnished Equipment (GFE), the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways. 8. If telework/remote clients use non-GFE, the VPN connection uses only access through specific Virtual Desktops/Application Gateways. TICAP clients may support additional telework/remote access connections for authorized staff and users using equivalent agency-managed security controls at non-TIC Access Point locations. The agency-level NOC/SOC is responsible for maintaining the inventory of additional telework/remote access connections and coordinating agency-managed security controls.		

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		Because of the difficulty verifying the configuration, sanitizing temporary and permanent data storage, and analyzing possible compromises of non-Government Furnished Equipment, it is the agency's responsibility to document in accordance with OMB M-07-16 if sensitive data may be accessed remotely using non-GFE, and informing the TIC Access Provider of the appropriate security configuration policies to implement.		
TS.RA.02	External Dedicated Access	The TIC access point supports dedicated external connections to external partners (e.g., non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities are supported for external dedicated VPN and private line connections at the TIC Access Point: 1. The connection terminates in front of NCPS to allow traffic to/from the external connections to be inspected. 2. The connection terminates in front of the full suite of TIC capabilities to allow traffic to/from external connections to be inspected. 3. VPN connections use NIST FIPS 140-2 validated cryptography over shared public networks, including the	INCLUDED	NOT ASSESSED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		Internet. 4. Connections terminated in front of NCPS may use split tunneling.		
TS.RA.03	Extranet Dedicated Access	The TIC access point supports dedicated extranet connections to internal partners (e.g., TIC federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other internal networks. The following baseline capabilities are supported for extranet dedicated VPN and private line connections at the TIC Access Point: 1. The connection terminates behind NCPS and full suite of TIC capabilities which means all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected by NCPS. 2. The connection terminates in front of TICAP-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected. 3. VPN connections use NIST FIPS 140-2 validated cryptography over shared public networks, including the Internet. 4. Split tunneling is not allowed. Any VPN connection that allows split tunneling is considered an external connection, and must terminate in front	INCLUDED	NOT ASSESSED

FedRAMP -TIC Capabilities Version 2.0			PILOT ASSESSMENT	ASSESSMENT STATUS
ID	**SUMMARY**	**CAPABILITY DEFINITION**		
		of NCPS. TICAP clients may support dedicated extranet connections with internal partners using equivalent agency-managed security controls at non-TIC Access Point locations. The agency-level NOC/SOC is responsible for maintaining the inventory of extranet connections with internal partners and coordinating agency-managed security controls.		

Notes

[1] https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf

[2] https://www.fedramp.gov/files/2015/04/Description-FT-Overlay.docx

[3] https://www.fedramp.gov/draft-fedramp-tic-overlay/