# The FedRAMP-TIC Overlay

**Overview**

The Department of Homeland Security (DHS), in collaboration with the Federal Risk Authorization Management Program (FedRAMP) Program Management Office (PMO), has developed a DRAFT overlay for the Trusted Internet Connection (TIC) with the FedRAMP requirements. This DRAFT overlay is the first step in updating TIC’s current reference architecture to allow agencies greater flexibility as they move to securely adopt cloud solutions. It is the first overlay the FedRAMP PMO is releasing as part of FedRAMP Forward. Once finalized, it will allow agencies to ensure cloud services they use both meet FedRAMP requirements and have all capabilities needed for agencies to meet the TIC Initiative. The coordination of these two programs will provide for the security of data within cloud environments and the security of the network connections between agency networks and cloud services.

**Background**

TIC Initiative

OMB Memo M-08-05 created the TIC Initiative in 2008. The intent of this initiative is to optimize and standardize how the Federal government secures external network connections including connections to the Internet. The initiative improves the Federal government's security posture and incident response capabilities by reducing and consolidating the total number of external connections as well as by providing enhanced monitoring and awareness external connections.

The TIC Initiative released a TIC Reference Architecture v2.0 that helps clarify the TIC strategic goals and how agencies can meet the TIC Initiative. The TIC Strategic Goals include:

1. Reduce and consolidate external access points across the federal enterprise,
2. Manage the security requirements for Network and Security Operations Centers (NOC/SOC) for incident response capabilities, and
3. Establish a compliance program to monitor department and agency adherence to TIC policy.

In order to meet these three goals, agencies must reduce the number of external connections to their networks and ensure all external connections enforce TIC capabilities at the perimeter of their networks to monitor and provide for the security of Federal data. The TIC Reference Architecture v2.0, defines e 74 capabilities in technical, management, and operational capacities. Currently, DHS verifies these capabilities at the external network perimeter for agencies at external network perimeters in one of three ways:

1. An agency can implement the capabilities on their own perimeter of external connections and become an agency designated as TIC Access Provider (TICAP);
2. Procure external network connections and security of their network perimeter through commercial carriers designated as Managed Trusted IP Service (MTIPS) providers through the GSA Networx Contract; or
3. Work with another agency designated as a TICAP to leverage their external connections perimeter security.

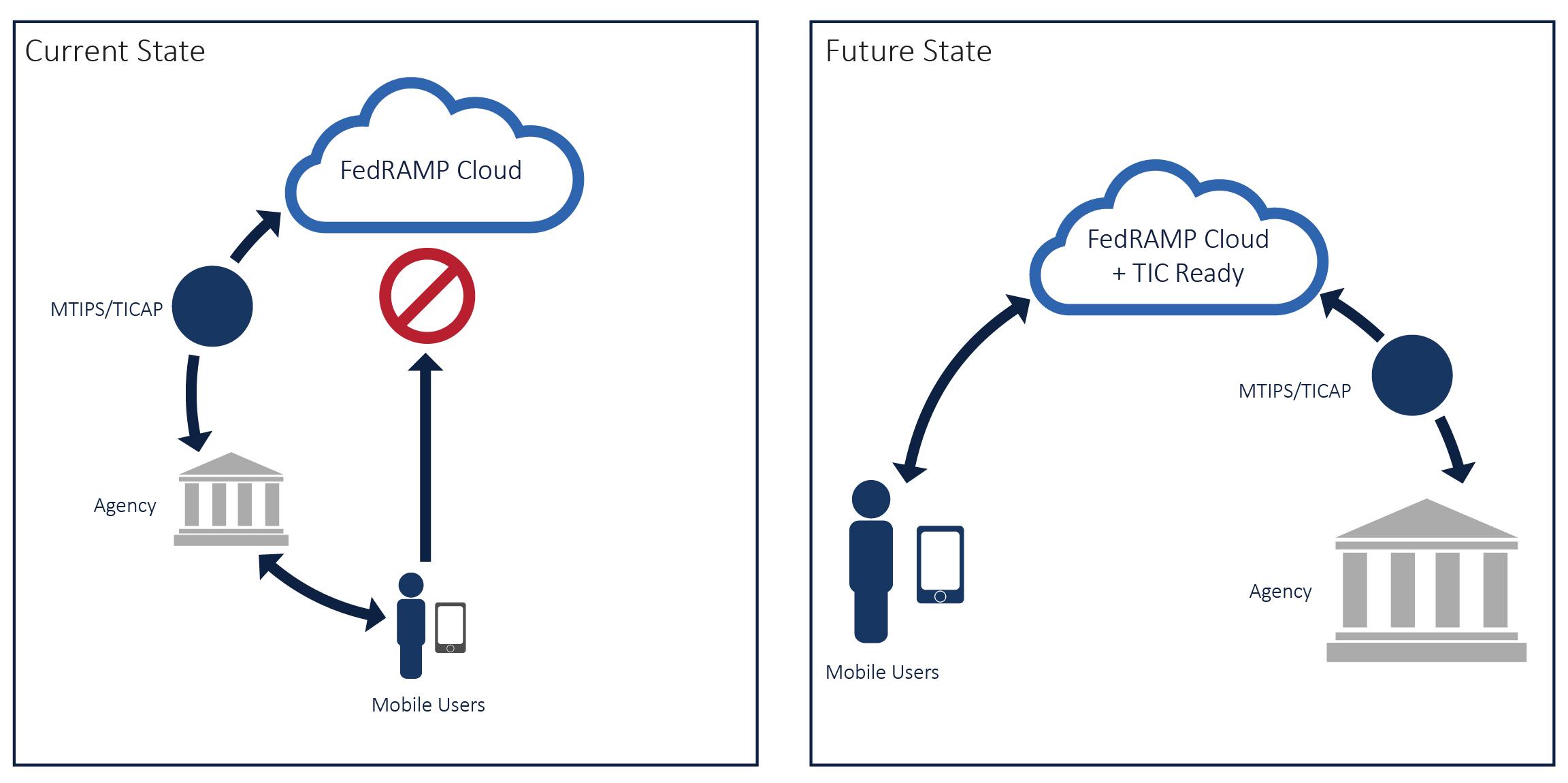
FedRAMP

OMB Memo “Security Authorization of Information Systems in Cloud Computing Environments” established FedRAMP in in December of 2011. The goal of FedRAMP is to accelerate the adoption of secure cloud solutions and ensure consistent application of the Federal Information Security Management Act (FISMA) on cloud systems to enable re-use of security authorizations across the US Government. All agencies are required to use the FedRAMP security requirements and framework when procuring and using any cloud services.

FedRAMP security requirements are based on the NIST 800 series Special Publications (SP). In order to receive a FedRAMP security authorization, Cloud Service Providers (CSPs) must document, implement, and be assessed against the baseline FedRAMP security controls, which are a selection of the NIST SP 800-53 (as revised) security controls.

**Purpose**

Currently the only way a Federal user can connect to a FedRAMP compliant cloud and comply with TIC is to do so from an agency network. With the increasing number of mobile users connecting (e.g. via smart phones, tablets) to cloud services, these mobile users must route their connection through their agency network and then through a MTIPS or TICAP connection. This creates significant strains on agency networks and eliminates one of the key benefits of using a cloud: ubiquitous access.

The FedRAMP PMO and the TIC Initiative have worked together to determine a way for agency mobile users to directly access cloud services without having to use a TICAP or MTIPS connection. This new approach uses the FedRAMP framework to allow CSPs to demonstrate their ability to provide the TIC required controls, which enables agencies to enforce the TIC capabilities. To do this, the TIC capabilities have been mapped to the FedRAMP security controls through a DRAFT FedRAMP-TIC Overlay. CSPs will be able to use this overlay during a FedRAMP security assessment to prove they can t provide agencies with the ability to enforce TIC capabilities for mobile users. This will allow agencies to be confident that if they authorize a CSP that has undergone a FedRAMP assessment with the TIC Overlay, the cloud service is “TIC Ready” and the agency can fully enforce TIC independently of how users connect to the cloud. CSPs that undergo a FedRAMP security assessment with the FedRAMP-TIC overlay would be able to:

1. Document how the FedRAMP security requirements are met;
2. Document how TIC capabilities for Federal customers coming from an Agency network and supported alternatives for mobile users are met;
3. Undergo one combined assessment to demonstrate compliance with both FedRAMP and TIC;
4. Have that combined TIC/FedRAMP assessment be completed by a FedRAMP accredited 3PAO;
5. Achieve a FedRAMP security authorization by an authorizing official (agency or JAB) based on the 3PAO Security Assessment Report; and
6. Be deemed “TIC Ready” by DHS based on DHS’s review of a 3PAO TIC Capabilities Assessment Report.

**Request for Comment**

The FedRAMP PMO and TIC Initiative are jointly requesting feedback on the DRAFT FedRAMP-TIC Overlay. We would like to ensure that CSPs have the ability to provide the capabilities as mapped.

The release of this DRAFT overlay is the first step in providing finalized guidance for the ultimate completion of a FedRAMP-TIC overlay. The TIC Initiative will be working concurrently with Federal Departments and Agencies through the ISIMC under the CIO Council to vet these requirements and make any necessary updates to the TIC Reference Architecture v2.0 over the coming months.

All feedback should be provided in the documents as described below and should be mailed to [info@fedramp.gov](mailto:info@fedramp.gov) with the subject line: “FedRAMP-TIC Overlay Feedback.” The feedback period will be for 30 days from March xx the April xx. **All feedback must be submitted by 5pm EST on April xx.**

**Documents For Review**

TIC Reference Architecture v2.0

This document is included in order to provide context to the TIC Initiative as well as provide the specific TIC capabilities that have been mapped to the FedRAMP security controls baseline.

FedRAMP Security Controls Baseline

This document is provided in order to provide context to the FedRAMP security controls as well as provide the baseline of controls the TIC capabilities were mapped to.

FedRAMP-TIC Overlay Spreadsheet

The FedRAMP-TIC Overlay Spreadsheet maps the applicable TIC capabilities within the TIC Reference Architecture v2.0 to the FedRAMP Security Controls Baseline, currently for low and moderate impact levels. The spreadsheet has three tabs:

1. README Tab

This tab provides definitions of each column with the “FedRAMP to TIC Mapping” and “TIC to FedRAMP Mapping” tabs. Additionally it provides a list of relevant acronyms or other terms.

1. FedRAMP to TIC Mapping

This is a mapping of the FedRAMP controls to the TIC capabilities. It is provided as a reference so reviewers can see how the FedRAMP controls map to the TIC capabilities in the context of the TIC program and assessments.

1. TIC to FedRAMP Mapping

**All comments should be provided in this tab.** This is the key tab for reviewers. It identifies which controls map to TIC capabilities and specifies what a CSP must implement in order to demonstrate their ability to meet these capabilities through a FedRAMP assessment. Some notes on the mapping:

* + Not all TIC capabilities are represented in the FedRAMP-TIC overlay as not all TIC capabilities are applicable to CSPs.
  + The TIC capabilities and the FedRAMP security control requirements are not a one-to-one mapping; some are one-to-many, many-to-one, or many-to-many.
  + The TIC Reference Architecture v2.0 defines TIC capabilities as either Recommended or Critical. For purposes of this overlay, ALL applicable TIC capabilities are considered Critical (and therefore mandatory) for external cloud service providers.