

# **Trusted Internet Connection (TIC) and the Cloud Draft Talking Points**

**Draft 3a  
6/14/10**

## Program Mission:

Government-wide optimization of individual federal agency network services into a common federal government solution.

## Objectives:

1. Reduce and consolidate external connections through TIC Access Providers (TICAPs)
2. Develop and maintain baseline technical requirements for TICAP Network and Security Operation Centers (NOC/SOC)
3. Oversee federal agency transition to approved TICAPs
4. Maintain relationships with Agencies and stay informed with their concerns, including TIC Compliance Validations (TCVs)

- One of the Trusted Internet Connection (TIC)'s key responsibilities is detecting "advanced persistent threats" and eventual preventing "data ex-filtration" of government data by external entities.
  - Other TIC goals include government-wide situational awareness, preventing disruption of government operations, providing defense-in-depth.
- The TIC Program Office's initial focus is detecting anomalies, future plans included prevention (Einstein, operated by US-CERT)
- Agencies continue to have primary responsibility for their own IT security; some aspects of TIC add capabilities for prevention, auditing, and reporting.
- Unrestricted data systems may be outside of the TIC, unless they cross a federal network boundary
  - Unrestricted data is described as government data fully and freely available to all, and excludes "For Official Use", personally identifying information, etc.
  - Covert channels within unrestricted data flows is a concern.
- TIC Program Office focus is on demonstrable capabilities, not a particular architecture or implementation
- Data flows within the government entities and between trusted government entities do not need to pass through a TIC
  - Internal communications is the largest volume of traffic, and TIC would like to keep to the minimum what need to be inspected.

# Trusted Internet Connection Requirements

GSA

TIC Requirement	Cloud Impact
Identifying and Monitoring restrictive data moving between USGov and external entities	Cloud installations need to: <ul style="list-style-type: none"><li>• Analyze the paths data can take to and from agencies</li><li>• Identify logically separate, and provide TIC PO with data feeds from USGov to external entities</li><li>• Locate government connections and monitor traffic.</li></ul> Any communication/network channels from government tenants to external entities/co-tenants (considered as external channels) need to be provided to TIC
Exclude inspection of data moving purely between external entities	Logically exclude external-to-external co-tenant data from TIC inspection
If possible, exclude inspection of data moving within an agency or in most cases between agencies	Logically exclude undesired intra-agency data from TIC inspection

**None of these requirements require a specific architecture or purely physical separation, and all could be met in a variety of innovative ways by different vendors**

# TIC Challenges for Cloud Computing

- TIC PO requires data to be inspected, without mandating any specific architecture for doing so
  - Cloud computing is not “ruled out” by any specific TIC requirements
- Cloud computing presents some special challenges to meet TIC requirements
  - All-Government (Community and Private) Clouds
    - Less challenging because all tenants are government agencies
    - Fewer and better defined paths to external entities makes it easier to identify and monitor connections
  - Public (Mixed Government and Commercial) Clouds with unrestricted data
    - “Public” sites may be outside of TIC, so long as all data is unrestricted
    - The current IaaS RFQ is immediately usable for unrestricted data applications
    - Many public-use systems contain some restricted data, such as personally identifying information and therefore must meet TIC requirements
  - Public (Mixed Government and Commercial) Clouds with restricted data
    - The vendor must demonstrate an effective capability to enable TIC inspection, and eventual intrusion prevention, of data between government and non-government co-tenants/entities
    - Includes both external network connections and internal cloud communications with non-government entities
  - The cloud vendor management access requires in special attention within cloud environments

# TIC PO and Cloud PMO Challenges: Strategy and Approach

- Clearly document and disseminate the capabilities TIC requires in the cloud
- Engage industry partners to propose and develop multiple innovative ways to demonstrably meet the requirements
- Pursue interim less-efficient approaches such as dedicated network connections, TIC-enabled mail routers, etc.

DRAFT