Trusted Internet Connection Architecture for Single Service Providers

April, 2009

For further information, questions and comments please contact Cisco Corporate Positioning.
Contents

Executive Summary .................................................. 3
    TIC Internet Gateway Consolidation .................. 3
    Internet Portal Security Architecture ............... 4
Internet Portal Overview ........................................ 6
WAN Consolidation – Challenges for Network Managers ............. 8
    Departments or Agencies with Many Internet Connections ...... 8
Conclusion ..................................................................... 10
Cisco Products for Single Service Provider TICAPs .................... 10
Cisco Product Information ........................................ 14
Executive Summary

In today’s U.S. government, federal agency CIOs are faced with numerous challenges beyond meeting their agency’s mission, including data protection, operational efficiency, regulatory compliance, and cost containment. The Trusted Internet Connection (TIC) initiative, mandated by the Office of Management and Budget (OMB) in November 2007, is one of many requirements that agencies face. Cisco offers solutions specifically designed to help federal agencies meet their important requirements and can help agencies plan and successfully achieve their migration to a TIC-compliant architecture.

Adoption of the TIC initiative will minimize the overall number of Internet connections to the U.S. federal government. This will be accomplished by sharing resources (Internet portals) and creating new intranets to provide access to these Internet portals. This paper provides insight and guidance for agencies that have elected to function as their own TIC Access Provider (TICAP) and to provide access services only to themselves (Single Service TICAP).

Cisco can provide a secure and flexible infrastructure that allows federal agencies to evolve to a highly productive and efficient IT model. The infrastructure enables each user to easily access data anywhere that user resides, using any device that is required – securely and reliably. New modes of collaboration such as high-definition (HD) video, Web 2.0 tools, and a combination of real-time and non-real-time applications demand an infrastructure that is always on and flexible, yet controlled in such a way to deliver critical information on time. A Cisco® framework offers these capabilities and enables federal agencies to meet the new TIC requirements while utilizing their current network investments and readily available components.

Cisco is committed to providing solutions and services to all federal government agencies, now and in the future. Investing over $4 billion annually in research and development, Cisco continues to innovate, whether in the infrastructure with 10-Gbps and 40-Gbps solutions LAN/WAN solutions or in the application space with ultra-high-definition Cisco TelePresence™ video conferencing. Cisco is prepared to bring networking and collaboration to new heights and provide the best support possible in serving our federal government.

TIC Internet Gateway Consolidation

The TIC initiative will improve the federal government’s overall Internet communication situational awareness while providing incident-response capability in the case of an external cyber attack. This is accomplished through the reduction of external connections and the establishment of centralized gateway monitoring at a select group of Trusted Internet Connection Access Providers (TICAPs).

Recently, departments and agencies had to select their preferred type of TICAP by defining themselves as follows:

- **Single Service Provider**: Departments and agencies that propose to function as a TICAP and provide services to customers internal to their organization only. (This paper focuses on solutions for Single Service Provider TICAPs).

- **Multi Service Provider**: Departments and agencies that propose to function as a TICAP and provide shared services to internal customers and customers outside of their own organizations.

- **Seeking Service**: Departments and agencies that propose to receive services from an approved TICAP.
As agencies consolidate and/or remove their Internet connections, two dramatic results emerge. First, the consolidation will require a new Internet portal architecture that meets all security and communication needs for each respective agency, and can be scaled appropriately to support the new loads. Secondly, the new traffic flows will require, at a minimum, agencies to review/renew their routing architecture, and will likely drive them to create an agency TIC backbone for access to these portals.

The remainder of this paper will focus on TIC portals and the interconnecting WAN infrastructure that agencies use to access the portals. Figure 1 demonstrates in generic terms the existing agency Internet connectivity and the new method required TIC compliance.

**Figure 1.** Before and After View of the Impact of TIC on a Generic Agency

**Internet Portal Security Architecture**

As consolidation and modernization efforts continue to challenge the federal government, the TIC initiative provides direction for how the government can reduce its exposure to cyber threats while increasing situational awareness. The goal of reducing the number of portals within departments has been underway for some time. Portals provide a common framework for access to the federal government, regardless of the systems (legacy or modernized) that may be accessed via the portal.

Portals can be defined in many ways. They control access to resources and data based on the rights of the user. Within a portal, functionality is integrated into a system architecture that satisfies the requirements and provides the utmost protection of the data that is accessed via the portal. Portals also support objectives such as security, management, connecting similar and disparate systems, and bridging distant functions.

Figure 2 depicts common functionality found in a portal.
Figure 2. Conceptual Diagram of Internet Portal Connection

- **Internet connection:** The Internet connection is an exposure point for most agencies. It provides connectivity for external users to access the agency’s Internet portal and for internal users to access the Internet and other business partners. Web traffic (HTTP and HTTP Secure [HTTPS]) are the most prevalent protocols traversing the Internet.

- **WAN termination point:** The first and outermost point of control and contention for access to the portal is the WAN termination point. As a critical component to the overall system, the WAN termination point serves as the first line of defense for the agency.

- **Web portal:** A web portal provides the functions to authenticate and identify its users and provides them with a personalized web interface for accessing information and services. These services can include presentation of static and dynamic information, rendering of customized content, and real-time e-commerce transactions over encrypted sessions. Traditionally, web portals provided external users (such as customers and suppliers) access to an organization’s resources, but they have since evolved to grant employees and contractors access to resources that are typically provided to those connected via intranet or remote VPN connections.

- **Extranet for B2B partners:** An extranet can be defined as a private intranet mapped onto the Internet or some other transport system separated from general public access. These connections are typically approved and accredited connections with a pre-existing security policy based on the mission that the business partner supports within the agency or department. The communications channel is secure and offers the ability to exchange data in a private manner. A demilitarized zone (DMZ) is typically used to stage information for use between organizations while also protecting the actual repositories of information on the intranet.

- **Remote access gateway:** The remote access module can extend the full range of information services to remote offices and teleworkers. Applications such as email, extranet access, video and voice services, and online e-learning classes should all be available to users via the remote access gateway. Extending the office environment to employees’...
alternative work locations allows continuous business operation and provides the flexibility to work from anywhere and at any time.

- **Application awareness**: The system (combination of hardware and software) should provide application-layer protocol translation capabilities. The purpose of this functionality is to further secure application requests and to translate the application protocol to access the data in whatever format it lives within its legacy or existing schema/database.

- **US-CERT Einstein Monitoring**: As mandated by the OMB, TIC Internet portals will be monitored by the US-CERT Einstein program. Einstein does not eliminate the need for intrusion detection and prevention systems; rather, the 24-hour monitoring program aims to provide incidental information collection and situational awareness tools for federal agencies.

### Internet Portal Overview

The security and protection of agency data (including employee information) is of the utmost concern for federal agencies. A shared infrastructure model for the TIC provides scaling and cost efficiencies by using high-performance hardware. However, to provide a high level of security, individual security policies are still required. Virtualization (multiple security policies or contexts supported on the same hardware) makes this possible. There are too many variables to accommodate multiple agencies or communities of interest with a single security policy. Security policies must be very granular and tailored to specific agency traffic characteristics in order to provide adequate security.

Consolidating many Internet connections and portals into a single portal will require network flexibility and agility. This is especially true when Internet portals will support other agencies, sub-agencies, and various communities of interest. Network components must be able to act in a coordinated fashion to protect assets.

**Figure 3. Internet Portal Solution**
Depicted in Figure 3, the Internet portal solution provides defense in layers by decoupling the Internet portal into sub-components, each with discrete security capabilities and components. Grouping the similar attributes or requirements into their own security zones reduces the overall exposure to threats as fewer protocols are open for Internet scrutiny.

At the top layer, Internet access routers provide connectivity to and from the Internet. In addition, they serve as a first layer of perimeter defense. In that capacity, they provide the preliminary screening of traffic in and out of the Internet portal by filtering out certain data and denying address-spoofing traffic. These routers can provide the first-level alert system, using NetFlow information, which baselines traffic patterns and detects traffic anomalies when they occur.

The next layer of the model contains the security zones where dissimilar security policies are separated into respective zones, and where those policies can be enforced. Traffic associated with communities of interest is sent to specific zones. Component virtualization provides the basis for having zones of varying policies and configurations, integrated in a single system. Each zone can be enabled to allow different policies based on the needs and requirements of that community of interest. By leveraging the virtualization capabilities, a security administrator can segment logical networks into multiple zones, with a single physical infrastructure.

In this model, each zone supports its own security policy, interfaces, routing tables, firewall, intrusion prevention, and deep packet inspection system. Multi-tier service-level agreements can be created by allocating and guaranteeing hardware resources for each zone. A true benefit of this architecture is the ability to deploy, create, and modify policy-based services dynamically to meet critical demands.

Today’s advanced viruses and Trojan horses require measures beyond the protection offered by firewalls and intrusion prevention system (IPS) devices alone. To address this need for security inside the perimeter, a third layer of defense is introduced where advanced application-level security appliances are coupled with security zones to increase the effectiveness of security measures. Following are some specific examples that demonstrate this point:

- To secure email exchanges, appliances such as the Cisco IronPort® Email Security Appliance can be used in conjunction with antivirus gateways to reduce spam, viruses, spyware, and phishing attacks directed at an email security zone.
- By coupling Cisco’s Network Admission Control service and IP Security (IPsec) VPN concentrators with the B2B connections, agencies can enforce security posture policies such as OS version, hot-fix level, and antivirus signature updates, and can ensure the integrity and confidentiality of the connections.
- To secure the web portal where critical protection is needed at the service perimeter between un-trusted and trusted zones, a Cisco ACE XML Gateway with the integrated XML firewall should be used. An XML gateway provides a comprehensive XML threat defense system where it protects against identity, content-based, personnel, response-compliance, message-transport, and XML denial-of-service (DoS) attacks. In addition, it integrates easily with existing infrastructure such as directories, Single Sign On (SSO), Public Key Infrastructure (PKI), and network system management.

A multilayer security design integrates many layers of technology into a single security operation center. System monitoring must provide operators real-time analysis of individual device health and behaviors. A more comprehensive monitoring system, such as Cisco Security Monitoring, Analysis and Response System (MARS), can provide proactive situational awareness of the Internet portal by gathering data from these device information logs, intrusion detection system (IDS), and
firewalls as well as traffic flows from routers. This awareness is critical in making decisions during
an attack or service outage. And as many operators know, many outages are caused by human
error rather than divisive attacks. Therefore, the monitoring system should provide access to audit
compliance capabilities along with fallback tools in the event of misconfiguration.

To summarize, the TIC and the Internet portal requirements will drive changes in security policies
for all government agencies. For some agencies, making some minor modifications to their existing
practices will be enough to meet the TIC mandate, while others may need to revamp a major
portion of their security policies and practices to become compliant. A defense-in-depth strategy
based on a combination of secure connectivity, threat defense, and a trust and identity
management system should be used to mitigate virus outbreaks, prevent unauthorized network
access, and circumvent DoS attacks. This strategy provides safeguards needed to maximize
network uptime and minimize threat impact.

WAN Consolidation – Challenges for Network Managers

While the benefits of a TIC-compliant government are obvious, this initiative will require certain
network modifications for both large and small agencies. In order for the OMB to meet its stated
objective of approximately 50 Internet portals servicing the federal government, many agencies will
need to either consolidate or remove their Internet connections. As mentioned earlier, departments
or agencies will either need to be an Internet portal provider for their organization, be an Internet
portal provider for other departments or agencies, or they must utilize Internet portals from other
providers. It is estimated that over 1000 Internet connections will be removed through this initiative.
Consolidation of these independent connections will require a change to the architecture of each
agency’s WAN connection to accommodate new connectivity or new traffic flows.

Depending on an agency’s existing infrastructure, WAN modifications can be as simple as adding
new routes to the edge routers, or the more extreme case of creating a completely new access
WAN to the new Internet portals. The following sections describe the modifications needed to
facilitate TIC compliance.

Departments or Agencies with Many Internet Connections

In many departments, agencies, and sub-agencies, basic Internet connectivity consolidation will
occur with the creation of two main Internet portals at the department level, as shown in Figure 4.
All other Internet connections within the department, including those for sub-agencies, will be
removed. In this scenario, either an existing department backbone will support access to the
Internet portals or a new intranet will be created to facilitate that traffic flow. For example, when the
Department of Defense consolidated its Internet connectivity to 17 Internet point of presence (POP)
sites, it used the NIPRNet as the WAN backbone to provide intranet traffic between agencies and
access to the Internet.

To facilitate a smooth transition to TIC compliance, departments will need to assess current traffic
patterns and model new traffic patterns caused by the removal of the Internet connections. At the
Internet portals, high-speed routers and upgraded Internet connections will be required to handle
the consolidated Internet traffic. An intranet backbone will be needed to facilitate intra-agency
communication and provide onramps for sub-agencies and remote agency sites to the Internet. In
many cases, existing sub-agency networks can remain the same with current WAN implementation
and security strategies. However these new systems will need to be reviewed to ensure that the
impact to security-policy integrity and performance is minimized.
Many agencies’ remote sites utilize the Internet as a cost-effective IP transport for backhauling traffic to their department-level resources. Some small sites and branches also use that same Internet connection for Internet access. For these agencies, TIC compliance means using Internet portal services from their dedicated TICAP solution. In this model, inter-site communication can be supported via the Internet with FIPS-approved encrypted VPNs between sites. However, since the TIC will no longer permit “split tunneling,” all Internet-bound traffic must traverse an agency’s dedicated Internet portal before leaving agency network boundaries.

An alternative is to create an overall agency backbone where all sites are connected virtually and the Internet is accessed via an Internet portal. In either scenario, the impact on these sites includes the creation of one or two hubs to connect all agency sites together in support of an agency backbone. These two hubs are then used as connection points for the remote sites accessing the Internet via the agency’s TICAP. Traffic patterns will be substantially different in this new design, so agencies must perform due diligence before and during the migration process. Security solutions will need to be evaluated and possibly rebuilt to support this dramatically different model.

Figure 5 highlights several options for small agencies that require TIC-compliant Internet access but lack the operational and budget capabilities to own and manage a TIC-compliant Internet portal.
**Figure 5.** Options for TIC-Compliant Internet Portal

**Conclusion**

As federal agencies plan their migration toward compliance with the OMB mandate to consolidate Internet connections and reduce exposure to cyber threats, two architectural challenges must be addressed. First is the consolidation or elimination of these connections, which could require a new, scalable Internet portal architecture that meets all security and communication needs for any agency. Second, the new traffic patterns may require agencies to optimize their routing architecture, and likely compel agencies to create a TIC backbone for access to these portals.

Cisco has proven, deployed solutions available to address the architectural challenges agencies face in complying with OMB’s mandate. Cisco is prepared to support federal agencies in the planning, testing, and deployment of a TIC-compliant architecture.

**Cisco Products for Single Service Provider TICAPs**

The following section presents the Cisco products that align with the TIC requirements per the OMB’s Statement of Capability form. Federal agencies were required to submit this form to identify the type of TIC they intend to deploy and to disclose their technical capabilities relative to the TIC requirements. The following recommendations are for agencies electing to serve as their own TICAP and to deliver services to internal users only (known as the Single Service Provider TICAP).

Cisco recommends the following architecture for the Single Service Provider TICAP (Figure 6).

---

1 Information Systems Security Line of Business (ISS LoB) Statement of Capability form
Table 1 maps the requirements of Single Service Provider TICAPs with the appropriate Cisco solutions.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Priority</th>
<th>Cisco Solution Set</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can the TICAP monitor unencrypted inbound/outbound SMTP messages and filter messages based on, but not limited to: unauthorized/known bad mail source or destination, suspicious text patterns, unauthorized file attachment type, message size, unsigned and undesirable active content, and agency security policy criteria?</td>
<td>Critical</td>
<td>IronPort C Series</td>
<td>Can perform SMTP monitoring, filtering, spam blocking, infection outbreak blocking, various anti-spam techniques, custom lists for whitelists and blacklists, and logging.</td>
</tr>
<tr>
<td>Can the TICAP scan unencrypted inbound/outbound SMTP messages for malware and block infected messages?</td>
<td>Critical</td>
<td>IronPort C Series</td>
<td>Can perform SMTP monitoring, filtering, spam blocking, infection outbreak blocking, various anti-spam techniques, custom lists for whitelists and blacklists, and logging.</td>
</tr>
<tr>
<td>Does the TICAP provide users with the ability to tag potential spam messages, allowing users to create client-based filters?</td>
<td>Critical</td>
<td>IronPort C Series</td>
<td>Can perform SMTP monitoring, filtering, spam blocking, infection outbreak blocking, various anti-spam techniques, custom lists for whitelists and blacklists, and logging.</td>
</tr>
<tr>
<td>Question</td>
<td>Criticality</td>
<td>Product(s)</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can the TICAP manage exception lists for authorized protocols?</td>
<td>Critical</td>
<td>Cisco ASA adaptive security appliance, IPS, Cisco Security MARS, Cisco IOS® Firewall, IronPort S Series, NBAR</td>
<td>Cisco Security MARS used for validation. Network-Based Application Recognition (NBAR) used for protocol inspection in conjunction with policing policies.</td>
</tr>
<tr>
<td>Can the TICAP support session traceability and auditability for 7 days?</td>
<td>Critical</td>
<td>Cisco Security MARS, NetFlow</td>
<td>A properly deployed Cisco Security MARS installation will provide up to 30 days of auditing. In addition, the use of archiving will allow long-term auditing as needed.</td>
</tr>
<tr>
<td>Does the TICAP provide the ability to filter web sessions (HTTP, HTTPS) based on URL and/or direction from US-CERT, regardless of the direction of traffic (inbound/outbound), unless an exception is granted?</td>
<td>Critical</td>
<td>Cisco IOS Firewall, Cisco ASA CSC-SSM (Trend Micro as well as WebSense), IronPort S Series</td>
<td>Cisco IOS Firewall via CLI or Trend Micro services. Cisco ASA via CLI or Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) services. WebSense protocol support for both platforms.</td>
</tr>
<tr>
<td>Can the TICAP filter the content of all proxied web sessions and does the outbound web proxy server filter based on destination URL or IP address, text content of web pages, and/or the presence of active content (such as Java or Active X) based on internal direction and/or direction from US-CERT?</td>
<td>Critical</td>
<td>Cisco ASA, Cisco IOS Firewall, IronPort S Series</td>
<td>Capabilities supported via CLI as well as subscription services (Trend Micro, WebSense, etc.)</td>
</tr>
<tr>
<td>Can the TICAP filter non-proxied traffic unless prior approval is granted?</td>
<td>Critical</td>
<td>Cisco ASA, Cisco IOS Firewall, IronPort S Series</td>
<td>Cisco ASA cut-through proxy, Cisco IOS authentication proxy, IronPort passive proxy/authentication</td>
</tr>
<tr>
<td>Does the TICAP offer the capability for agency customers to recover, retrieve, or release email blocked as spam for inbound/outbound SMTP messages?</td>
<td>Critical</td>
<td>IronPort C Series</td>
<td>Standard services</td>
</tr>
<tr>
<td>Does the TICAP monitor all encrypted SMTP traffic, filtering spam, and conduct a malware scan of all content?</td>
<td>Desired</td>
<td>IronPort C Series</td>
<td>Standard services. <strong>Note:</strong> IronPort provides mail encryption services</td>
</tr>
<tr>
<td>Does the TICAP require authentication to proxies?</td>
<td>Desired</td>
<td>IronPort S Series</td>
<td>Supported</td>
</tr>
<tr>
<td>Does non-proxied traffic require strong authentication and prior approval for https:// sites?</td>
<td>Desired</td>
<td>Cisco ASA, Cisco IOS Firewall, IronPort</td>
<td>AAA services (OTP, AD, etc.) supported for authentication</td>
</tr>
<tr>
<td>Does the TICAP require multifactor authentication for administrative access to all TICAP devices?</td>
<td>Desired</td>
<td>TACACS RADIUS</td>
<td>Supported over a majority of product lines</td>
</tr>
<tr>
<td>Does the TICAP provide stateful packet inspection services?</td>
<td>Critical</td>
<td>Cisco IOS Firewall, ASA</td>
<td>Cisco IOS Firewall as well as ASA supported.</td>
</tr>
<tr>
<td>Does the TICAP have the ability to inspect outbound and inbound encrypted traffic?</td>
<td>Important</td>
<td>Cisco IOS Firewall, ASA</td>
<td>NOTE: Supported as long as IPsec terminates or originates on the respective ASA or Cisco IOS device.</td>
</tr>
<tr>
<td>Does the TICAP provide site-to-site VPN capabilities, including enterprise-to-enterprise customer pass-through VPN capabilities with a formal review and approval process?</td>
<td>Critical</td>
<td>Cisco IOS Easy VPN, GETVPN, Dynamic Multipoint VPN (DMVPN), client</td>
<td>GETVPN and DMVPN are supported on Cisco IOS only.</td>
</tr>
<tr>
<td>Does the TICAP use Deep Packet Inspection (DPI) services for non-proxied but permitted protocols?</td>
<td>Important</td>
<td>Cisco ASA, IPS, IronPort S Series, Cisco IOS Firewall</td>
<td>Various Layer 4–7 protocols/applications supported. Please refer to URLs in the following section for details.</td>
</tr>
<tr>
<td>Can the TICAP host government employee VPN services for Government Furnished Equipment (GFE) with multifactor authentication and Network Access Control (NAC) restrictions, including hosting of partitioned external customer VPN services, allowing customer data management?</td>
<td>Desired</td>
<td>Identity Based Networking Services (IBNS) or NAC with Cisco IOS Firewall or ASA</td>
<td>SSL or IPsec VPN with NAC capabilities; with support for OTP and AAA.</td>
</tr>
<tr>
<td>Question</td>
<td>Criticality</td>
<td>Technology Details</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Does the TICAP correlate data from multiple sources and vendors, and multiple types of data as needed to support customer security requirements?</td>
<td>Critical</td>
<td>Cisco Security MARS; NetFlow, NBAR, syslog</td>
<td>In addition to Cisco Security MARS providing this information, NetFlow, syslog, and NBAR can provide this information to various third-party systems for analysis.</td>
</tr>
<tr>
<td>Does the TICAP use a network intrusion detection system (NIDS)?</td>
<td>Critical</td>
<td>IPS, ASA, Cisco IOS Firewall</td>
<td>Cisco ASA with SSM will provide full functionality with respect to IPS custom signatures.</td>
</tr>
<tr>
<td>Can the TICAP utilize custom IDS signatures?</td>
<td>Critical</td>
<td>IPS, ASA, Cisco IOS Firewall</td>
<td></td>
</tr>
<tr>
<td>Does the TICAP retain log data defined by National Archives and Records Administration (NARA) standards or customer agency requirements?</td>
<td>Critical</td>
<td>Cisco Security MARS</td>
<td>A properly deployed Cisco Security MARS will provide up to 30 days of auditing. In addition, the use of archiving will allow long-term auditing as needed.</td>
</tr>
<tr>
<td>Does the TICAP report on threats and incidents/events to the pertaining agency in accordance with established federal laws, regulations, guidance, and in accordance with customer-specific SLAs and requirements?</td>
<td>Critical</td>
<td>Cisco Security MARS, CiscoWorks Network Compliance Manager (NCM)</td>
<td>The Cisco NMC provides compliance reports and the Cisco Security MARS offers standard and customized reports.</td>
</tr>
<tr>
<td>Does the TICAP supply a means to ensure secure (encrypted) electronic communication between the provider and the customer?</td>
<td>Critical</td>
<td>DMVPN, GETVPN, Cisco IOS Easy VPN, client</td>
<td>GETVPN and DMVPN are supported on Cisco IOS only.</td>
</tr>
<tr>
<td>Does the TICAP have the capability to define customer risk levels in addition to default risk levels pertaining to the agency?</td>
<td>Critical</td>
<td>IPS Risk Rating</td>
<td>IPS Risk Rating allows the customer to allocate specific risk levels depending on a variety of factors.</td>
</tr>
<tr>
<td>Does the TICAP use Host-Based Intrusion Detection (HID) on all TICAP devices providing shared services to TIC customers and for systems hosted on the TIC?</td>
<td>Important</td>
<td>Cisco Security Agent</td>
<td></td>
</tr>
<tr>
<td>Does the TICAP provide FDCC patch distribution services to its subscribers?</td>
<td>Important</td>
<td>Cisco Security Agent</td>
<td>Utilizing Cisco Security Agent, agencies can build an FDCC security policy to ensure compliance with this regulation.</td>
</tr>
</tbody>
</table>

Service-Level Capabilities

<table>
<thead>
<tr>
<th>Question</th>
<th>Criticality</th>
<th>Technology Details</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the TICAP have the ability to collect and provide metrics?</td>
<td>Critical</td>
<td>NetFlow, Cisco IOS IP SLA, NBAR, syslog, RMON</td>
<td>Metrics can be collected and sent to various systems for reports (for example, Cisco Security MARS).</td>
</tr>
<tr>
<td>Can the TICAP provide customers with standard reports of normal and peak network activity?</td>
<td>Critical</td>
<td>Cisco Security MARS</td>
<td>Standard and customized reporting is available.</td>
</tr>
<tr>
<td>Does the TICAP have a formal configuration-management and change-management process per service management framework (ITIL)?</td>
<td>Critical</td>
<td>CiscoWorks NCM</td>
<td></td>
</tr>
<tr>
<td>Operating under a formal configuration-management and change-management process, can the TICAP communicate all changes to customers as defined in the SLA?</td>
<td>Critical</td>
<td>CiscoWorks NCM</td>
<td>CiscoWorks NCM allows agencies to enforce a workflow process of approval prior to making network changes.</td>
</tr>
<tr>
<td>Does the TICAP have the mechanism to make reports available to customers upon request?</td>
<td>Important</td>
<td>Cisco Security MARS, CiscoWorks NCM, Cisco Security Manager</td>
<td>Reports available upon request; customized reporting is also available.</td>
</tr>
<tr>
<td>Does the TICAP have the capability to provide detailed SLAs to each agency or bureau?</td>
<td>Critical</td>
<td>Cisco IOS IP SLA, CiscoWorks NCM, NetFlow Top Talkers</td>
<td>Cisco IOS IP SLA provides various metrics that can be reported by various platforms.</td>
</tr>
</tbody>
</table>
### Cisco Product Information

Additional information about the products and features described in this document can be found at the following websites.

<table>
<thead>
<tr>
<th>Cisco Product/Feature</th>
<th>URL</th>
</tr>
</thead>
</table>