

Providing a Secure Collaboration Framework

In the federal government, different communities of trust must share information and collaborate closely, whether to help keep the peace, respond to humanitarian needs, deal with intelligence data, or promote commerce.

Increasingly, agencies are expected to proactively store, access, and move information in order to respond quickly to requests from other agencies as well as the public. At the same time those agencies require strong security to protect data integrity and sensitive information. What these communities need is a secure collaboration framework for protecting sensitive content. Instead, each agency has a separate, complex, and customized network to accommodate information needs that were spawned by technology limitations and purchasing processes. Despite huge expenditures on IT—topping \$150 billion each year—U.S. federal agencies still represent “an analog government in a digital economy and culture,” according to the former U.S. House Committee on Government Reform.

The Costs of Isolation

Government policies and technology have discouraged agencies from creating a common infrastructure and from realizing its benefits. Thwarted by security concerns and IT practices based on technical limitations, agencies have created their own isolated networks. The duplication of networks, servers, and storage systems represents the purchase of excess equipment and greatly increased acquisition and management costs.

Using non-integrated solutions from disparate vendors reinforces this isolation. What’s more, agencies must deal with multiple points of contact, which can generate confusion, reduce responsiveness, and promote inefficiencies.

In this setting, data sharing has been virtually nonexistent or primitive at best. “Sneaker netting”—hand-carrying data media to the appropriate recipient—is still commonplace.

Meeting the Need for Dynamic Collaboration

Secure collaboration architectures that support dynamic communities of trust would alleviate those woes and usher the federal government into the digital economy. Those architectures would allow each agency to maintain its

information separately but instantly share selected, sensitive data among authorized individuals or groups when the need arises.

This is specifically what an IT industry consortium now provides the government. By joining forces in the Secure Information Sharing Architecture (SISA), this group has developed a comprehensive approach for enabling information sharing and consolidation among agencies.

The group offers a policy-based architecture for managing “need to share” scenarios as well as multiple levels of protection across hardware software and storage platforms. The architecture is scalable to meet the requirements of efforts ranging from local to global, using interoperable, standards-based components.

At the crux of SISA lies a secure, end-to-end, commercial off-the-shelf architecture that was created to easily, but securely, share data among multinational environments for the military. That same architecture can now help governments to securely

share both infrastructure and data, and boost their operating efficiencies, for less than current solutions. It combines the strengths of robust technology components from Cisco, EMC, and Microsoft with other leading technology innovators.

Together those components provide integrated, overlapping layers of security based on flexible policy management as well as information assurance at four layers—access protection services, data protection services, content protection services, and watchdog services.

For example, Microsoft’s Active Directory, with its support of a fully integrated public key infrastructure and Internet secure protocols such as LDAP over SSL, authenticates user identity. It supports Kerberos and x.509, among other login authentication mechanisms within the SISA framework. When paired with Cisco security solutions, user classification and identity information stored in the directory can determine how, where, and if a user accesses the network and what elements of the network that user is allowed to see.



How It Works

SISA promises to greatly improve the way government organizations store, access, move, and share data. For example, with SISA security measures in place a command center workstation connected to the network will display a standard login screen that uses Microsoft Active Directory to access a user profile.

Based on the user's login credentials, Cisco's Network Admission Control (NAC) appliance verifies that the user's device complies with the accepted security posture, then designates which parts of the network the user may access to reach applications and content. After the user is authorized and assigned to the appropriate VLAN, Cisco Security Agent protects the workstation by using behavior-based defenses to detect and block abnormal activity before it can cause damage. The user can now access the familiar suite of Microsoft and other agency applications and collaborate and share files for which that user has been authorized. Access to specific resources—such as CD-ROMs, write-capable serial ports, and USB devices—may be restricted by policies implemented through Cisco Security Agent. Content contained within e-mails and documents is protected using Liquid Machines and Microsoft Rights Management Services (RMS), which are also integrated with the content management features of SharePoint.

Benefits of SISA

SISA creates a single, secure foundation for members of established and ad hoc communities of trust to share information,

and simultaneously protects stored and in-transit data while enforcing policies and privileges. The platform lets partners add network security measures and applications. And federal agencies will reduce IT costs by making better use of existing investments in technology, applications, and skills.

SISA At-a-Glance

- Defines a complete architecture and roadmap of well-known products and services that are available today
- Creates a foundation for deploying agile communities of trust by operationalizing business processes and policies
- Automates authentication and authorization; encrypts data in use, in transit and at rest
- Provides alerting and notification services with geospatial data for real-time situational awareness
- Integrates a comprehensive, secure audit trail with standardized reporting and alerts
- Enables scalable, progressive deployment, building on and unlocking the value of existing IT investments

Together Cisco, EMC, Microsoft, and the SISA partners—Liquid Machines, Swan Island Networks, and Titus Labs offer great breadth and depth of experience as well as commercial, off-the-shelf solutions that form a secure collaboration framework for protecting sensitive content among communities of trust within the federal government and defense communities. The SISA partnership is focused on supporting customers' needs for software that works well with their current IT infrastructure,

defining a new generation of software to enable greater interoperability by design, and harnessing the power inherent in disparate software platforms to boost overall effectiveness.

SISA Alliance Members

The core technology and services of the SISA solution are provided by Cisco, EMC, and Microsoft. In addition, three innovative partners—Liquid Machines, Swan Island Networks, and Titus Labs, Inc., provide complementary technologies. SISA and the formalized business alliance are managed by Addx Corporation, serving as the SISA Joint Program Office.

www.SISAalliance.com



DS070707