



Network Transformation

(TIC, IPv6, FISMA, Collaboration)



Executive Summary

Today's federal CIOs and their staffs face numerous challenges, including security, compliance, collaboration, operational efficiencies, and cost containment. At the same time, several initiatives including technology and policy changes, new contract vehicles, and agency-wide initiatives have aligned to transform our government's internal and public-facing communications strategies. Two of the most significant—the U.S. General Services Administration's Networkx contract and the Office of Management and Budget's (OMB) Trusted Internet Connection (TIC) initiatives—present significant challenges, and potential rewards for agencies that can capitalize on these initiatives.

The Networkx Transition

Uniquely positioned to help agencies make successful transformations, Cisco offers valuable solutions to meet these new requirements and to help you develop and execute your migration plan. Cisco's dedicated teams for each of the Networkx primes have the capability to align agency requirements with Cisco's innovative solutions to maximize the Networkx contract opportunity. This means a movement to the managed services model, so that the agency's operational role evolves from the agency being the provider of IT services to overseeing providers. Now agencies can focus on mission needs and evolve from a capital expenditure (CapEx) to an operational expenditure (OpEx) spending model, providing a predictable cost structure and a reduced risk of technology obsolescence.

Scalability and Investment Protection

Investing over US\$4 billion annually in research and development, agencies throughout the federal government can rest assured that Cisco will be there to support them now and in the future. Cisco continues to innovate in every area from network infrastructure solutions to advanced applications such as high-definition video collaboration with Cisco TelePresence. You can rely on Cisco to bring networking and collaboration to new heights and provide the best support possible in serving your agency.

Security Solutions

Cisco has worked with leading technology partners such as Microsoft and EMC to develop a framework that supports secure collaboration. The Secure Information Sharing Architecture (SISA) empowers agencies to securely collaborate with both internal and external parties, helping to meet TIC requirements while leveraging existing investments and readily available components. SISA is a key element of the Cisco Self-Defending Network, where security is pervasive throughout the network, enabling network and security components to work seamlessly together to configure, manage, and monitor these assets while ensuring FISMA compliance.

What You'll Learn

In this document, you'll learn how Cisco is helping agencies achieve their missions while fulfilling these new government objectives.

Top-Level Issues: Thinking Green, IPv6, Collaboration, FISMA, and TIC

Thinking Green

Infrastructure

Agencies are reacting to rising energy prices, current and pending legislation, and a desire to be environmentally responsible. Cisco can help by providing expertise, partners, and solutions to assist agencies in delivering eco-friendly results that benefit citizens and mission-success alike.

Cisco is committed to helping agencies use IT to make their operations greener. By enabling significant reductions in travel with collaborative tools driven by Web 2.0 technologies, agencies can dramatically reduce their impact on the environment. Additionally, with offerings such as the Cisco Unified Communications family of products, including Cisco TelePresence, Cisco Unified Video Advantage, Cisco Unified MeetingPlace, and WebEx, or tools such as blogs, wikis, podcasts, and other social-networking applications, your workforce can maintain the in-person, high-touch and high-feel experience without ever leaving the agency.

Power Consumption

The importance of energy conservation has never been greater than it is today. In 2006, Cisco established the Energy Efficient Data Center (EEDC), a solutions and best practices focus area. Working in partnership with the Green Grid and the Cisco Research, Architectures and Technology Exchange (CREATE) team, Cisco's aim is to provide measurement, monitoring, and management of data center power consumption. While the work continues to meet this long-term goal, incremental advances across a range of products and services are continuously being developed and implemented.

In addition to energy conservation in the data center, Cisco supplies energy-efficient products and solutions throughout the agency environment. These include low-power switches, energy-efficient integrated platforms (integrated services routers, aggregation services routers), IP phones, and network virtualization and consolidation.

Learn More

Visit: newsroom.cisco.com/ciscogreen and www.cisco.com/go/telepresence.





IPv6

In planning your Networkx transformation, IPv6 capabilities are a critical consideration. While applications that produce an ROI specific to IPv6 are not presently available, the long-term benefits of having an IPv6-capable infrastructure make IPv6 an essential investment.

Cisco offers a wide range of IPv6-implementation capabilities to address short-term requirements while also supporting a more gradual, long-term approach that incorporates best practices and knowledge derived from previous customer deployments. No other technology partner is better suited to design a migration roadmap to meet your specific needs while taking into account transition, cost, security, and training concerns.

Cisco provides agencies with IPv6 assessment services that include a customized scorecard, assessment, and audit based on your IPv6 readiness. Cisco then works with you to establish a migration path aligned with your strategic agency objectives.

Learn More

Visit: www.cisco.com/go/ipv6.

(For detailed technical guides about how to plan or deploy IPv6 in your agency's network, refer to Cisco's "Deploying IPv6 in Campus Networks" and "Deploying IPv6 in Branch Networks.")

Secure Collaboration and Information Sharing

Agencies are faced with the complex challenge of how to securely share information between and within internal and external communities of interest. The Secure Information Sharing Architecture (SISA) breaks through information-sharing barriers with a commercial off-the-shelf (COTS) solution that allows agencies to communicate and collaborate openly, while protecting sensitive internal content. It consolidates disparate systems and networks into a cost-effective infrastructure that secures, governs, and accelerates the distribution of mission-critical knowledge. Elements of this framework are currently deployed for the Department of Defense and civilian agencies.

SISA combines products from Cisco, EMC, and Microsoft with best-of-breed innovations from Liquid Machines, Swan Island Networks, and Titus Labs to address the urgent need for sharing sensitive materials across organizational, IT, and jurisdictional boundaries. With SISA, agencies can participate with confidence in communities of trust knowing they have the controls to precisely govern how information is accessed and used. SISA provides the power to determine how, when, where, and with whom the agencies share materials according to mission requirements, not the constraints of technology or resources. The information-sharing architecture incorporates best practices and design considerations surrounding virtual storage area networks, data privacy, and network management to facilitate and protect information sharing across organizational boundaries.

Learn More

Visit: www.sisaalliance.com and www.cisco.com/go/sisa.

SISA At-a-Glance

- Defines a complete architecture and roadmap of well-known products and services available today
- Creates a foundation for deploying agile communities of trust by supporting agency processes and policies globally, which was previously not possible.
- Automates authentication and authorization, and 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

FISMA

To meet compliance requirements of the Federal Information Security Management Act (FISMA), federal agencies must tie together planning, processes, and technology to make effective use of agency resources while protecting the confidentiality, integrity, and availability of mission-critical information systems. The Networx transformation and move to TIC is an ideal time to address security issues at an architectural level to allow for interoperability among security solutions and across the enterprise.

The Cisco Self-Defending Network solution helps protect federal agencies from threats originating both internally and externally. This protection helps government organizations take better advantage of the intelligence in network resources, thus improving overall security while addressing FISMA requirements, including protection against unauthorized access, malicious code, scans and probes, improper usage, and denial-of-service attacks.



Figure 1 (below) lists areas in which Cisco can support agencies in meeting FISMA requirements.

Figure 1 (below) Cisco Solutions and Services to Support FISMA Security Requirements

FISMA SECURITY CONTROLS		MANAGEMENT	OPERATIONAL	TECHNICAL
CA	Certification, Accreditation, and Security Assessments	X		
PL	Planning	X		
SA	System and Services Acquisition	X		
CP	Contingency Planning		X	
IR	Incident Response		X	
MA	Maintenance		X	
MP	Media Protection		X	
PE	Physical and Environmental Protection		X	
PS	Personnel Security		X	
AT	Awareness and Training		X	
CM	Configuration Management		X	
RA	Risk Assessment		X	
SI	System and Information Integrity		X	
AC	Access Control			X
AU	Audit and Accountability			X
IA	Identification and Authentication			X
SC	System and Communications Protection			X

Controls that apply to Cisco Advanced Services

Controls that apply to Cisco solutions, products, and services

Learn More

Visit: www.cisco.com/en/US/products/ps6923/index.html and www.cisco.com/go/sdn.

TIC Internet Gateway Consolidation

Cisco is ready to partner with agencies as they move toward consolidating Internet connections to satisfy OMB's Trusted Internet Connection (TIC) initiative, which will improve the federal government's incident response capability through the reduction of external connections and through centralized gateway monitoring at a select group of TIC Access Providers (TICAP).

As agencies consolidate or remove Internet connections, two dramatic facts emerge. First, Internet connection consolidation will require a new Internet portal architecture that meets all Internet communication needs and is scaled appropriately to support the new loads. Second, the new traffic flows will require, at a minimum, that agencies review and renew routing architectures, and may create the need for an agency WAN if one does not presently exist.



Things to Consider When Moving to Networx

The transformation to a converged network environment brings on a new breadth of services, establishing the network as the platform for all forms of communications. As a result, network resiliency is critical to achieving mission success.

In planning for future services (Web 2.0, video, and so on), be sure the solution you request can accommodate near-term requirements for bandwidth expansion, levels of service, and new technology insertion. These qualifiers will allow agencies to plan for expansion so the deployed equipment can sustain at least a three-to-five-year lifecycle (be aware that minimum requirements become actual requirements in an RFQ). Anticipating future requirements facilitates smoother site upgrades and fewer outages as new services are deployed. A few important issues to consider for your Networx transition:

- Energy efficiency
- WAN optimization capabilities (compression, caching, TCP optimization) for more predictable application experience
- Integrated voice-over-IP (VoIP) solutions for improved cost efficiencies and enhanced collaboration
- Using integrated security in new solutions to drive FISMA compliance

Conclusion

Cisco offers the expertise and solutions to address the main challenges facing agencies today, including energy efficiency, collaboration, IPv6, FISMA, and TIC. Cisco is committed to providing superior, best-valued solutions with unparalleled support. Cisco looks forward to helping you achieve mission success.



Additional Resources

Security

www.cisco.com/go/security

www.cisco.com/go/asa

www.cisco.com/go/csm

www.cisco.com/go/csa

www.cisco.com/go/nac

www.cisco.com/go/mars

www.cisco.com/web/strategy/government/popup-copss-flash.html

Collaboration

www.sisaalliance.com

www.cisco.com/go/sisa

www.cisco.com/cdc_content_elements/flash/nac/demo.htm

Green Initiatives

newsroom.cisco.com/ciscogreen

www.cisco.com/go/telepresence

<http://tools.cisco.com/search/JSP/search-results.get?QueryText=green>

Networkx

www.cisco.com/go/federal

www.cisco.com/go/networkx

Learn More

Please contact networkx@external.cisco.com to discover how Cisco can help you successfully accomplish the Networkx and TIC transitions.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2008 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)