



WHITE PAPER

## SECURING COMMUNITIES WITH CISCO INTEGRATED SECURITY FOR STATE AND LOCAL GOVERNMENT

Today's state and local government agencies are transforming the way they operate, communicate, and deliver services. Increasingly, agencies are using Internet-based network solutions to offer a broad range of programs that enhance public safety and enable new citizen services while lowering costs to accommodate shrinking budgets. By using the network to improve communication between agencies and their constituents, governments are making their services more effective and enhancing safety in their communities. A prerequisite for delivering services over the network is security.

### CISCO INTEGRATED SECURITY FOR STATE AND LOCAL GOVERNMENT DELIVERS THE COMPREHENSIVE NETWORK SECURITY NEEDED TO ACHIEVE AGENCY GOALS

#### Executive Summary

To improve services without increasing operational costs, state and local governments developed new business processes made possible by networking technology, such as IP Communications and wireless networks. As a prerequisite to making these processes widely available, networks must be secured against a rising volume of viruses, worms and other hacker attacks that threaten the continuity of government services. In addition, network security is needed to ensure privacy, which involves controlling access to sensitive information such as property tax bills, personal citizen records, or health information.

This white paper is intended for government IT officials concerned with the security of their IP networks. It begins by explaining the growing need for network security in government networks. Next it describes Cisco® Integrated Security for State and Local Government solutions that meet these requirements. The paper concludes by summarizing the benefits of Cisco Integrated Security State and Local Government and presenting the unique qualifications of Cisco Systems® as a provider of network security solutions.

#### Urgent Need for Network Security in Government Networks

The volume of threats to network security is rising, and so is the potential damage that can result. Although effective security technology is readily available, many government agencies still do not adequately protect their infrastructure and their citizen data. Until recently, many state and local government administrators considered viruses to be mere nuisances, and were not concerned with protecting their networks. Today, however, a combination of self-propagating threats, collaborative applications, and interconnected environments has thrust security, or rather its absence, into the headlines. Recent examples of network security threats impacting state and local government agencies include the shutdown of all of the state of Maryland's motor vehicle offices, the Sobig.F virus affecting all agencies in California, and an event in Kentucky that required the Louisville emergency dispatch call centers to resort to pen and paper when its network was affected. In perhaps the most widespread event, in January 2003 the SQL Slammer worm took down a sizable number of government and commercial networks worldwide.

Network security plays an essential role in helping state and local governments meet their three top goals:

- *Improve service effectiveness.* As governments increasingly rely on their networks to deliver services, from driver's license renewals to Web-based building permit applications, network availability has become even more critical. Network security helps prevent viruses, worms, and hacker attacks that otherwise might threaten continuity of government services.
- *Increase citizen safety.* Protecting the network from hacker attacks and disruption helps ensure services such as emergency dispatch or highway traffic control remain available. Similarly, measures such as encrypting sensitive data for transmission over a virtual private network (VPN) help protect citizens from loss of privacy and crimes such as identity theft.

- *Drive economic development.* A state or local government agency that delivers services effectively and protects citizen safety gains an edge in attracting residents, businesses, and tourists. Service effectiveness and safety hinge on the availability and privacy of the network.

Security not only is essential for ensuring the continuity of government service and protecting private citizen data, it's required by law. A growing body of regulations, such as the Federal Information Security Management Act of 2002 specifies minimum standards of data and application security. Therefore, government agencies require comprehensive, end-to-end security solutions that replicate best practices and adapt quickly and easily for emerging threats.

## CISCO INTEGRATED SECURITY FOR STATE AND LOCAL GOVERNMENT

Cisco Integrated Security for State and Local Government solutions provide agencies with a comprehensive defense against both internal and external threats to sensitive data and business processes. This integrated suite of products and services protect the IP applications that governments use to solve problems, complete tasks, and conduct transactions with constituents and other agencies.

**“Networks have evolved from closed systems to more open, sophisticated systems. As a result, security threats have grown exponentially, both at the network perimeter and from within. Cisco has responded with a strategy to integrate security services into the network infrastructure. This provides a flexible, cost-effective, and comprehensive approach to secure today’s extended network.”**

—Zeus Kerravala, The Yankee Group

Designed specifically for deployment on public networks, the Cisco Integrated Security for State and Local Government solutions fortify the network against outages, service degradation, and security breaches. These solutions incorporate the three critical factors in effective network security for governments—threat defense, secure connectivity, and trust and identity management—as well as professional services (see Table 1):

**Table 1.** Cisco Integrated Security for State and Local Government

Cisco Network Technology	Purpose
<b>Threat Defense</b>	<ul style="list-style-type: none"> <li>• Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) monitor and respond to security events as they occur.</li> <li>• Central management tools define and distribute configurations, monitor and audit device usage, and enforce policies.</li> </ul>
<b>Secure Connectivity</b>	<ul style="list-style-type: none"> <li>• Virtual private networks (VPNs) help ensure data privacy and integrity during transmission to and from remote locations over low-cost public lines.</li> <li>• Wireless local area networks (WLANs) provide security over mobile infrastructures.</li> <li>• Firewalls protect the network edge, controlling access to critical network applications, data, and services to help ensure unfettered availability for legitimate users</li> </ul>
<b>Trust and Identity Management</b>	<p>Using Authentication, Authorization and Accounting (AAA), the network:</p> <ul style="list-style-type: none"> <li>• Identifies users and the network resources to which they wish to connect</li> <li>• Grants or denies access</li> <li>• Creates audit trails of network access built on standards based protocols like 802.1x</li> </ul>
<b>Professional Services</b>	<p>Cisco and its partners assess an agency’s network security posture, providing guidance on next steps and long-term strategies.</p>

## Threat Defense System

Network threats have become more destructive and frequent. Internal and external threats such as worms, denial of service (DoS) attacks, man-in-the-middle attacks, and Trojan horses can disrupt the continuity of government services. The Cisco Threat Defense System provides a strong defense against both known and unknown attacks. Because attacks can start anywhere and spread rapidly, the solution enhances security throughout the network: in the existing network infrastructure, at the endpoints (both server and desktops), and network devices. The solution is tied together with a centralized management system that allows customers to readily and accurately identify, control, and eliminate network attacks. This enables customers to make more effective use of network and security devices by combining traditional security event monitoring with network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification and automated mitigation capabilities. The result: a proactive defense of the government agency, its network, applications and users.

## Secure Connectivity System

As government agencies deploy extranets for their constituents and provide remote access to the network for teleworkers, they need to maintain security, data integrity and privacy across all connections. Government LAN connections, traditionally considered trusted networks, now also require higher levels of security. Finally, because internal threats are just as damaging—both financially and in terms of public confidence—as external threats, government agencies must take steps to ensure the confidentiality and integrity of the data and government services delivered over wired or wireless LANs.

The Cisco Secure Connectivity System uses encryption and authentication to provide secure transport across untrusted networks. To protect data, voice, and video applications over wired and wireless media, Cisco offers IP Security (IPSec), Secure Sockets Layer (SSL), Secure Shell (SSH) and Multiprotocol Label Switching (MPLS)-based VPN technologies. These are augmented by the extensive security capabilities incorporated into Cisco wireless and IP telephony solutions for government.

## Trust and Identity Management System

A trust and identity management system serves as the foundation for any secure network and is especially critical for a government network. It involves providing or denying access to government applications and networked resources based on an employee's or constituent's specific privileges and rights. The Cisco Trust and Identity Management System offers network-based admission control, providing access to specific government resources or networks only after validating the identity of a user or device and their compliance with the agency's security policy. The network is responsible for identification, authorization, and enforcement. Solution components include the Cisco Secure Access Control Server (ACS), authentication protocols such as 802.1x, and the AAA (Authentication, Authorization and Accounting) capabilities in Cisco switches and routers.

## Integrated Solutions

The components of the Cisco Integrated Security for State and Local Government solutions work together to prevent or respond to threats to government networks. For example, integrated firewall, intrusion detection and protection, endpoint security functionality, and one-touch lockout on routers mitigate disruption from security breaches. Similarly, Cisco Security Agent enables government agencies to recognize and prevent future malicious behavior before it causes damage.

Cisco Integrated Security solutions are easy to maintain, and offer agencies what has become hallmarks of Cisco technology products—high availability and quality-of-service (QoS) features. Because the solutions are scalable and based on the highly adaptable Cisco IOS® Software architecture, they not only meet agencies' current security needs but also position networks for tomorrow's challenges. Agencies can more efficiently share information, establish the highest possible levels of security, while simultaneously reducing administrative, maintenance, troubleshooting and training costs.

## BENEFITS TO GOVERNMENT

Cisco Integrated Security solutions defend desktops, servers, and networks throughout the agency’s metro, campus, edge, and wireless LANs to deliver multilayered protection for distributed information assets. The benefits of the Cisco Integrated Security solutions are outlined in Table 2 below:

**Table 2.** Benefits of Cisco Integrated Security Solutions for State and Local Government Agencies

Government Need	Solution Benefits
<b>Ensured Continuity of Services by Protecting Infrastructure</b>	<ul style="list-style-type: none"> <li>• Mitigates worm attacks</li> <li>• Prevents unauthorized access</li> <li>• Prevents denial-of-service (DoS) and distributed DoS (DDoS) attacks</li> <li>• Protects confidential information assets and network access points</li> </ul>
<b>Ensured Continuity of Services by Responding to Network Threats</b>	<ul style="list-style-type: none"> <li>• Safeguards infrastructure in the event of an attack, thereby reducing the damage of attacks from “Day Zero,” before they spread</li> <li>• Troubleshoots and, as necessary, reconfigures the network</li> <li>• Provides decision makers with meaningful and relevant security information</li> </ul>
<b>Ability to Comply with Data-Handling Regulations</b>	<ul style="list-style-type: none"> <li>• Delivers products and services that help customers conform to specifications of government regulations</li> <li>• Audits government networks using advanced professional services</li> </ul>
<b>Improved Productivity</b>	<ul style="list-style-type: none"> <li>• Minimizes user disruption and network downtime</li> <li>• Provides Web-based tools for security tasks such as configuring, monitoring, and troubleshooting VPNs, firewalls, and network and host-based intrusion detection systems</li> <li>• Eliminates network investment “add-ons” for separate purchases, vendor relationships and management expertise related to security</li> <li>• Positions an infrastructure to provide security for future capabilities, such as IP telephony, video conferencing, and customer service applications</li> <li>• Simplifies ongoing network maintenance, operations, and management</li> </ul>
<b>Ability to Provide Secure Connectivity to Remote Offices</b>	<ul style="list-style-type: none"> <li>• Facilitates interagency collaboration</li> <li>• Helps ensure data privacy using VPNs, which provide high-performance encryption and tunnels</li> <li>• Enables remote employees or partner agencies to access the network over secure, high-speed connections, facilitating workgroup collaboration, extranets, mobile operations centers, and virtual, worldwide contact centers</li> <li>• Provides assurance that network connections are secure, available, and high-performing, through service level agreements (SLAs) with Cisco service provider partners</li> </ul>

## WHY CISCO?

### Comprehensive Solutions for Government Network Security

Cisco Integrated Security for State and Local Government offers solutions that integrate industry-leading hardware and software end-to-end across the network, protecting data and applications from the network core to the desktop. Advanced security functionality is embedded in Cisco routers, switches, appliances, and end points in the standards-based solutions. Security services are tightly integrated with network services: VPNs, for example, work transparently with Cisco IP Communications applications, enabling public administrations of all sizes to securely deploy advanced IP applications that increase service effectiveness, improve public safety, and drive economic development.

Uniquely, Cisco offers:

- *Unmatched technical expertise*
  - Almost 20-year track record as the industry leader in networking
  - World-class Cisco certified networking engineers with in-depth networking expertise
  - Extensive experience in scalable, network design, operations, management, and support
  - Extensive network deployment experience in the public sector around the world
  - Broad range of technical experts and engineers who understand government needs, standards, and important initiatives
- *Unrivaled partnerships*—Cisco maintains partnerships with industry IT leaders to help governments deploy a highly adaptable network infrastructure, as well as innovative applications that allow governments to extract the most value from their infrastructure investment to serve citizens.
- *Highly interoperable solutions*—Industry-leading, open, and standards-based, network solutions from Cisco deliver unmatched interoperability, which protects and extends customer investments.

### Cisco Security Specialized Partners

Cisco and its partners employ consultants with in-depth experience in the government intelligence community. Government agencies can take advantage of these services to extract maximum return on their network security investment. For example, security posture assessments help agencies proactively identify points of potential network vulnerability and gauge the exposure of internal systems, thwarting network attacks before they can be executed. Among the other security services available include:

- Business analysis and planning
- Technology planning
- Project management
- Business-process redesign
- Multivendor network support
- Deployment support
- Training

To find a Cisco Security Specialized Partner, visit the Cisco Partner Locator at: <http://www.cisco.com/go/partnerlocator>

### SAFE Blueprints from Cisco Systems

For public administrations, the first step in securing the network is presenting a compelling business case for officials and constituents. Customizable SAFE Blueprints from Cisco provide the information necessary to developing a case, including:

- Roadmaps that show how Cisco solution components support changing application requirements and evolving government regulations
- Flexible deployment scenarios, with and without assistance from Cisco channel partners

## CONCLUSION

A comprehensive approach to network security is mandatory for state and local government agencies to meet their goals of making services more effective, improving citizen safety and providing effective and efficient government services. Cisco Integrated Security for State and Local Government solutions help protect networks end to end—from the network core to end-user devices—and address the need for secure networks with advanced security hardware, software, and consulting services.

To learn more about Cisco Integrated Security solutions, and the Cisco Self-Defending Network, visit the following Websites:

- Cisco Integrated Security for State and Local Government: <http://www.cisco.com/go/slg-security>
- Cisco Government Resources: <http://www.cisco.com/govnow>
- Cisco State and Local Government Industry: <http://www.cisco.com/go/localgov>
- Cisco Network Security: <http://www.cisco.com/go/security>
- Cisco Self-Defending Networks: <http://www.cisco.com/go/selfdefend>
- Cisco Security: <http://www.cisco.com/securitynow>
- To speak with a Cisco representative, visit: <http://www.cisco.com/go/industrysoln>



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel  
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan  
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R) 205209\_e\_ETMG\_JC\_2.05