White Paper

CIPHEROPTICS
Network security made simple

Securing data transmission on government networks

The federal government's evolving networks create new security concerns

Table of Contents

CipherOptics

October 2004

Securing data transmission on government networks

As government networks are becoming increasingly complex, they are more vulnerable to security breaches. Just like the commercial sector, the federal government has experienced dramatic growth in the number of attacks on information networks. According to CERT, a federally-funded security research institute, security incidents have grown at an annual rate of 94 percent since 2000. With heightened national security concerns, the government recognizes that even random, unclassified data can be re-constituted, allowing sensitive or classified information to be accessed and misused by unauthorized users.

The increased risks to government networks have grown out of technological innovation, including the ubiquity of the Internet and the prevalence of electronic data, as well as policy-driven measures. In 1993, government agencies began a cost-saving initiative by migrating their networks from private leased lines to IP-based networks. More recently, the president's *E-Gov* strategy has focused on using federal government networks as a strategic tool to improve the quality of service to citizens and businesses. Early on, *E-Gov* eliminated networks that duplicated tasks, and identified new ways for agencies to work together across non-traditional boundaries. The next fundamental transformation is underway to provide ubiquitous access to government IP networks from anywhere in the world. This means using a combination of "trusted" networks, which the government controls, and "untrusted" networks—the Internet and wireless networks.

According to Edward Allen, an independent consultant and retired FBI senior executive, "In today's world, information provides value if it is accurate, timely and shared appropriately. The sharing of information requires access and availability by authorized users regardless of their geographical location.

"Networks that facilitate information sharing can introduce unacceptable risk and exploitation if not properly designed and managed," he said. "Robust encryption technology for the transmission of data is an essential aspect of any viable information security strategy to mitigate these risks."

As a result, the government is seeking the best practices for securing mission-critical data traversing its networks. A number of policies and directives have been developed in recent years that provide broad direction on security matters.

Government initiatives, policies and directives on IT security

In addition to technological innovation, forces driving change in government networks are regulations and mandates designed to ensure data integrity and confidentiality on those networks. Here are some of the directives requiring a new look at network security:

The National Security Agency (NSA) CNSS Policy #15 directs government agencies to use National Institute of Standards and Technology (NIST)-approved algorithms for securing sensitive but unclassified (SBU) data. NIST provides a validation process for cryptographic devices using the Advanced Encryption Standard (AES), known as the Federal Information Processing Standard (FIPS-140-2 L2) cryptographic validation process. Once a vendor has met the FIPS validation, government agencies can purchase the security device with confidence that the device provides the approved level of data security.

Department of Defense Directive 8100.2, released by the United States Department of Defense on April 14, 2004, establishes the policy under which commercial wireless devices may be used on DoD networks. While some of the requirements of this policy discusses other aspects of device management, many of the requirements identified relate directly to the security of the devices and of the wireless networks and requires that "*all wireless communications be encrypted*."

The FBI's Criminal Justice Information Services Division (CJIS) requires that all federal, state and local agencies communicating with CJIS-managed criminal justice networks and databases encrypt all transmissions to and from the originator of any information exchange. This means, for example, that the local law agency in Tulsa, Oklahoma must encrypt its online query to the CJIS databases in West Virginia for information on a suspect's criminal history.

The Federal Information Security Management Act (FISMA) of 2002 eliminated the statutory provision that allowed federal civilian agencies to waive mandatory Federal Information Processing Standards (FIPS). FISMA also supercedes some components of the Computer Security Act of 1987.

The National Strategy to Secure Cyberspace (NSSC) is part of government's overall effort to protect the nation. Its purpose is to engage the entire society—federal, state and local governments, industry and the public—to secure the portions of cyberspace that they own, operate, control, or with which they interact. The strategy states that all parties must take proactive steps to identify and remedy vulnerabilities in the absence of known threats. NSSC makes the case that the cost of a cyber attack is far greater than the investment to prevent it.

The Homeland Security Act of 2002 mobilizes the U.S. government to protect the country from terrorist attacks. The Department of Homeland Security (DHS) was established to provide a unifying core for the vast national network of organizations and institutions involved in efforts to secure the nation. DHS's strategic goals are to identify threats, assess vulnerabilities and mitigate terror attacks to safeguard people, critical infrastructure, property and the economy. Government networks fall into the critical infrastructure category that must be protected.

These policies and directives collectively advocate government entities to act now to secure data on networks. But how does government find the right security solution that fits with existing budgetary constraints? By examining some common network vulnerabilities, government IT managers can gain a better understanding of their own network exposure.

Network vulnerabilities: Looking beyond the perimeter

Government agencies must look at network security from a holistic perspective. Firewalls, intrusion detection systems (IDS), anti-virus software and other perimeter security technology do their part in preventing many outside threats from entering the network through an Internet gateway. But what about the data once it travels from one site to another over an agency's core IP network, inside the perimeter?

The only way to protect that data is to encrypt it while in transit, because even private lines are vulnerable to people with access. Unauthorized access of data while it travels the network can result in one of two possibilities: unauthorized monitoring of data in transit, or unauthorized modification of data in transit. Either of these can have a devastating, effect on data integrity, confidentiality and network operations.

Unauthorized monitoring and access of data in transit
Network users take for granted that the data they send over government networks will be viewed only by the intended receiver. However, users never really know if someone else is listening, reading or even copying data as it passes over a network. For example, a government agency could be using high-speed data replication over an IP network for redundant storage. If not properly secured, an intruder or unauthorized person could monitor or "eavesdrop" on transmission of that storage data.

Unauthorized modification of data in transit
A simple route traced between any two government networks may show myriad routers and service providers between two points. Each link provides an opportunity for an intruder to inconspicuously modify data. It is important to ensure that data is not altered as it goes across a network. Imagine the impact of an intruder modifying an agency's financial transactions in transmission as they are retrieved from a data center, or altering maps being downloaded to support a military mission. Unauthorized users could also insert unauthorized information during transmission.

Protecting the core transport network is critical because there is a growing list of vulnerabilities that must be addressed beyond the perimeter:

Denial of service (DOS) attacks - type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols.

IP spoofing - In IP spoofing, an attacker gains unauthorized access to a computer or a network by masking a malicious message as a message from a trusted machine by "spoofing" the IP address of that machine.

Insider breaches – employees, contractors and others with legitimate network access can bypass perimeter security to access sensitive but unclassified (SBU) data on the network.

Social engineering – the process of deceiving people into giving away confidential information or access. In a survey of office workers in the Liverpool Street Station in London, 71% of employees will part with their password for a candy bar.

Man-in-the-middle attacks – also know as TCP Hijacking, where an attacker sniffs packets from the network, modifies them and inserts them back into the network.

Port mirroring -- Port mirroring is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. While this is used by network administrators as a diagnostic tool, in malicious hands it can be used for unauthorized data access.

IPSec – authentication, confidentiality and integrity

There is proven technology that dramatically diminishes the impact and occurrence of these network vulnerabilities. IP Security (IPSec), defined by the Internet Engineering Task Force (IETF), is the accepted standard for protecting data in transit over an untrusted network and provides three levels of security: confidentiality, authentication and integrity.

- Confidentiality – Keep your data private
  IPSec uses industry standard encryption algorithms (AES and 3DES) to keep data secret
- Authentication – Trust your sources
  Verify the identity of the peer IPSec gateway to verify the source of the data
- Integrity—Trust your data
  IPSec uses industry standard hashing algorithms (SHA1 and MD5) to ensure data has not been altered in transit

IPSec works on Layer 3, the network layer of the Open Systems Interconnection 7-layer networking model. By running on Layer 3, IPSec is able to function transparently to higher layer applications; the applications do not require any knowledge of IPSec in order to use it. Combined with Internet Key Exchange (IKE), IPSec users can exchange keys, authenticate one another, and securely tunnel encrypted data between peers.

CipherOptics network encryption appliances use IPSec and AES or 3DES to provide the highest level of encryption possible for high-speed networks.

Securing data in transit

Securing data in transit is critical to a "defense-in-depth" network security strategy, especially in protecting your core IP transport network. As government networks become accessible to outsiders, including citizens and contractors, focusing on hardening the perimeter becomes much less effective, leaving your core network vulnerable. According studies by CERT, the FBI and InterGov, nearly 80% of security breaches are conducted by insiders. Encrypting data as it travels on the core network, as well as when it goes to remote sites, becomes the only way to effectively protect unauthorized access to data.

There are several ways to encrypt data as in travels on your network:

- Routers/switches with VPN blades
- Multi-purpose devices that combine numerous security functions in one box
- VPN appliances

Router/Switches with VPN blades
Usually available from router manufacturers, VPN blades are a server-based encryption solution. The drawbacks of VPN blades are that they add complexity to the network, meaning multiple IT hours in configuring the blade, and reconfiguring the routers and network. VPN blades also have a relatively slow encryption-decryption cycle that introduces latency, and can produce network bottlenecks, decreasing network performance.

Multi-purpose security devices
Also called "God boxes," these perimeter devices integrate several security functions into a single unit, usually including firewall, intrusion detection, encryption and virus protection. While often easy to manage, they offer varying degrees of the effectiveness of each function. These devices can also introduce significant latency, which can negatively affect applications like VOIP and storage networking, and can reduce throughput.

VPN appliances
CipherOptics is the leading provider of IPSec VPN appliances. Because they are purpose-built, these appliances have the advantage of not adding complexity to the network, latency to the applications or degradation of network performance. They are particularly well-suited for high-speed networks (100 Mbps – Gigabit) and for latency-intolerant applications like VoIP, IP storage networking and video conferencing.

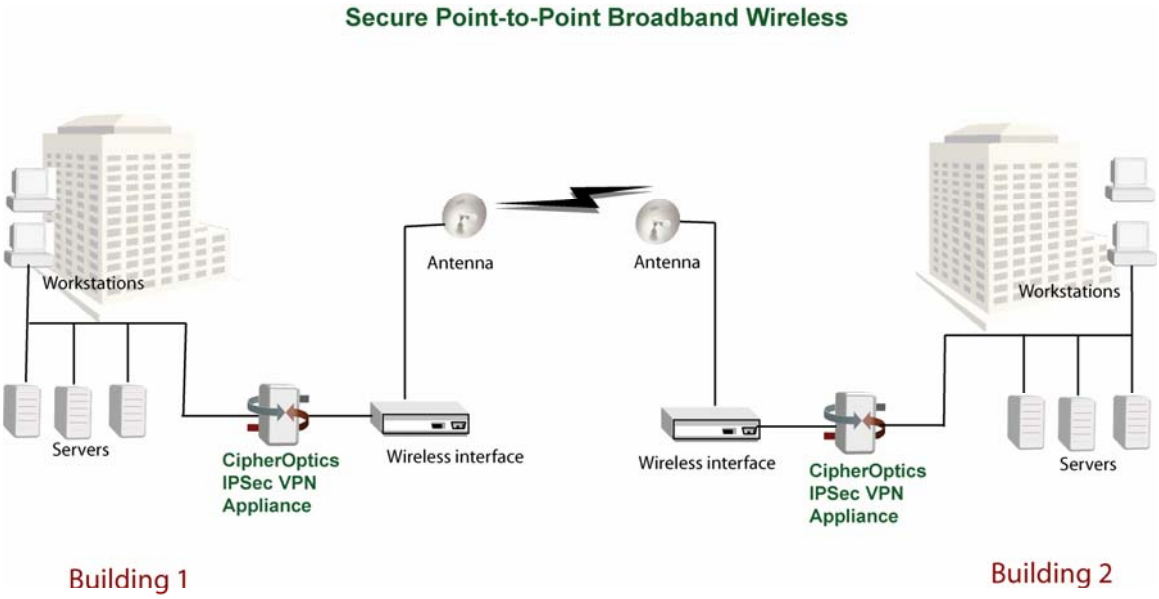
Common networks and their security vulnerabilities

Broadband wireless
Government agencies sometimes use point-to-point wireless connections between buildings and in places where cable or fiber is not feasible. Point-to-point wireless can be implemented using licensed or unlicensed frequency bands or line-of-sight optical technology. However, the "air" that wireless network data goes across is not secure. In fact, DoD Directive 8100.2 mandates that all Department of Defense wireless communications be encrypted.

The insecure airspace expands geometrically beyond the wireless radio dishes to anywhere the wireless signal can be intercepted. This extra space for unauthorized interception leads to a significant additional risk placed upon network and security managers managing wireless wide-area networks.

In wireless transmissions, there is no sophisticated standard to enforce the overall protection of the headers and payload while the data is in transit. Additionally, the architecture of wireless networks influences the probability of theft. Since the size of the spectrum varies dependent on distance and location, transmission paths are vulnerable to unauthorized individuals with sensitive monitoring equipment designed to intercept the data.

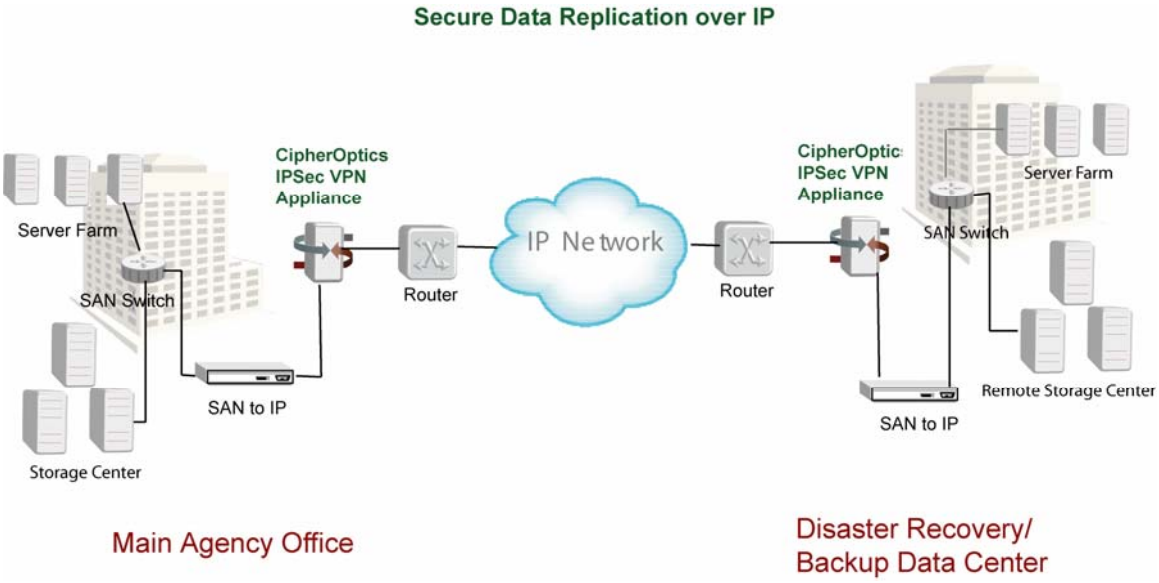
In point-to-point wireless data transmissions, this virtual communication link is inherently un-secure unless that data stream is encrypted.



Data replication over IP

As government agencies look for simple, affordable and effective technologies to ensure that they can replicate and back up their data, and implement effective disaster recovery strategies, more and more are turning to IP-based storage networking. Many have found that they can restore their application processes and resume their normal business practices as quickly as possible—even in the face of a major catastrophe— at a much lower cost when using IP-based storage networking. Network users take for granted that the data they send over government networks will be viewed only by the intended receiver. However, users never really know if someone else is listening, reading or even copying data as it passes over a network. If not properly secured, an intruder or unauthorized person could monitor or "eavesdrop" on transmission of that storage data. By encrypting data before it travels over an untrusted network, the originator can be assured that the data arrives securely at the back-up location.

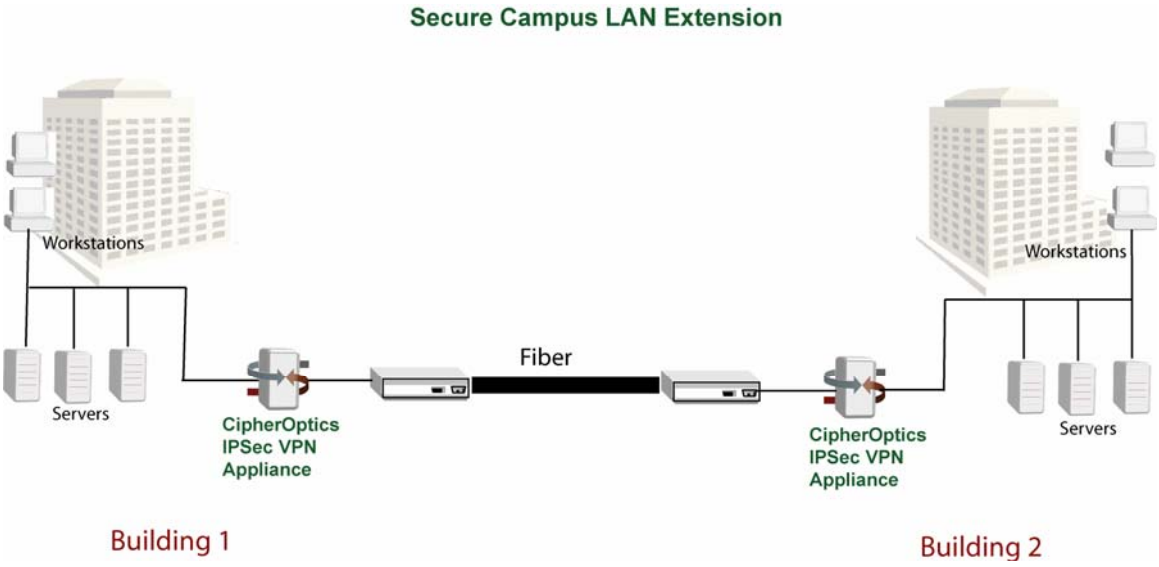
When selecting a security solution for protecting storage data in transit it's important to note that storage networking is notoriously latency-intolerant and often uses jumbo frames in transporting data (greater than 1518 bytes). This means that any security solution must not introduce any discernable latency when deployed. CipherOptics network security appliances are uniquely able to provide robust AES or 3DES encryption without introducing latency, and provide jumbo frame support as well.



Campus LAN Extension

A campus LAN extension is often used by agencies who want to extend their LAN between buildings of close proximity. Common ways to connect LANs between such buildings is with a fiber connection, either a private connection on a contiguous campus or a dark fiber service from a local exchange carrier. While this provides a level of security since outsiders may not even know that it exists, data traveling on fiber is still vulnerable to insiders with knowledge about where the fiber is and what kind of data may be on it.

As with other site-to-site networks, CipherOptics IPSec VPN appliances can provide the highest level of protection possible for data traveling on a campus LAN extension with no impact on applications or the network. In a campus LAN extension, it is important to have VLAN transparency so that there is no network re-configuration required. With "bump-in-the-wire" implementation, CipherOptics IPSec VPN appliances offer network transparency.



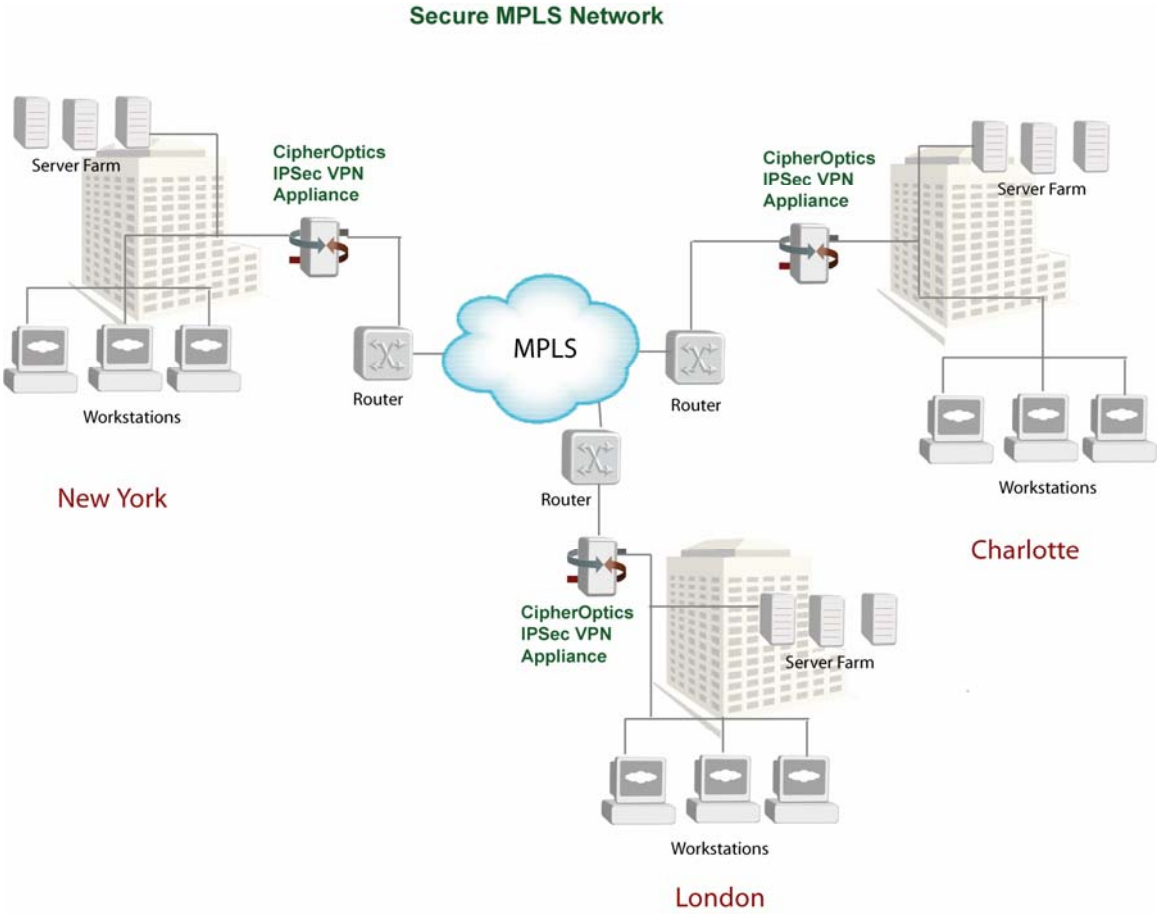
MPLS networks

Multi-Protocol Label Switching (MPLS) networks are becoming a preferred solution for many government agencies. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion and bottlenecks. MPLS-based networks typically run over a carriers' private IP backbone, where service level guarantees and various classes of service can be provided.

It is often taken for granted that MPLS is inherently secure because it segregates data streams into private segments. Some will be surprised to learn that "*private is not secure*," especially when it comes to MPLS networks. MPLS, as a VPN technology, provides the same level of security as other virtual circuit alternatives such as ATM or Frame Relay. All three separate users, enabling organizations to be private. However, they are not secure because the data runs over a common IP infrastructure. Anyone with access can view or alter the data.

As with all government networks, it is important to ensure that data is not accessed by an unauthorized user as it goes across a network. Imagine the impact of an intruder modifying an agency's financial transactions in transmission as they are retrieved from a data center, or altering maps being downloaded to support a military mission.

CipherOptics network security appliances provide an IPSec VPN that secures data on MPLS-based networks, without sacrificing any of the network availability and performance benefits of MPLS. This ensures that the data remains confidential until it reaches its destination. A network security appliance creates a unique fingerprint for each packet transmitted. Only the originator and intended recipient, who share a common key, are able to correctly calculate this fingerprint. The fingerprint, which is based on a mathematical computation involving the packet data and the key, becomes incorrect if data is altered in transit.



Characteristics of an optimal data transmission security solution

Given tight networking budgets, government must strive to provide maximum security with minimum investment. Here are the characteristics essential for an optimal network security solution:

FIPS validation
FIPS 140-2 Level 2 certification is awarded to products after thorough testing by an accredited independent laboratory. It is a benchmark used by government agencies as well as corporations implementing secure applications to determine which products offer robust, standardized protection. Government agencies are required to verify that the security products they are using are FIPS validated.

Performance
The government must evaluate the performance a security solution provides. With so many government applications being latency-intolerant (e.g., streaming video, voice over IP, storage replication, disk mirroring), a security solution must not impact network performance—it must introduce virtually no latency.

Transparency
A network security solution should be easy to deploy and not add complexity to the network. It should be simply inserted between a trusted and untrusted network. The installed device should have no impact on network design or network operation. Security should be achieved without sacrificing network performance.

Easy management
An optimal security solution should be easily managed from a central site through the use of industry standard management interfaces such as Simple Network Management Protocol (SNMP) and secure web access for security policy and configuration changes.
The network administrator should be able to quickly and easily build security policies, set filters and view system status. In general, the devices, once configured, should require very little day-to-day management. Administrators should receive alerts for potential security breaches such as unsuccessful log-ins.

Conclusion
Because the government relies heavily on data and networks to accomplish its mission, now is the time to act to secure this critical infrastructure. Government agencies simply cannot afford to overlook the importance of confidential data transmission in the overall security process.

CipherOptics plays a key role in meeting government's need for affordable security for the confidential transmission of data. CipherOptics SG100 and CipherOptics SG1001 network security appliances, which are unmatched in performance, received FIPS validation in 2004. All government agencies can be assured they are making a wise investment when purchasing CipherOptics.

About CipherOptics

CipherOptics, the leading innovator of gigabit-speed IPSec VPN appliances, protects data in transit as it travels over IP networks. With easy installation, virtually no latency and robust AES encryption capabilities, CipherOptics appliances outperform router and firewall add-on solutions in price, performance and network transparency.

The CipherOptics family of IPSec VPN appliances is field-proven in some of the most security sensitive networks in the world, and has received FIPS-140-2 Level 2 validation. CipherOptics appliances enable financial institutions, government agencies, and global enterprises to protect their sensitive information, mitigate risks and comply with security regulations.

Privately-held CipherOptics is based in Raleigh, North Carolina. In 2004, the company closed $10.3 million in Series C funding from Adams Capital Management, Kodiak Venture Partners, Origin Partners L.P. and Axiom Venture Partners L.P. For more information about CipherOptics visit the company website at www.cipheroptics.com.