

# Continuity of Operations Strategies in the Federal Government:

## Part Two

### The Role of Privacy and Regulatory Compliance

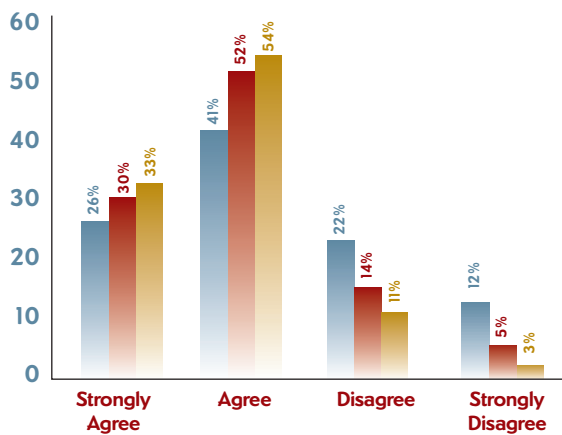
By Rhonda Raider

At the heart of a growing collection of privacy regulations for public and private sector organizations is the issue of public trust. Storing mountains of information electronically and transmitting it online multiplies the risks of inadvertently disclosing that information. The consequences of loss of privacy for federal agencies are grave, ranging from loss of citizen trust to compromised homeland security. In acknowledgement of the magnitude of the problem, government has implemented a spate of privacy regulations discussed later in this report.

It's important to recognize that privacy does not become optional in the event of disruption. Arguably, it becomes even more important because decision-makers might need to collaborate across organizational boundaries not ordinarily crossed during normal operations. To ensure that information can flow between organizations freely and expeditiously during emergencies or other disruptions, federal agencies cannot afford to rely on time-consuming manual security processes requiring human oversight. Rather, they need integrated security technologies that facilitate rather than hinder inter-organizational collaboration. Therefore, privacy and security are inextricable from federal government continuity of operations (COOP) planning.

A Larstan Business Reports survey of 533 government IT professionals investigated attitudes and progress pertaining to COOP and privacy ([www.larstan.net/COOP](http://www.larstan.net/COOP)). The good news is that general COOP planning is well underway, with 67% of civilian, 82% of military/non-combatant, and 89% of military/combatant organizations reporting that they have already implemented a COOP plan and the technical infrastructure to support it.

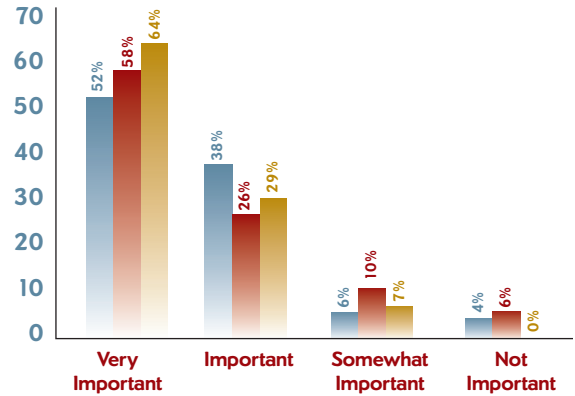
**My organization has already implemented a COOP plan and technical infrastructure to support that plan.**



Furthermore, the vast majority of survey respondents agree that ensuring privacy and complying with relevant regulatory mandates is important to their COOP plans. It's significant that

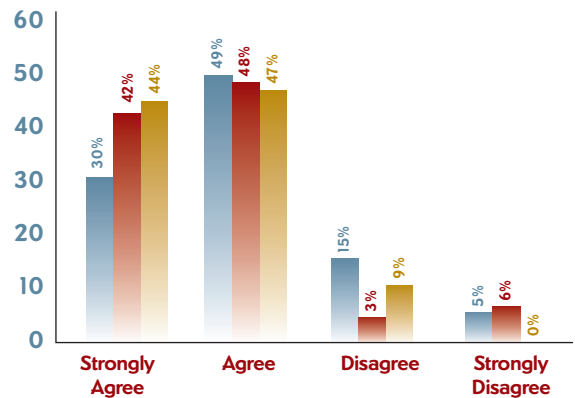
the respondents agree emphatically: approximately twice as many respondents ranked data privacy as "very important" rather than simply "important."

**Please rank the importance of ensuring privacy and compliance with critical regulatory mandates when developing effective continuity of operations (COOP) plans within your organization.**



Interestingly, there appears to be some confusion as to what it takes to comply with privacy regulations. As would be predicted, about the same percent of respondents who state that privacy is important to their COOP plans also agree that they have implemented COOP plans that provide for privacy and regulatory compliance even during a disruption.

**My organization has in place COOP plans that ensure privacy and regulatory compliance even during a disruption.**



However, they're not nearly so emphatic: fewer than half of government agencies surveyed feel confident enough to strongly agree. What's more, a startling 20% of civilian agencies and 9%

**Note:** In the Larstan survey charts, blue denotes civilian respondents; red, intelligence/military combatant; yellow, military/non-combatant.

of military agencies do not yet have COOP plans that address privacy and regulatory compliance.

Something is amiss: Either federal agency IT groups need clarification on the regulatory requirements themselves or they lack certainty that the solutions they have implemented effectively address the requirements.

This paper is intended to clarify the role of privacy in COOP planning. It begins by summarizing laws governing privacy and safeguarding of information. Next it outlines the three main types of COOP scenarios in which privacy and regulatory compliance are most vulnerable. The remainder of the report explains network solutions that federal agencies can deploy to remain compliant with privacy and security regulations even during disruption.

### **Laws Governing Privacy and Safeguarding of Information**

The government is required to enforce an array of privacy laws including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley (GLB) Act, as well as to safeguard information that may have been submitted by the private sector in compliance with the Patriot Act and the Sarbanes-Oxley Act. At the same time, agencies must be prepared to meet the requests of citizens under the Freedom of Information Act (FOIA) and comply with foreign privacy rules such as the European Union Data Protection Directive.

*“Many of today’s compliance requirements evolved from what had been industry best practices. Now, rather than being followed by a few best-of-breed organizations, they’re mandated for everybody.”*

—Paul Reymann, CEO of ReymannGroup, Inc. and Co-Author of the Gramm-Leach-Bliley Act Data Protection Regulation

#### **Health Insurance Portability and Accountability Act of 1996**

Congress passed HIPAA to help people keep their health insurance or obtain other insurance if they lost their jobs. The law requires the Department of Health and Human Services (HHS) to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. HIPAA also contains stringent privacy provisions to protect individuals’ medical records and other personal health information maintained by certain healthcare providers, hospitals, health plans, health insurers, and healthcare clearinghouses.

#### **Gramm-Leach-Bliley Act**

The Financial Modernization Act of 1999, commonly known as the GLB Act, protects consumers’ personal financial information

held by financial institutions. GLB gives authority to eight federal agencies and the states to administer and enforce the financial privacy rule and safeguards rule. The agencies are: Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Secretary of the Treasury, National Credit Union Administration, Securities and Exchange Commission, and Federal Trade Commission.

#### **USA Patriot Act**

Congress passed the USA Patriot Act in response to the terrorist attacks of September 11, 2001. Section 326 requires financial institutions to verify the identity of their customers at account opening and report suspicious activities. Financial institutions can verify a customer’s identity by checking various databases such as the Office of Foreign Assets Control (OFAC) list, which contains names of known or suspected criminals such as terrorists and drug dealers. Other existing databases include the FBI Control List and an import/export control list designed to stop exports of strategic materials from the U.S.

#### **Sarbanes-Oxley Act**

The Sarbanes-Oxley Act of 2002 was designed to restore public trust following corporate scandals at major corporations like Enron, WorldCom, and Tyco. Most important is Section 302, which requires principal executives and financial officers to certify financial reports. Sarbanes-Oxley is not privacy legislation per se, but the SEC must hold sensitive information private until such a time when it is to be made public.

#### **Freedom of Information Act**

The Freedom of Information Act (FOIA) gives all citizens the right to request government information without having to identify themselves or explain why they want the information. All branches of the federal government must adhere to the provisions of FOIA with certain restrictions for work in progress (early drafts), enforcement of confidential information, classified documents, and national security information.

#### **European Union (EU) Data Protection Directive**

Anyone obtaining, holding and disclosing personal data within the EU must comply with a few enforceable principles of good practice. Generally, the data must be fairly and lawfully processed, processed for limited purposes, adequate, relevant and not excessive, accurate, not kept longer than necessary, processed in accordance with the data subject’s rights, secure, and not transferred to countries without adequate protection.

The EU Data Protection Directive prohibits European data processors from “exporting” the personal information of European citizens to countries that do not have adequate privacy protection laws in place. Companies may be prosecuted for wrongful transfers abroad.

## IT Infrastructure to Support Privacy and Compliance

Federal agencies can comply with and enforce privacy legislation using solutions from Cisco Systems®, which has established partnerships with systems integrators to build and deploy secure, resilient infrastructure solutions for COOP.

*“When creating COOP plans, organizations need to address all the factors relating to security, including privacy. If you simply create a quick-and-dirty COOP solution without considering all factors you consider when you design a complete infrastructure, you might open yourself to vulnerabilities that reveal themselves at the time when you most need that system.”*

— *Shailendra Sharma, CIO, Comtech*

Privacy arises as an urgent component in COOP plans in the following scenarios:

- **Connecting from home** — Providing access to the network from employees’ homes is a COOP strategy to ensure workforce resilience in the event of building damage, contamination (from anthrax, for example), and weather or other conditions that prevent travel. In these cases, employees can work from home by accessing network resources and conducting voice over IP (VoIP) over a secure virtual private network (VPN). Cisco Integrated Security — infused throughout the network — protects the privacy of traffic in transit from the employee’s home to the agency’s LAN or WAN and enables agency IT personnel to manage the connection remotely.
- **Connecting from temporary facilities** — Rapidly establishing network connectivity in a temporary facility is another COOP tactic for workforce resilience. If a building is damaged, contaminated, or destroyed, federal IT groups can quickly set up operations in another building with an “office in a box” that enables IT to provide secure voice and data communications over a VPN.
- **Backing up data to alternate data centers** — In the event of disruption to a data center, agencies can ensure application resilience by backing up the agency’s data center or core information to alternate data centers. COOP planning requires attention to the privacy of the data in transit between data

centers and between virtual storage locations. Replicating large volumes of data between data centers can be accomplished using optical disks and either Fibre Channel, Ethernet, or SONET (Synchronous Optical Network).

The remainder of this report summarizes network technologies that are effective for ensuring application and data privacy during these three COOP scenarios.

*“Instead of attaching point solutions to the network infrastructure, Cisco provides government customers with an end-to-end integrated security solution that rides on top of the networking infrastructure. This makes it easier and less expensive to manage.”*

— *Bruce Klein, Vice President,  
Cisco Systems Federal Sales Organization*

## Virtual Private Networks: Site-to-Site or Remote-Access

VPNs support federal agency COOP plans by enabling workers to perform their jobs from another facility or from their homes. The VPN creates secure tunnels through public broadband networks, keeping data private in transit by encrypting it with powerful standards such as 3DES (Data Encryption Standard), FIPS (Federal Information Processing Standard) 140-2, and EAL (Evaluation Assurance Level). Cisco offers VPN solutions that support from a few to up to thousands of tunnels.

The disruption that causes the employee to work from another site might persist for a relatively short period of time, as in the case of a biological hazard or snowstorm, or a longer time, as when a building is destroyed. Regardless, agencies can rapidly provision VPNs so that communication is quickly restored (see sidebar on page 5).

## IP Communications

Information sharing is critical in all three types of COOP scenarios: working from home, working from an alternate facility, and backing up applications and data to a secondary data center. Therefore, if the primary access system goes down, government agencies need a backup access technology that can be deployed rapidly without compromising data privacy. Time-division multiplexed (TDM) systems are prohibitively expensive and take too long to provision to satisfy COOP requirements.

The quickest and most cost-effective way to restore communications after a disruption is through IP communications, which includes IP telephony, conferencing, collaboration, voice messaging, and unified messaging. Whether or not an agency uses IP communications for day-to-day operations, IP communications is an important tool in COOP

### Rapid VPN Provisioning

Traditionally, federal agencies have had to rely on third-party service providers to provision VPNs for secure communication from employees' homes or temporary facilities. To meet COOP requirements for rapid provisioning, agencies either had to pay the service provider for pre-provisioning or pay premiums for short-notice service during times of crisis.

Cisco Systems provides solutions that enable agencies to provision VPNs without help from a service provider, for faster deployment, reduced IT burden, and lower costs. Cisco EasySecure Device Deployment services enable federal employees to establish a secure VPN connection from home or a temporary facility using a Web-based interface. The solution automates the VPN configuration based on the agency IT group's established policies. Another solution, Cisco IP Solution Center (IPC), enables IT to provision both Layer 2 and Layer 3 VPNs with quality of service (QoS), for much faster deployment than engaging a service provider.

initiatives because the call-processing platform can be located anywhere on the network, a useful capability if one or more buildings are damaged. Federal agencies can prepare an "office-in-a-box" to quickly re-establish communications after a disruption. Office-in-a-box components typically include IP phones, wireless access points, an integrated SONET router (ISR), and switch. If IT employees are unavailable, federal agencies can ensure continuity by taking advantage of Cisco Remote Operations Services (see sidebar below).

### Remote Operations Services

In catastrophic conditions when government IT employees are unavailable to perform their assigned network management duties, privacy and security may be at risk. Federal agencies can mitigate the risk of loss of privacy and regulatory compliance by using Cisco Remote Operations Services for ongoing operations management of their IP telephony networks. Services include proactively and remotely monitoring, diagnosing, and resolving IP network management problems.

IP communications supports the privacy requirement for employees working from home because they can use their VPN connection to securely make and receive calls from an IP phone connected to their PC, using their ordinary work phone number. The security characteristics of the employee's home LAN is augmented with the encryption and security offered through the FIPS 140-2-compliant encryption in the SOHO router or the VPN client running on the PC.

IP communications also protects privacy when employees work from another location instead of from home if a building is damaged, contaminated, or destroyed. Employees who relocate can simply connect their IP phones to any Ethernet connector in the new location. No assistance from IT is required because there is no need for re-cabling or entering moves, adds, or changes on the call-processing system. A secure VPN tunnel is established through the temporary network from the computer or IP phone to the agency's own VPN concentrator, which is usually located in the primary or back-up data center. Therefore, the connection is secure regardless of the characteristics of the network providing the connection.

### Storage Area Networking (SAN) and Optical Technology

Escalating storage requirements, rising management costs, and the need to share information is driving federal agencies to consolidate their storage. Consolidating multiple smaller storage devices — often one per application — improves utilization, facilitates scalability, enables access from any location on the network, and reduces total cost of ownership. Storage consolidation also simplifies privacy because IT can secure fewer storage devices.

Replicating and mirroring data between data centers and storage systems is critical for rapid recovery of applications and data in the event of a serious disruption in the production data center. The replication can be carried out over campus, metro area networks, or wide area networks, depending on the business needs, data center locations, and acceptable downtime and data loss.

Federal agencies often achieve the best results for COOP by creating a storage area network (SAN) using an optical infrastructure based on optical DWDM (dense wavelength division multiplexing), SONET, and metro IP technologies. Benefits of these technologies include:

- Privacy of data while in transit
- Reduced risk of data loss and down time
- High performance, low latency storage transport
- Cost-effective consolidation of SAN, network-attached storage, and storage management resources

Cisco solutions provide advanced capabilities for protecting data in flight between data centers and also between virtual storage locations. For federal agencies whose security requirements demand the use of encryption technologies that are not available

**Table 1 — Strategies for Ensuring Privacy**

Strategy for Ensuring Continuity and Privacy	Cisco Solution
<b>Block viruses and hacker attacks</b>	<ul style="list-style-type: none"> <li>• Firewalls</li> <li>• Intrusion detection systems (IDS) that detect unauthorized access and send an alert</li> <li>• Intrusion prevention systems (IPS) that detect unauthorized access and automatically block the attempt</li> </ul>
<b>Prevent malicious code that enters the network from causing damage</b>	<ul style="list-style-type: none"> <li>• Cisco Security Agent, which identifies anomalous behavior for a given application and stops the behavior until explicitly approved by a person</li> <li>• Cisco Network Admission Control (NAC), which scans devices that attempt to connect to the network and grants admission only if they have the latest protection software, such as antivirus and patches; non-compliant devices are directed to another site for remediation</li> </ul>
<b>Protect sensitive information from disclosure to unauthorized people, either internal or external</b>	<ul style="list-style-type: none"> <li>• VPNs</li> <li>• Encryption</li> </ul>

to the public, Cisco SAN solutions can be integrated with third-party proprietary encryption products.

**Policy-Based Access**

During disruptions, agencies must provide access to the information employees need to ensure service continuity — possibly from home or another remote location — while preventing unauthorized access to information. In these cases it might be necessary to quickly authorize or restrict information access in order to facilitate rapid decision-making among collaborating agencies.

*“Infrastructure systems need to be able to support agency policies. On a policy level, it is critical to decide the types of data that can be shared and who should be allowed to access it.”*  
 — John Morrell, Director of Marketing, Cisco Systems

Cisco end-to-end security solutions enable policy-based access to information. For example, Cisco Identity-Based Networking Services (IBNS) identifies users and devices using strong authentication technologies, and then allows or restricts access to content and applications according to the agency’s policies. That is, a user’s ability to access specific content or applications depends on the user’s role, department, or other attributes. Administrators can quickly adjust access policies or applications as the business need warrants, and the new policy is implemented immediately and automatically.

As a corollary to providing policy-based access, agency IT groups must ensure that employees who access the network from remote locations do not infect the network and thereby disrupt continuity. Cisco Security Agent protects applications against unknown threats before they can disrupt operations by detecting anomalous application behavior and blocking the behavior until approved by an administrator.

**AAA and Encryption**

Even in normal times, workers may inadvertently compromise the security of sensitive data by leaving their PCs on and unattended, or by writing down their passwords where they might be seen. Emergencies exacerbate the risk because people are more likely to inadvertently reveal their passwords in the mayhem, or to intentionally share their passwords as they scramble to perform critical functions from a remote site. What’s more, emergency response personnel such as firefighters and police officers, who ordinarily do not have security clearances, might enter the building and potentially gain access to sensitive data.

Agencies can comply with privacy regulations by using authentication, authorization, and accounting (AAA) systems, the public key infrastructure (PKI), and encryption. AAA solutions provide:

- Authentication: The person is who he says he is.

- Authorization: The person has the right to access that data.
- Accounting: The person's network actions are tracked.

The authentication component is accomplished using a PKI. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using his or her own private key. Network solutions from Cisco Systems support a wide variety of encryption schemes used within a PKI, including 3DES, FIPS 140-2, and EAL.

### Antivirus Protection and Intrusion Protection Systems

The volume and speed of network threats such as viruses, worms, and distributed denial-of-service (DDoS) attacks is increasing exponentially. They threaten continuity and make agencies vulnerable to privacy breaches and loss of compliance with regulatory requirements. To ensure COOP and protect privacy, agencies need three types of network security, illustrated in Table 1 (previous page).

The Cisco Self-Defending Network concept was conceived to provide proactive protection by automatically identifying, preventing, and stopping threats. Unlike "point" security solutions that are not integrated and can themselves be compromised, Cisco Self-Defending Network solutions are integrated into all layers of the network. For example, a traditional IDS recognizes malicious traffic and sends an alert to a person, who generally has to take manual steps to block the traffic. In the intervening seconds or minutes, privacy and security can be violated. Because Cisco solutions are integrated, the IDS can instantly send a message to the firewall to block the traffic, for proactive intrusion prevention.

*"The Cisco Self-Defending Network extends traditional endpoint security to create a secure infrastructure that continuously, proactively manages risk."*

*—Paul Reymann, CEO of ReymannGroup, Inc and Co-Author of the Gramm-Leach-Bliley Act Data Protection Regulation*

### Summary

The **Larstan Business Reports** survey suggests that federal agencies lack certainty that the privacy component of their COOP plans is adequate to ensure regulatory compliance during a disruption. Agencies can validate that their current COOP approaches address privacy requirements by confirming that privacy is assured when employees work from home or from alternate facilities, and when data is replicated to alternate data centers. Cisco Systems offers solutions and services to help government protect privacy during COOP scenarios. With privacy solutions in place, federal agencies fulfill their fiduciary responsibility to protect sensitive citizen and government data and to comply with regulations designed to protect the public trust and security.

To view the entire results of the Larstan Continuity of Operations Survey, go to [www.larstan.net/COOP](http://www.larstan.net/COOP). For a full range of Larstan reports and surveys, go to [www.larstan.net](http://www.larstan.net).

### Resources:

Cisco Systems, Inc. is the worldwide leader in networking for the Internet, celebrating 20 years of commitment to technology innovation, industry leadership, and corporate social responsibility. Cisco IP networking solutions can help government organizations increase their productivity, improve safety and effectiveness, maintain continuity of operations, and reduce operating costs.

Chris Shenefiel, Federal Government Industry Solutions Manager, Cisco Systems: 703-484-5729, [cshenefi@cisco.com](mailto:cshenefi@cisco.com)