Securing Data at Rest in a Mobile Environment

White Paper

June 2007
Securing Data at Rest in a Mobile Environment

Section I: Introduction

Federal agencies today more than ever before, operate in a complex mobile environment, involving multiple sites and a dispersed workforce. Given their access to portable electronic devices such as laptops, PDA’s, and smart-phones, coinciding with various teleworking initiatives, today’s federal employee carries the capacity to perform their job in just about any location. However, along with increased mobility comes increased concern about the security of government data.

Telework, in particular, has been cited as an area of immense concern. When the Federal Telework Legislation was passed in 2000, the major focus appeared to be on meeting the congressional mandate that within six months, 25% percent of the eligible federal workforce had to be able to telework to the largest extent possible. However, with the recent wave of data protection breaches across the federal government, scrutiny of data security is at an all time high. Government organizations have experienced exploitation of government data in areas of classified information, personnel data, and financial information of millions of federal employees and citizens.

However, these issues do not diminish the critical requirement for transitioning to telework for federal government employees. While data security in teleworking is of obvious importance, the value of teleworking and remote access to information becomes critical in the case of a major disaster or other situation to ensure the federal government’s continuity of operations (COOP). Many of the federal civilian agencies that collect and handle personal information also depend on remote access to data such as tax records, medical information, and social security numbers.

Furthermore, while there are obvious physical security measures agencies can employ for data security, this alone will not suffice to ensure appropriate protections of government information resources in today’s teleworking environment. Thumb drives, for instance are easily concealable, can pass through metal detectors, and can be easily lost by agency personnel.

Therefore, it is imperative that federal agencies develop and employ a comprehensive approach to protect their critical information resources, and the technology used to transmit, store, and process it. Ad-hoc and stove-piped approaches only serve as temporary or “band-aid” solutions. Federal agencies today are operating in a world where unauthorized access to military or homeland security documents can threaten our national security, compromise personal information, and lead to identity theft. Additionally, intellectual property rights must be preserved for US citizens and businesses.
The timeliness of securing data could not be more critical. Agencies must take a strong comprehensive stance in securing their data before incidents occur or risk repercussions down the line.

Section II: Securing Data

As government agencies conform to cross-agency and inter-government data sharing and collaboration requirements, agency CIOs need to implement data security processes that protect their information resources, as well as ensure the security required to meet demands of a mobile environment. More and more federal agencies are using shared resources of data today and must be required to support and implement prudent security measures to ensure the information they manage is protected to the degree required by law, agency regulations, and due diligence.

It is important that federal agency CIO’s carefully consider the needs of their users and implement comprehensive security policies, such as use of role-based data security, in which access to particular data is granted only to those who need it based on their role in the organization. For example, a human resources professional would logically need to access a mailing address for a particular employee; however, a program manager should not. Security controls should limit the type of data access the professional has, as a mailing address may require minimal protection, whereas salary information and social security numbers would no doubt be considered data requiring safeguards commensurate with the mandates of both the law and agency policies.

“Software-based data security measures must be centrally administered to be effective at preventing intrusion,” said Bruce Brody, former CISO of the Department of Energy and Veterans Affairs. According to Brody, “voluntary network security measures are only as good as their enforcement mechanisms,” - the best way to ensure adherence to rules is to push compliance to the users, thereby removing negligent or willful circumvention of data networks.

Telework

On October 23rd 2000, the Federal Telework Legislation was passed and required that:

> Each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the maximum extent possible without diminished employee performance

The legislation further stipulates that no later than 6 months after the date of the enactment, the Director of the Office of Personnel Management shall provide that the requirements of this section are applied to 25% of the federal workforce

---

The United States Congress gave several reasons for enacting the legislation: relieve overcrowding; lower real estate costs; reduce absenteeism; cut gas consumption; relieve traffic congestion in the Washington D.C. area; and to provide jobs to the disabled.\(^2\)

Not surprisingly, however, the issue of data security in telework has been in the spotlight. Recent security breaches have called for increased security among federal workers, especially those who perform their work on mobile laptops and have access to other mobile devices.

“What this has done is shift the focus from meeting the congressional mandate to enhancing security and establishing continuity of operations planning,” said Tom Simmons, Area Vice President of U.S. Government Operations at Citrix Systems of Florida.

In addition to the security concerns, telework is also facing cultural resistance among federal agency managers. In a 2006 survey conducted by the Telework Exchange and the Federal Managers Association, 67% of federal managers surveyed said fear of losing control over employees remains a major concern along with lowering their workers’ overall productivity. However, the same survey reported a 75% favorable impression of the telework initiative overall.\(^4\)

\[
\text{“Many managers don’t believe telework is a priority for their agencies.”}
\]
\- Darryl Perkinson, President of Federal Managers Association

“The study highlights the disconnect between the perception of telework and the practicality of telework. The survey suggests that many managers don’t believe telework is a priority for their agencies. In addition continuity of operations (COOP) and pandemic planning don’t appear to be significant factors promoting telework. FMA believes that it shows managers are out of step with their agencies,” said Darryl Perkinson, National President of Federal Managers Association (FMA).

**Section III: Necessity of Security for Data at Rest**

In the past year, federal government departments such as the Departments of Agriculture, Energy, IRS, Navy, Transportation Security Administration (TSA), and Veterans’ Affairs (VA) have reported incidents of computer systems being exploited, stolen or lost notebooks, and the accidental release of data. The most significant of all of these breaches concerned Veterans' Affairs in 2006.
The VA incident began with the theft of a laptop from the home of an employee which contained information on 26.5 million veterans and service members. The repercussions within the agency were severe: the employee who took the laptop to his home was terminated and his superiors submitted their resignations, as did numerous other senior VA officials. Congressional hearing resulted in severe criticism of VA leadership and the culture it had fostered. Finally, legislation elevated the position of VA Chief Information Officer (CIO) to Undersecretary, and modified the Federal Information Management Act (FISMA) to clarify the enforcement authority of the CIO.5

“What people don’t realize is that the agencies already have the authority to deal with this scenario,” said Steve Benowitz, Former Associate Director at Office of Personnel Management (OPM). “They can restrict the use of government—owned laptops from personal and other forms of use not related to government work.”

One of the most recent losses of data took place in May of 2007 at the Transportation Security Administration (TSA). An external hard-drive that contained payroll data of about 100,000 current and former employees, including their Social Security Numbers, bank account and bank account routing information was either lost or stolen. The hard-drive was discovered missing from a controlled area at the TSA headquarters’ Office of Human Capital in Arlington, Virginia.6

**Government Policy and Legislation**

In light of these recent breaches, the federal government has enacted several initiatives and legislation to prevent these scenarios and also to promote teleworking within agencies.

- **The Office of Management and Budget’s (OMB) Memorandum M-06-16** includes a security checklist that recommends best practices for the protection of personally identifiable information as determined by the National Institute of Standards and Technology (NIST)
  - NIST has published its Federal Information Processing Standard (FIPS) 140-2 for encrypting data
- **The Office of Management and Budget’s (OMB) Memorandum M-07-16** issued to federal agencies on safeguarding against and responding to the breach of personally identifiable information
- **The Federal Information Security Management Act (FISMA) of 2002** continues to be a market driver in secure data initiatives. Following the release of the 2005

---


© 2007 by INPUT. All rights reserved.
FISMA grades in which the government received an overall grade of a “D plus,” the 2006 result was only slightly better with a “C minus”

- **The Federal Agency Data Breach Protection Act** introduced by Representative Tom Davis (R-Virginia) would require agencies to better protect the sensitive data they collect and promptly notify those whose data is lost or stolen
  - The act further directs OMB to establish practices and standards for informing citizens of lost data and provides a clear definition of the type of sensitive information to which the law would apply

- **The Notification of Risk to Personal Data Act** was introduced by Senator Dianne Feinstein (D-California) which would protect individuals from identity theft by requiring agencies and businesses to notify consumers in the event of a security breach that exposes their personal data.

- **The Personal Data Privacy and Security Act of 2007** sponsored by Senators Patrick Leahy (D-Vermont) and Arlen Specter (R-Pennsylvania) would notify individuals with provisions identical to Feinstein's bill, but on a more comprehensive scale.

Telework has also seen some recent urgency in Congress:

- **Telework Enhancement Act of 2007** a bipartisan act introduced to the Senate in March 2007, by Senators Ted Stevens (R-Alaska) and Mary Landrieu (D- Louisiana), under which agencies will be required to designate a Telework-managing Officer. This officer would be responsible for implementing Telework programs, serving as a liaison between employees and managers.

**Disaster Recovery and Continuity of Operations (COOP)**

Federal Continuity of Operations (COOP) program guidelines mandate that essential government functions must be carried out in an emergency from remote locations. Critical to implementing an effective COOP program is the use of portable devices normally used in a teleworking capacity in non-traditional and non-secure environments. Whether government workers use smart-phones, flash-drives, or other devices, to provide a seamless transition in services, sensitive data is at risk in these dynamic mobile environments.

A recent GAO report found that although agencies are not required to use telework in continuity planning, about 39% of the agencies that were surveyed reported plans for essential employees to telework during a COOP event. This is up from 13% defined in a previous GAO survey. One reason for the low level of preparation is that FEMA has not provided enough specific guidance on capabilities and policies needed to use telework during
emergencies. This prompted the White House to announce the release of an implementation plan in support of the National Strategy for Pandemic Influenza. This plan calls on OPM to work with DHS and other agencies to revise existing network guidance and issue new guidance on human capital planning and COOP.

The value of remote access to information is central in Disaster Recovery and COOP scenarios, as well as military operations and intelligence activities. Many civilian agencies that collect and handle personal information also depend on remote access to tax records, medical information, legal case documents, and social security numbers.

**Accelerated Adoption of Mobile Devices**

The new generation of portable devices, such as laptops, handhelds, PDAs, and smartphones, make it easier than ever before to perform work functions away from traditional workplaces and physically-secure office environments. While mobile computing opens new application areas, it can introduce vulnerabilities to attacks, varying from inadvertent actions to deliberate, aggressive interferences with operations. These new devices retaining organizational information have limited computing power, memory, interfaces, and battery life, which impose new constraints on the practicality of applying safeguard standards. Because mobile computing devices are designed to be lightweight and portable, they are most easily susceptible to loss or theft. And because these mobile devices are meant to access networks remotely, they offer the easiest entry for unauthorized access.

**Section IV: A Comprehensive Approach to Securing Data at Rest in a Mobile Environment**

The inverse relationship between the need for a stronger comprehensive approach to data security and the increasing number of mobile devices in telework used by federal employees will surely continue for the foreseeable future. It is critical for agency personnel to realize there is not just one approach or list of best practices that will be the answer to securing data. Rather, agency security officers must not only employ a comprehensive approach to data security but, due diligence demands, they must remain ahead of the federal security mandates and evolving data security requirements. Too often, an agency that relies on federal mandates will find itself more vulnerable to data breaches. One cannot expect lawmakers to remain ahead of the threats to organizational information resources.

The optimal solution to the data security issue will be one that ensures the protection of: the data; the infrastructure; the endpoints; and all devices used in a teleworking environment.

---

7* Continuity of Operations; Agencies could improve planning for Telework during disruptions*, Statement of David M. Walker, Comptroller General of the United States before the Committee on Government Reform, House of Representatives, May 11, 2006

© 2007 by INPUT. All rights reserved.

A publication of INPUT, 10790 Parkridge Boulevard, Suite 200, Reston, VA 20191
Phone: 703-707-3500    Fax: 703-707-6201    www.input.com
Federal CIO’s must become familiar with government and industry trends for securing their mobile environments. They then must institute agency-wide security practices ensuring all users understand the consequences of using their mobile devices.

Protecting the Data Infrastructure

Agency CIO’s need to implement security processes that not only protects the critical information resources within their boundaries, but ensure their security policies are enforced with their data regardless of where it is being used.

Agency CIO’s must ensure that their enterprise applications and access to the data infrastructure are reliable, responsive and resilient. This process requires the simplification and standardization of operations across the essential elements of the data infrastructure while ensuring service delivery on standard software across application, server, and storage platforms. To enhance protection of the data infrastructure:

- Deploy data protection from desktops to vaults across storage networks to ensure performance and efficiency
- Centralize backups at remote sites through web-based tools and simplify administration, data recovery, and compliance
- Employ metrics in order to quickly resolve problems and restore performance to required levels

Enabling Safe Mobile Data Devices

It is inevitable that some government functions will be performed away from traditional physically-secured government facilities. Furthermore, as teleworking continues to gain momentum, we must assume the number of these functions will increase as well. It is therefore imperative for federal agencies to ensure that the types of mobile data devices being used to store, transfer, and process data have the appropriate safeguards are employed to manage the risk. If these devices are lost or stolen, agencies must also ensure that the data remains accessible only to authorized federal employees.

Enabled flash cards armed with software encryption protects data with complex algorithms, and some cards provide a layer of hardware encryption on top of the software limiting the number of attempts to access data on the mobile device. This makes the algorithm immune from unauthorized personnel using an algebraic “brute-force” attack. Some mobile devices offer biometric barriers to unauthorized entry as another option. Finally, various mobile devices can be equipped with a fingerprint reader right on the device that cannot be used by non-registered users.

---

In fact in May 2007, Veteran’s Affairs awarded a contract to Kanguru Solutions for 25,000 encrypted USB thumb drives. These drives are equipped with 256-bit encryption and meets NIST’s FIPS 140-2 for encrypting data and these thumb drives can now carry no more than up to 8 gigabytes, depending on the security level of the individual employee.\(^\text{10}\) “The effort is to drive down the use of thumb drives,” said Bob Howard, the VA CIO. “This will help us eliminate future problems by shutting down an easy way to take massive amounts of data out of the office.”\(^\text{11}\)

**Enabling Safe Data Transfer**

To manage the flow of information in transit over a network, federal agencies need to minimize risks and interruptions by using a layered approach that stops potential threats at network gateways, the end-users, and in archiving and storage systems. Secure solutions must ensure that only relevant email messages and other data transfers are delivered and stored in a protected, yet accessible, location.

Other portions of the overall solution must include protection against spam, fraud, viruses and spyware. This includes a variety of protective technologies central to which is accomplished by leveraging traffic-shaping technologies that eliminate unwanted-email at the source. Finally, threat protection software must be enabled for all network tiers across all enterprise mobile devices.

---

**Securing Data in a Mobile Environment Quick Checklist**

*Former CISO of the Department of Energy and Veterans Affairs Bruce Brody, stated that “For any CIO or CISO in a federal agency that is looking over the security aspects of their infrastructure, he or she must know with 100% certainty at all times the following:*

1. What are the boundaries and topologies of the interconnected enterprise?
2. What mobile devices are on that enterprise?
3. What are the configurations of the mobile devices?
4. Who is accessing those devices?
5. And finally, what are they doing when accessing those devices?”

---


Enforcing Data Integrity Protocols and IT Policy Compliance

Federal agencies should recognize the environment where data has to travel: disparate networks; potentially compromised computing environments; and instances where data can be easily removed from its storage area. The challenge facing agencies today is how to mitigate these risks while staying abreast of vulnerabilities of new technologies being introduced on a daily basis. Agencies must adopt protocols stipulated by NIST ensuring mobile devices and data security procedures, but agency managers should be well aware of technology advances that could place them one step ahead of NIST requirements.

When making technology procurement decisions, agencies should buy devices that define, measure, report on, and demonstrate the compliance of information systems against security policies, standards, and federal government regulations.

Necessity for Adoption and Challenges

Federal agencies that find themselves lagging behind guidelines set forth by NIST and OMB, may find themselves vulnerable to a large organizational changes should their data centers become compromised. The most obvious example can be found in the Veteran’s Administration, where several senior officials resigned or were terminated as a result of the potential loss of sensitive government records. In addition, the agency has attempted to expend nearly $200 million dollars in end-of-year IT dollars to shore up its infrastructure. While this may be good news for vendors, there are challenges to face in this arena.

The data loss incident at the VA was the result of a long trail of problems; two of the most significant are a decentralized network and organizational structure. They formed the basis for the information security failures in the department. The culture of resistance to a centralized authority (i.e., Washington DC headquarters) is systematic where headquarters-initiated information security policies often are ignored or misunderstood by field offices. Furthermore, the current citizen-centric program and funding model results in decentralized operating units and, as a result, decentralized IT networks.

At this point FISMA may be regarded as having ‘a lot of bark, but little bite’
- Prabhat Agarwal, Manager of Information Security Analysis at INPUT

Finally, there is some speculation that the efforts of FISMA and OMB are going unheeded. “FISMA may come out with grades that say you better shape up, or else. But the fact of the matter is that no one has stated what the ‘or else’ will entail,” stated Prabhat Agarwal, Manager of Information Security Analysis at INPUT. “There may be some pressure in terms of funding levels, but at this point FISMA may be regarded as having a lot of bark, but little bite.”

Section V: Conclusions

There is no doubt that there are some potential substantial benefits to be gained by incorporating a secure data environment into the telework initiative. Agencies are able to perform their mission faster and more efficiently from dispersed locations. Smart implementations of a protected data network will further drive valuable government goals, such as telework, COOP, and data sharing between agencies.

To effectively realize these benefits, federal agencies must create an environment where the benefits of mobile technology and secure data can be realized without compromising the security of government networks and critical information assets. To do so, government agencies must ensure that the data infrastructure and those who access it will not pose undue threats. The very first step that must be made is a comprehensive organizational effort to ensure the data computing environment is secure at every instance: at the enterprise level and on any device, including laptop, PDA, and thumb drive that can interface with the network.

Finally, agencies must educate their staff on the appropriate use of technology in a mobile environment that does not needlessly expose data networks to exploitation. Agency CIO’s must put in place policies and regulations that prohibit the use of unauthorized access and devices while promoting proper and responsible use of authorized devices.

About the Sponsor: Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance.

Symantec helps enterprises manage IT risk and maximize IT performance by standardizing and automating their software and processes. The company delivers solutions for storage, security, information management, business continuity, IT operations and IT compliance. For
consumers Symantec offers security, data backup and PC tuneup solutions that protect consumers’ connected experiences so that they can enjoy the best of what the online world has to offer.

Customers benefit from the breadth of Symantec’s industry-leading technology, research and response capabilities as well as the diversity of our customer base and global reach. Symantec’s open approach to serving customer needs helps to ensure that the enterprise solutions are interoperable across multiple platforms and operating systems. In addition, solutions are backed by Symantec’s Global Intelligence Network, one of the most comprehensive sources for Internet threat data in the world.