



**RSA**

The Security Division of EMC

RSA Solution Brief

## **Securing Remote Access in the Federal Government: Addressing the Needs for Telework and Continuity of Operations**

The Telework Improvements Act of 2009 that was introduced earlier this year would expand and improve telework programs in the Federal government, allowing employees to work remotely at least 20 percent of the time. According to a report released by the Office of Personnel Management, while 60 percent of federal agencies had included telework as part of their continuity of operations planning, only 7.6 percent of employees eligible to work remotely did so in 2007.

The proposed legislation to implement a uniform and consistent telework policy across federal agencies offers many valuable benefits:

- Increases employee productivity
- Enables continuity of operations
- Reduces operating costs
- Reduces environmental impact
- Promotes work/life balance

While telework numbers are small within the federal government, the threat of natural disasters or a pandemic, like the scare that resulted from the recent Swine Flu outbreak, serves as a reminder to government agencies the importance placed on establishing a viable plan that would enable a mobile workforce to be deployed quickly in the event of a business disruption.

#### **Layered Security for Telework**

Teleworking offers many benefits, yet it also introduces a number of risks to government networks. The traditional view of securing remote access has focused on strong authentication to assure the identities of users accessing internal systems from outside the organization. However, the sophisticated nature of the cyber threat environment and increasing number of attacks against the federal government require a layered approach to security to ensure the highest levels of protection.

This paper examines several best practices that federal agencies can follow.

The sophisticated nature of the cyber threat environment and the increasing number of attacks against the federal government require a layered approach to security to ensure the highest levels of protection.



---

## Best Practices

---

### Best Practice #1

*Data discovery and classification. Identify where sensitive or classified data resides within the organization and categorize it by its risk level.*

Not all data is of equal importance from a risk management perspective. The first step to ensuring telework security is to discover where sensitive data resides and determine which data is most sensitive or at greatest risk to be targeted. By discovering sensitive data and classifying it according to its risk level, government organizations can define appropriate policies for handling that data – from which employees and applications are authorized to access this data and how, when and from where they are allowed to access it. For example, a teleworker logging in from a government-owned laptop may be able to access most resources while a teleworker logging in from a mobile device may have access to a limited set of resources.

The following RSA service helps government organizations identify where sensitive data resides and effectively classify it according to its appropriate risk level:

The RSA® Data Loss Prevention (DLP) RiskAdvisor Service provides a full understanding of where sensitive data exists across the organization. To achieve this, RSA Professional Services leverages the RSA® Data Loss Prevention Suite for automated discovery of sensitive data and provides a snapshot of potential exposure. The RiskAdvisor Service encompasses a high-level mapping of internal processes and functions to sensitive data to help determine potential risks.

RSA provides a final report which summarizes the list of machines scanned, a list of files found containing sensitive data and a profile of the incidence sensitive data appears within those files. It also includes a series of recommendations on how to optimize processes to protect sensitive data and establish a foundation for preventing data loss.

### Best Practice 2#

*User identification and authentication. Ensure users are uniquely identified and authenticated before granting access to government systems. Utilize a risk-based approach that aligns authentication mechanisms with the user, the telework device and type of access granted.*

Upon determining where sensitive data resides, it is important to implement strong authentication to uniquely identify each user requesting access to those resources. A core part of implementing an authentication solution and determining what level of authentication to apply requires that organizations consider the risk posed by several factors including:

- **The value of the data.** The more sensitive or classified the data is and the higher the risk to an individual or agency if accessed by an unauthorized user will determine the authentication mechanism that is needed to protect it.
- **Planned usage.** Who are the user(s), what types of data are they accessing and what activities do they perform.
- **Needs of the end user population.** From the user's perspective, organizations must consider things such as ease-of-use and the user's willingness to adopt. From the organization's perspective, they must consider things such as total cost of ownership, training requirements and scalability to end users.
- **Client device.** Depending on the type of device being used for remote access, whether a laptop or a mobile device, organizations may determine additional authentication layers are needed.



RSA offers a number of choices for strong authentication so government organizations can ensure that critical resources are secured and only accessed by trusted users. RSA's authentication solutions enable organizations to balance risk, cost and end user convenience.

RSA® Adaptive Authentication is a strong authentication and fraud detection platform that offers cost-effective protection for an entire user base. Adaptive Authentication secures access to:

- Websites & portals
- SSL VPN applications
- Web Access Management applications

Adaptive Authentication conducts a risk assessment of all users behind-the-scenes by measuring a series of risk indicators, including a user's device and behavioral patterns, to positively assure a user's identity. Adaptive Authentication generates a unique score for each activity. If an activity exceeds a predetermined risk threshold (as customized by each organization), the user is prompted to provide an additional authentication credential to validate his identity. If the activity falls below the risk threshold established by the organization, the user is permitted to proceed without interruption.

Adaptive Authentication now protects nearly a quarter of a billion (225 million) online users worldwide. It is currently deployed at over 8,000 organizations in the healthcare, financial services, government, insurance, automotive, real estate, manufacturing and pharmaceutical industries.

RSA offers a number of choices for strong authentication so that government organizations can ensure that critical resources are secured and only accessed by trusted users.

RSA SecurID authentication offers a wide variety of token form factors



RSA SecurID® two-factor authentication is based on something you know (a PIN or password) and something you have (an authenticator). The authenticator generates a new one-time password code every 60 seconds, making it very difficult for anyone other than the genuine user to input the correct code at any given time.

To access resources protected by the RSA SecurID system, users simply combine their secret personal identification number (PIN) with the unique one-time code displayed on their authenticator. RSA SecurID authentication offers a wide array of one-time password authentication form factors including hardware authenticators, software authenticators for mobile devices and a software toolbar.

The RSA SecurID On-demand Authenticator enables teleworkers or contractors to securely access the network without pre-assigned credentials. The On-demand Authenticator is a "tokenless" access method requiring no hardware authenticator or software to be installed on the end user's device. It is an ideal solution to ensure continuity of operations in the event of a pandemic, natural disaster or other business disruption.

The On-demand Authenticator utilizes a self-service web URL where a user requests a one-time password. From an Internet-capable computer, accessing the interface requires traditional login and PIN/password combination. Upon successfully completing this phase, a one-time password is generated by the RSA Authentication Manager® sever and sent to the user's mobile device (pre-registered in the data store) via Short Message Service over the public cellular network. E-mail delivery is also supported.



### Best Practice #3

*Centrally manage and control access privileges to critical government systems based on risk, business context and user role. Require additional authentication be provided for users accessing the most sensitive data.*

As teleworking begins to increase within the government and remote access is extended to more users – each with their own unique access privileges – a new set of threats and challenges are imposed. As a result, organizations must initiate controls to mitigate risk. Some of these challenges might include the absence of a consistent framework for managing access control policy across multiple applications or ensuring the right users have the appropriate access to the government systems and applications needed in order to effectively perform their job.

Provisioning is essential to the process of defining policies for access to government systems and implementing those policies by creating IT accounts with the appropriate access rights, as dictated by each organization's unique telework policies. Provisioning involves creating, managing and terminating end user accounts, along with their associated access rights and entitlements, based on those policies.

Combining provisioning with role-based access can reduce the complexity of user administration by mapping a potentially large number of users with related functions into a smaller number of well-defined IT accounts and entitlements, thereby increasing efficiency and ensuring ongoing user security and access policy management.

As an added benefit, by integrating authentication with web access management (WAM), government organizations can provide an additional layer of security for teleworkers attempting to access the most sensitive or classified resources. For example, an organization may deem certain files that are highly classified can only be accessed once a user has passed an additional authentication step (sometimes referred to as step-up authentication). The process of invoking step-up authentication can be set up directly within the WAM application. To demonstrate, an organization may use risk-based authentication as the central mechanism for authenticating all users and deploy a one-time password solution as a form of step-up authentication for users that will be accessing highly sensitive information on a regular basis.

RSA® Access Manager provides secure access to Web applications in intranets, extranets, portals and exchange infrastructures from a single administrative console. With RSA Access Manager, organizations can centrally assign access privileges to ensure that only authorized users can access sensitive data within web-based applications – ensuring the right people have the right access at the right time. These privileges can be determined by select attributes, such as job function and responsibilities, and can be readily turned off if a person is terminated or takes on a new job role that does not require access to certain government systems.

#### Built-in vs. Bolted-on

By deploying authentication and authorization products that work together, administrators can initiate a policy vision based on security architecture – as opposed to a one-off solution. For instance, when users are authenticating using RSA Adaptive Authentication, they are assigned a risk score for each action they take (such as logging into an online account). This score is then used to determine if a stronger level of authentication is needed. It is then passed along to RSA Access Manager which determines, based on existing policies as well as the risk score, if the user should be given access to a given application or website.



Combining provisioning with role-based access can reduce the complexity of user administration by mapping a potentially large number of users with related functions into a smaller number of well-defined IT accounts and entitlements.

RSA Access Manager manages all authentication and authorization requests utilizing the risk-based capabilities of Adaptive Authentication. Organizations can establish policies to require additional authentication for access to certain data or resources in the event a logon or activity is assigned a high risk score by the Adaptive Authentication system.

RSA® Entitlements Policy Manager is a centralized authorization platform which extends web access management solutions by providing policy-based, fine grained controls to granular resources that contain sensitive data while preserving identity context. RSA Entitlements Policy Manager enables security officers to discover, manage, monitor, enforce and audit access controls across government applications. RSA Entitlements Policy Manager is built on a strong architectural foundation leveraging industry standards such as XACML and SAML creating a scalable and extensible system for government applications.

AccountCourier®, from RSA partner Courion Corp., is a user provisioning solution that automates the process of creating and managing user accounts and access rights across a wide range of systems, including web-based applications. RoleCourier®, from Courion Corp., is a role management solution that simplifies security and access policy enforcement by creating user roles that align business functions with IT accounts and access rights. This ensures that users are assigned only the level of access rights that are necessary to perform their job duties.

Both work seamlessly with RSA's authentication and authorization products to ensure teleworkers are provided with appropriate access rights and privileges.

#### How it works

1. RSA Access Manager determines, based on configurable policies – Smart Rules® – if a given action requires authentication. Actions include logon and transactions.
2. RSA Adaptive Authentication assigns a risk score to determine if a given activity is fraudulent.
3. Smart Rules functionality determines if secondary authentication is required based on the risk score and configurable policies.
  - a. If secondary authentication is not required a user is considered authenticated.
  - b. If secondary authentication is required RSA Access Manager determines which authentication method to use.
4. RSA Access Manager determines if a user passes or fails the authentication challenge.
5. Once a user is authenticated RSA Access Manager determines, based on configurable policies, if a user has permission to access a specific resource.



#### Best Practice #4

*Select and implement appropriate data controls based on risk levels and where sensitive data resides. Apply and enforce policies to control your data from loss or misuse.*

In establishing a telework policy, organizations should assume that anything done outside the network opens up the door for threats that could potentially put data at risk. Data controls that enable policy-based protection of sensitive data whether transmitted over the network or in use on a laptop, desktop or mobile device is essential.

Building effective policies by specifying the usage and handling rules based on the risk levels of data is important for determining when a violation has occurred and how that violation should be handled. Depending on the user, the device and the type of access granted, government agencies should define a broad set of usage conditions and handling rules that align to their specific data protection needs.

Data discovery and classification becomes key when it becomes necessary to establish data controls. In addition to offering a variety of policy capabilities with a wide range of handling options (e.g. encryption, quarantine, alerts, etc.), a data loss prevention (DLP) solution must ensure accuracy in identifying data that is intended to be protected. For example, if the wrong data is being singled out, it will not matter what remediation options are established to protect the data. Or worse, if documents or files with sensitive data are overlooked and policies are not established to protect them, this could increase the risk of inadvertent exposure at a later time.

The RSA Data Loss Prevention Suite offers a comprehensive data loss prevention solution that discovers, monitors and protects sensitive data in motion over the network, in use on a laptop, desktop, or mobile device, or at rest in a data center. The RSA DLP Suite provides a policy-based approach to securing data, enabling government organizations to classify their sensitive data, discover where it resides, enforce data controls and report and audit appropriately as mandated.

The RSA Data Loss Prevention Suite is offered in three distinct modules:

- RSA® Data Loss Prevention Network
- RSA® Data Loss Prevention Endpoint
- RSA® Data Loss Prevention Datacenter

RSA DLP Network and RSA DLP Endpoint are important components for establishing data controls for teleworkers.

#### Protect PII as it moves across the network

RSA DLP Network identifies and controls sensitive data as it is transmitted throughout the network and enables policies to be enforced across areas such as corporate email systems, web-based email systems, instant messaging and web-based protocols. RSA DLP Network can identify sensitive information through the analysis of the data inherent in a transmission and prevent data loss if a policy is violated using a number of different handling options.

#### Protect PII on laptops and portable devices

RSA DLP Endpoint identifies and controls sensitive data on endpoints such as laptops, desktops and mobile devices. RSA DLP Endpoint has the capability to monitor the usage and movement of sensitive data on endpoints, even as it is moved to external media such as USBs or CD/DVDs. RSA DLP Endpoint can enforce and control end user actions that violate policy using a number of different handling options.

Organizations should assume that anything done outside the network opens up the door for threats that could put data at risk.

## Best Practice #5

*Monitor for suspicious events that affect the confidentiality of sensitive data or indicate eavesdropping or interception of government networks. Investigate potential security risks or violations and take corrective action. Report to meet compliance requirements, as necessary.*

Government organizations are prime targets for malicious threats attempting to gain access to systems and data. Telework from external locations opens government systems up to greater risk for eavesdropping or interception. In order to combat these risks, organizations require real-time tracking and correlation of security events in order to identify potential threats and respond quickly to change.

Security information and event management (SIEM) systems enable organizations to analyze and report on security logs and real-time events occurring across the network. To enable proper auditing of the data security infrastructure, a SIEM system is needed that automatically collects, manages and analyzes the event logs produced by each of the security systems, networking devices, operating systems, applications and storage platforms deployed throughout the organization.

These logs monitor systems and keep a record of security events, information access and user activities both in real-time and for forensic analysis should a high-risk event occur. By correlating events in data control systems in real-time, organizations can quickly respond to incidents as they occur, reducing the risks of potential threats posed by teleworking.

The RSA enVision® log management solution turns raw log and event data into actionable information to help government organizations identify and respond to high-risk events and simplify reporting requirements. The RSA enVision platform offers comprehensive correlation, analysis, monitoring and alerting capabilities to make it easy to consolidate and review daily logs from different systems, including logs from all critical intrusion detection, authentication, authorization and accounting protocol servers.

The RSA enVision platform establishes a centralized point for tracking and monitoring all access to systems - from the users that access it to the activities they perform - and if those attempts are valid. With the RSA enVision platform, organizations can create custom watch lists for teleworkers to look for multiple login failures or and other security-related events that may be deemed potentially suspicious, whether successful or not. In the case of a high-risk event, the RSA enVision platform will automatically deliver a notification to assigned security personnel in real-time.

The RSA enVision platform also provides insight into an organization's most vulnerable assets. Through a user-friendly dashboard, the RSA enVision platform displays an organization's most vulnerable assets based on severity, business rating and those that have been least scanned. This enables organizations to be proactive and prioritize their most vulnerable assets and apply the appropriate patches before they become threatened to attack.

To achieve and maintain compliance, the RSA enVision platform automates reporting requirements by creating mapped reports that allow organizations to capture and report on the logs from network, security, infrastructure and application-layer events. The reports provide a complete picture of network usage and audit trails for user identification, success and failure indication, origination of events and validation of user views of information. The RSA enVision platform also offers reporting templates that ease the process of reporting on updates to anti-virus systems, a very important feature to ensuring the security posture of telework devices.

To combat risks, organizations require real-time tracking and correlation of events in order to identify potential threats and respond quickly to change.



### Best Practice #6

*Understand the cyber threat landscape and the potential risk they pose by enabling telework. Gather and share intelligence among different government organizations. Identify vulnerabilities and implement security solutions to address them.*

Government organizations are increasingly becoming affected by threats such as phishing, malware and botnets. According to the Department of Homeland Security, there were almost 5,500 installations of malware and unauthorized access to government computers in 2008. These nefarious threats could severely impact government systems and put sensitive information at risk. And as teleworkers operate in an external environment that is less controlled, the chance of becoming targeted by these threats and spreading them over the network is even greater.

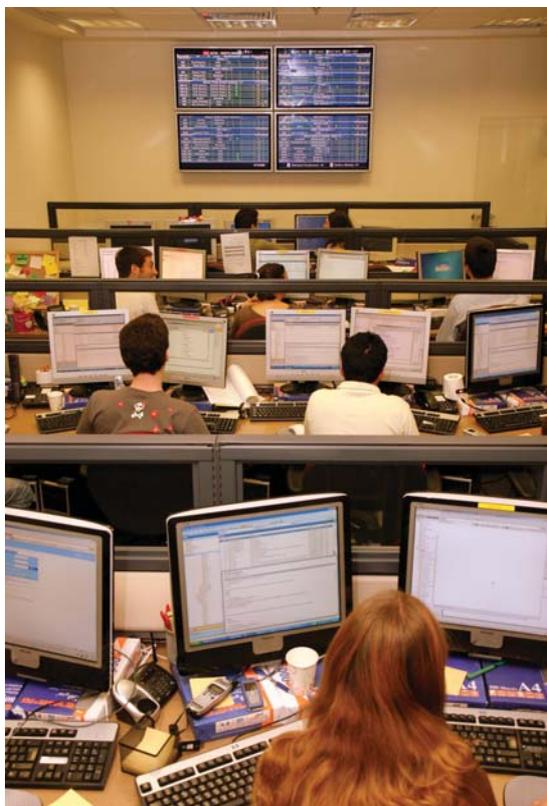
It is important for government organizations to proactively identify the threats that exist in order to mitigate the damage that is caused by an attack or even prevent it from occurring at all. By gathering and sharing intelligence across agencies and departments and developing a broad knowledge of potential threats, government organizations can better evaluate their vulnerabilities and implement security solutions to address them.

Another proactive measure government organizations should consider is to use a third party service that offers protection against threats such as Trojans and malware. By employing an anti-Trojan service,

organizations can prevent Trojans and malware from causing damage by detecting and stopping them at the source. An anti-Trojan service enables organizations to stay ahead of online criminals and provides insight into the malware that is targeting teleworkers and how it operates. By identifying the threat and taking action to curb it before a targeted attack is launched, government organizations can prevent unauthorized access to their systems.

The RSA® FraudAction<sup>SM</sup> service is an outsourced, managed service geared toward stopping and preventing phishing and Trojan attacks. RSA FraudAction is supported by RSA's Online Threats Managed Services organization, a team of experienced analysts dedicated to staying abreast of the latest threats and providing RSA customers with the most up-to-date information.

The RSA Anti-Fraud Command Center works 24x7 to monitor and shut down online attacks, deploy countermeasures and conduct forensic work.





At the core of the FraudAction service is RSA's exclusive Anti-Fraud Command Center (AFCC). Our experienced team of threat analysts, many who boast years of experience in military intelligence, work 24x7 to shut down online attacks, deploy countermeasures and conduct extensive forensic work to catch online criminals. The AFCC has established direct, open channels with dozens of ISPs around the world and provides multi-lingual translation support in nearly 200 languages to further enhance its ability to detect, block and shut down phishing and malware sites.

The AFCC is leading the way through results. Our fraud analysts have:

- Shut down over 150,000 online attacks
- Worked in over 140 countries
- Reduced the average lifespan of a phishing attack to a median of just 5 hours

The RSA enVision® platform offers government organizations the ability to conduct real-time monitoring of network activity in order to detect and prevent external threats from impacting teleworkers. Through a number of “out of the box” correlation rules, the RSA enVision platform is capable of identifying threats in real-time and giving security professionals insight into suspicious network activity. For example, the RSA enVision platform offers a unique correlation rule for detecting botnets on telework devices before they can impact the network and to prevent malware from gaining access to resources (see sidebar).

After extensive research into the nature and behavior of botnets and possible detection methods, several ways of identifying potential botnet activity through logs were created. While each method itself is not indicative of a botnet, when two or more of these activities are occurring together in parallel, there is a greater likelihood that a botnet exists on the network.

### Preventing Botnets from Targeting Government Teleworkers

Researchers recently discovered a botnet that had infected 1.9 million users across the globe, including many government and corporate computers. The botnet had infected devices from 51 U.S. government-owned domains. The malware associated with the botnet was capable of conducting several hostile actions including reading the user's email and injecting code.

To help prevent systems from being compromised, the RSA enVision platform offers a unique correlation rule to detect a botnet in action. After extensive research into the nature and behavior of botnets and possible detection methods, several ways of identifying potential botnet activity through logs were created. The RSA enVision rule studies network behaviors that are indicative of botnet activity including:

- An increase in detected AV activity with special emphasis on viruses that could be used to gain further system access
- Detected modifications to a host file where host lookup requests are rerouted to a different location
- Changes in DNS utilization
- Internet Relay Chat traffic from internal or external sources
- An increase in outbound SMTP traffic volume
- An increase in outbound SMTP traffic to known blacklisted servers



### Best Practice #7

*Education, training and awareness. Foster knowledge among employees and contractors that will enable them to reduce the risks of accidental misuse or disclosure of sensitive data when teleworking.*

Education and training among employees and contractors is critical to ensuring the security of any telework policy. Most data loss incidents are not the result of external threats or malicious intent; they are more likely to be caused by an employee inadvertently. According to a study conducted by the Ponemon Institute, insiders were the cause of 75 percent of all breaches in the U.S.

Making controls transparent to the user is important to demonstrating the key role they play in safeguarding data in performing their daily job functions. Implementing a DLP solution provides a good opportunity to raise awareness among employees and other users within the organization about the potential impact their behavior could have in causing and preventing data loss.

A DLP solution should have an effective process for alerting and remediation of incidents in order to avoid unnecessary disruption and potential data loss from occurring. A smooth and consistent workflow, which ensures that the right alert is delivered to the right person/people with all pertinent information, will reduce the time spent in routing and analyzing incident reports. Several issues could arise such as individuals receiving multiple alerts for the same incident, providing excessive or improper information that could inhibit administrators from quickly resolving the problem or failing to deliver an alert in a timely manner.

The RSA DLP Suite offers a simple and highly intuitive incident workflow with built-in notifications and alerts to inform data owners about affected files. The RSA DLP Suite correlates all related findings into a single alert along with all information that caused the alert to allow for quick remediation of incidents. Alerts and notifications can be customized based on a number of factors so that incidents are prioritized for review. To save time in incident handling, the RSA DLP Suite uses the Microsoft Active Directory hierarchy to directly notify data owners as individuals and/or groups.

According to a study conducted by the Ponemon Institute, insiders were the cause of 75 percent of all breaches in the U.S.



## RSA is your trusted partner

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

©2009 RSA Security Inc. All Rights Reserved.  
RSA, SecurID, enVision, FraudAction and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

GOVTEL SB 0609



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC