Fairfax County Internal Audit Office

Department of Information Technology
Remote Access Audit
Final Report

January 2010

"promoting efficient & effective local government"

Background

Remote access is a service provided by the county to the Fairfax county employees, contractors, and teleworkers for accessing the county's data and systems. The Board of Supervisors approved telework as a work option for eligible employees based on the benefits to the region in 1996 significantly increasing the volume of remote access users. Teleworkers work at home or another location such as a field site, library, or telework center. The county uses a variety of remote access technologies including Citrix servers, Virtual Private Network (VPN), and dial-up modems to meet the remote users' needs. Citrix is the main access method for county employees and most contractors; however, a number of contractors and DIT technical staff have access to the network via VPN as well. The Department of Information Technology (DIT) manages the county's technology, telecommunications, and security infrastructure, and provides technology support for remote access users including technical support through its help desk. The Fairfax County telework program included 3000 authorized remote access users and allowed 2000 concurrent users to securely access key authorized County systems and applications remotely via Citrix at the time of the audit. Remote access increases efficiency by enabling users to connect to the network from a remote site, however, there are risks associated with the access. Providing secure and resilient remote access to information systems decreases the risks of reduced worker productivity due to system unavailability. Also, unsecured or poorly secured remote access increases the risk of financial loss and other harmful business impacts through unauthorized disclosure, alteration, loss, misuse or destruction of sensitive information which may result from a failure in security.

Executive Summary

Our audit found that overall controls over remote access to the county network appeared to be adequate. The following areas had commendable controls:

- Remote access controls were enforced via two-factor authentication method using security tokens that provide one-time password authentication and valid user IDs.
- In general, remote access administration responsibilities and activities were adequately defined, and the access authorization process was performed in a timely manner.
- Distribution of secureID tokens were managed effectively. Additionally, there was proper segregation of duties between the individuals approving the request; the employee handing secureID configuration including connecting userIDs to remote access in RACF, ACE database, and Citrix Metaframe users group in Active Directory; and assigning secureID tokens and PIN numbers.
- Strong password usage was enforced to protect the data from unauthorized access.

However, there were areas where controls could be strengthened. The issues are listed below with additional information included in the detailed findings and recommendations section.

- There were control weaknesses in granting contractors least privilege access to the county's network specifically in the areas of removing contractor access in a timely

manner and sufficiently documenting contractor information and approvals on access requests.

- There were no written procedures with documented approval for granting Virtual Private Network (VPN) access to the users.
- There was no evidence that remote access activity logs, produced by RSA ACE/Software, were being reviewed on a regular basis for possible security violations.
- We found 12 generic userID's granted to the Police Department that did not have compensating controls for proper accountability. This increases the risk of improper access to county systems by unapproved individuals that cannot be identified.
- While access was terminated, secureID tokens were frequently not returned to DIT by terminated employees/contractors costing the county $52 a piece.

Scope and Objectives

This audit was performed as part of our fiscal year 2009 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered practices in place as of January 2009, and our audit objectives were to determine that:

- Adequate controls over remote access through Citrix and other county approved methods existed, and were effective to prevent unauthorized access to the county network.
- Adequate and effective controls over contractors and vendors remote access to the network were in place.
- User authentication, security administration, violation logging, data safeguard, and monitoring capabilities were in compliance with IT Security Policy PM 70-05.

Our testwork did not include Dial-Up modem user's access and VPN users testwork was limited. The VPN and Dial-Up modem user's lists were not provided; therefore, this was a scope limitation.

Methodology

Our audit approach included on-site visits to the Department of Information Technology, interviewing appropriate employees to understand remote access processes, and review of documentation provided including reports and audit logs, as well as related polices and procedures. We performed substantive sample testing of access control authorization and supporting documentation for employees and contractors to evaluate internal controls and compliance with departmental and county polices and procedures. We also performed sample testing of terminated employees'/contractors' access to the county network.

Findings, Recommendations, and Management Response

1. Contractors' Access to the County's Network

There were control weaknesses in granting contractors access to the county's network specifically in the areas of removing contractor access in a timely manner and sufficiently documenting contractor information and approvals on access requests. IAO noted the following:

a) While there was a section on the Remote Access Request form (September 2008 revision) for specifying the business days/hours that the user was authorized for remote access, there was no specific begin and end date for the access privileges granted to the contractors. ISO staff relied on agencies to subsequently notify DIT when their contractors no longer worked for them. ISO staff performed an annual audit to determine whether the users still worked for the department and needed the access. Also, supervisors of the users who had not logged in remotely for the past six months were contacted and the individuals' access were revoked if they no longer worked for the county or their jobs did not require access to the county network. However, their control did not fully address least privilege controls by potentially allowing contractors unauthorized access for a year.

b) The Remote Access Request form (online and/or paper copy) did not capture sufficient information about the user including the name of the company, type of access requested (Citrix or VPN), and business justification for VPN access.

c) Of the twenty contractors we reviewed, three had access to the county network through VPN. While there was a Remote Access Request form on file for these contractors, DIT was not able to provide any firewall documentation including the Firewall Ruleset Change Request form for either the individuals or their companies. Per the Firewall manager, VPN concentrators would be retired in the near future and Cisco ASA firewalls would be handling all VPN connections. At that time, any VPN account that was not documented would be deleted. Remote access through VPN poses additional risks to the county network security due to the fact that extensive access can be configured through the firewall; therefore appropriate access control measures should be adopted to minimize the potential risks. Additionally, users connected to the network by Citrix were automatically forced to use anti-virus software on their systems; however, DIT had not been able to automate the enforcement of anti-virus software on the VPN users' machines.

d) Of the twenty contractors randomly selected for review, twelve did not have a Contractor/Consultant Agreement form on file with ISO, and two forms did not have the appropriate signatures. These forms provide the county assurance that the contractor's company would be liable for any damages

caused by the contractors. Forms were to be maintained by the requesting departments. DIT provided the forms for their contractors during the audit.

Lack of proper access authorization procedures increases the risk of unauthorized user access to the system and its sensitive information resulting in misuse, disruption, modification, or destruction of the information. Additionally, computers connected to the network through VPN without anti-virus software could increase the risks of spreading unwanted software throughout the county's network interrupting operations and decreasing productivity.

Section 2.1 – Account Management/Access Control Policies of the county's IT Security Policy (revised PM 70-05.1, dated October 5, 2007) states that "The owner of information assets shall implement procedures and safeguards to ensure that access to Fairfax County Government information is made available only to those who have the right to such assess. The concept of "Least Privilege," i.e. providing only those privileges necessary to perform one's job function, will be used to insure the security of networks, computers, and Fairfax Government data."

Recommendation: We recommend DIT update the Remote Access Request form (online and/or paper copy) to include a section that requires agencies to specify a begin-and-end period for access privileges requested for contractors. Additionally, the form should capture information such as the name of the company, type of access, and business need for the access. Access expiration dates for each contractor should be entered into the system and access privileges should be revoked after the expiration date. The departments should also formally notify DIT if a user still needs access to the county network. We also recommend DIT continue educating the agencies of the risks of unauthorized user access to the county's data, and their responsibilities for notifying DIT in a timely manner for revoking access privileges when a user no longer has a need for such an access. DIT should send out written notices reminding departments of their requirement to maintain the original for the Contractor/Consultant Agreement form. A copy of the form should be sent to DIT to ensure that the contractor and his/her company representative have signed the liability clauses allowing the county to collect for any system damage caused by them. Another option would be for DIT to work with the Department of Purchasing and Supply Management (DPSM) to develop boiler plate language that addresses this issue for inclusion in all IT contracts, especially contractors with VPN access.

Management Response: The issue of notification by county agencies when their contractors are no longer working for the agency is of concern to DIT. While DIT is in the process of planned actions below, this condition may not be completely mitigated until a new procurement system in the ERP solution is implemented that will send action on contractors automatically to DIT ISO.

VPN access, unless otherwise approved, is for DIT staff and/or authorized DIT contractors supporting the county's network; or COTS vendors by contract directly responsible to support their products. A VPN user is the same as any county network user, and the same controls applied. The new firewall will address antivirus

updates for VPN users, and the risk is limited since DIT monitors system activity logs for all users regardless of access – remote or on-net.

DIT has updated the Remote Access Request form to include begin-and-end period for access privileges requested for contractor, name of the company, type of access, and justification. An automated notification of expiration process has been implemented.

DIT will meet with DPSM to review and update language about IT contractor responsibility for access to county systems already in the boiler plate contract language, and that the Contractor Agreement Form is attached. The anticipated completion date is March 2010.

DIT will send a memo to agencies regarding Contractor Use Agreements. The anticipated completion date is February 2010.

2. Virtual Private Network Controls

During the testwork of our randomly selected sample from the Users With Secure ID Token List, we found two VPN users that did not have documented justification on file for their access. Additionally, DIT was not able to produce a list of the VPN user population as of this audit. DIT did not have adequate written and approved procedures for granting Virtual Private Network (VPN) access to the users and there was an inconsistent application of their verbally communicated procedures such as requiring the completion of a Firewall Ruleset Change Request form. The Remote Access Request form on the ISO Web page stated that "VPN access requires separate approval from the DIT Information Security Office," but did not include a space for users to document the justification and ISO approval signature. We also reviewed the automated secure ID request work flow and noted that there were no specific processes for assigning VPN users.

Lack of documented justification and formal procedures that address users' access via VPN increases the risk of unauthorized access to the network. The inability to identify and periodically review the VPN population compounds the weak access controls by increasing the risk that inappropriate access would not be detected.

Section 2.1 and 4.1 of the county's IT Security Policy states that, "The owner of information assets shall implement procedures and safeguards to ensure that access to Fairfax County Government information is made available only to those who have the right to such access." And, users may not establish network tunnels to extend networks (home or otherwise) without an established business need and shall use DIT approved access methods (e.g. county provided VPN software or hardware.)

Recommendation: We recommend DIT document their policies and procedures for granting VPN access to the users, particularly to contractors. These policies and procedures should include controls to mitigate the risks of unauthorized access to the county's network, and staff should be properly trained in these policies. We also

recommend DIT include a data field in their ACE database to be able to track VPN users. A list of the VPN users should be produced on a regular basis and reviewed to confirm access privileges. The department should maintain formal documentation of business justifications and approvals and have them readily available for review. These policies should be incorporated into the new automated secure ID request work flow.

Management Response: Current VPN users have been added to the current remote access documentation. In addition, DIT forms and procedures have been updated to include VPN.

3. Review of Activity Logs

There was no documented evidence that remote access activity logs produced by the RSA ACE/Server, Version 5/1 were being reviewed on a regular basis for possible security violations. Lack of documentation of the review of activity logs decreases accountability for their timely review increasing the risk of security violations that could result in financial loss, staff productivity loss, compromised data and other serious effects. Section 3.6 – Security Monitoring of the county's IT Security Policy (revised PM 70-05.1, dated October 5, 2007) requires that user account logs and system event logs be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk. Additionally, PM 70-05.1, section 2.14 of the IT Security Policy states that, "Remote access control will be enforced via network and system level auditing. This information will be readily available for monitoring and review by appropriate personnel."

Recommendation: Activity log reviews by system administrators to detect potential security incidents and security breaches should be documented with reviewer's initials and date. The documentation should be retained for a period specified by the system owner and there should be evidence of staff review. Additionally, in the next upgrade, DIT should consider the possibility of implementing automated processes to monitor and document remote access-related security events and send alert e-mail messages to system administrators for possible attempts to compromise security.

Management Response: DIT has implemented a dual review process. The platform system administrator currently reviews logs for anomalies that may be a system error or malicious activity. Such incidents are reported to ISO. If an account is attempted for log on after three tries, the system locks the user out and reset is required by ISO.

The review of the activity logs to date is being completed. DIT is implementing a process to utilize Infra to document the review. ISO will conduct independent reviews of anomalies based on user activity. The anticipated completion date is March 2010.

4. SecureID Tokens Controls

It was noted by ISO staff that county departments were often not obtaining the secureID tokens from their terminated employees and/or contractors making it difficult for DIT to be able to retrieve the tokens. We found at least six instances where the ISO staff had to contact the department due to their failure to return the tokens. ISO receives a Termination Notice e-mail when an employee leaves the county. If the SecureID token has not been returned to ISO by the individual, a notification e-mail regarding the token is sent to the department. However, ISO relied on agencies that hire the contractors to notify DIT when the individuals no longer worked for them.
A secureID token that has been assigned to an individual who no longer needs use of the token can be re-assigned. Failure to return a token to DIT costs the county about $52 per token. Personnel/Payroll Administration Policies and Procedures, Memorandum No. 33, dated September 28, 2006, Employee Clearance Record procedures requires employees to return the remote access secureID tokens to DIT/ISO upon termination.

Recommendation: We recommend that DIT work with the Department of Human Resources/Payroll Division to develop procedures to enforce returning the secureID tokens to DIT upon termination of an employee. An option would be for DIT to be able to charge departments that fail to return their employees' tokens the replacement cost. For contractors, they could require the use of temporary/on-demand tokens instead of issuing the physical piece of equipment.

Management Response: County agencies are responsible for collecting county property from their terminated employees and/or contractors.

DIT is in the process of migrating vendors to virtual tokens and updating the remote access procedure to include virtual tokens which are half the cost. The newly purchased virtual tokens are not physical devices; upon revocation of access, a virtual token is re-assigned. The anticipated completion date is March 2010.

ISO will periodically check current physical token use to ensure tokens are being actively used and will initiate a process to notify, delete accounts, and recover the tokens. The anticipated completion date is March 2010.