SPECIAL REVIEW

STATUS OF DATA SECURITY MEASURES

DEPARTMENT OF FORENSIC SCIENCE

REPORT ON AUDIT

AS OF

JULY 31, 2006

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

August 3, 2006

The Honorable Timothy M. Kaine
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

As part of another review, we reviewed the data security measures, policies and procedures of the **Department of Forensic Science** as of July 31, 2006. During our review we found matters that warrant Forensic Science management's immediate attention and timely resolution. This document describes our concerns and recommends actions to resolve the matter.

Introduction

We are conducting a statewide review of data security measures, policies and procedures. In connection with the review, our staff is administering an information security review questionnaire and conducting on-site evaluations of agency data security measures, policies and procedures.

Our security review questionnaire has four information security subject areas, with questions that constitute industry best practices. Our questionnaire combines the Commonwealth's security standard SEC501 with industry best practices, such as Cobit, Fiscam, and ISO 17799. The following is the content matter of each subject area.

1. **Security Management Structure** evaluates whether an agency has incorporated information security into their business objective and management structure.

2. **Data Protection, Integrity, Availability, and Confidentiality** evaluates whether the agency has controls documented that protect the agency's data from, for example, unauthorized alteration, disclosure of sensitive data and data corruption.

3. **Configuration and Change Management** evaluates whether the agency has controls documented that provide the agency with a structured approach to configuring and changing its information technology environment.

4. **Monitoring and Logging** evaluates whether the agency has controls documented that provide a configuration or process change in response to monitoring its systems or examining its systems' logs.

Although, we plan to issue the report on the Commonwealth’s information security measures on December 1, 2006, our review of the Department of Forensic Science found matters requiring immediate attention. Presented below are our findings.

Background

The Department of Forensic Science (Forensic Science) is a nationally accredited forensic laboratory system serving all state and local law enforcement agencies, medical examiners, and Commonwealth's Attorneys. Forensic Science examiners provide technical assistance and training, evaluate and analyze evidence, interpret results, and provide expert testimony related to the full spectrum of physical evidence recovered from crime scenes. Much of the information and data in the possession of Forensic Science is highly sensitive and subject to view during legal proceedings.

A comprehensive information security program provides the essential framework necessary to protect the data on information systems and the data handled by employees. Without a security program, management cannot determine the current or potential risks to their data.

Therefore, management cannot adequately prevent or minimize those risks. Given the sensitivity of some of the information maintained by many agencies, information security is critical to ensuring the confidentiality, integrity, and availability of the data.

Finding

Forensic Science does not have a complete or current information security program. Forensic Science should have a security program that includes policies and procedures that management and staff can apply to provide reasonable assurance that appropriate levels of confidentiality, integrity and availability covering data in their possession. Industry best practices, as well as state technology standards, provide that a well developed security program should include documented policies and procedures covering the following areas.

- Security Management Structure
- Information Security Responsibilities and Separation of Duties
- Information Security Officer Role
- Security Awareness Training
- Resource and Data Classifications
- Information Asset Inventory
- Risk Assessment
- Business Impact Analysis
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Procedure
- Authorization and Authentication Controls
- Change and Configuration Management
- Monitoring and Logging

As previously discussed, a comprehensive information security program provides the essential framework to protect the data on information systems and the data handled by employees. The lack of a comprehensive information security program prevents Forensic Science's management from assessing the current or potential risks to their data, and enabling them to adequately prevent or minimize those risks. Given the sensitivity of some of the information maintained by Forensic Science, a properly implemented information security program is critical to ensuring adequate protection of their data.

Forensic Science's management realized the importance of having a security program and asked Virginia Information Technology Agency (VITA) staff to perform an information security assessment. VITA completed the review in February 2006, which assessed Forensic Science's state of security as benchmarked against industry-best practices.

Forensic Science used the review to issue a request for proposal to have a consultant develop a comprehensive information security program. Forensic Science is currently reviewing proposals from outside vendors to help complete and implement the agency's information security policy.

Forensic Science, while commended for starting to take action, should re-evaluate the risk and exposure of not having a documented information security program in place. Further, the program policies and procedures is only the initial phase of the process. Staff training and awareness, as well as monitoring and logging, are the key implementation phases of the process.

Considering the highly sensitive nature of the systems and data in Forensic Science's possession, management should determine if it has made sufficient allocations of time and resources necessary to complete a comprehensive information security program that will meet industry best practices, as well as incorporate the VITA recommendations promptly. We believe the nature of Forensic Science's operations require the review of this matter prior to the release of our final report.

We discussed this letter with management at an exit conference held on August 7, 2006 and have attached their response to this matter.

AUDITOR OF PUBLIC ACCOUNTS

WJK:sks
sks:29

COMMONWEALTH of VIRGINIA

DEPARTMENT OF FORENSIC SCIENCE

August 15, 2006

OFFICE OF THE DIRECTOR
A Nationally Accredited Laboratory

700 NORTH 5TH STREET
RICHMOND, VIRGINIA 23219
(804) 786-2281 FAX (804) 786-6857

Walter J. Kucharski
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218-1295

RE: Special Review of Data Security Measurers

Dear Mr. Kucharski:

The Special Review of the Status of Data Security Measurers of the Department of Forensic Science (DFS) dated July 31, 2006 has been reviewed. DFS management understands from the information provided in the report and the conference held on August 7th with the Auditor of Public Accounts that the lack of a fully documented IT security policy, including a Business Impact Analysis and Risk Assessment may expose the agency to potential security risks that may not have been discovered through past or current practices which DFS has deployed to ensure the security of agency computer systems and data. While there is no evidence of any security breech to any of the DFS computer systems, agency management acknowledges the importance of a thoroughly documented and implemented security program given the nature of the data maintained by the Department.

Prior to July 1, 2005 DFS was part of the Department of Criminal Justice Services and fell under that agency's policies for IT security. Under a Memorandum of Understanding with DCJS, administrative support for DFS was continued through FY2006. DFS has recently been provided information from DCJS regarding their Continuity of Operations Plan, Information Technology Security Plan (Business Impact Analysis, Risk Assessment, Safeguards and Contingency Plan) and Access Procedures and this information has been forwarded to your office. Specific security practices relating to DFS information technology systems are documented in the DFS Administrative Operating Procedure 9. Specific security practices relating to DFS facilities security are documented in DFS Quality Manual section 16. DFS acknowledges this documentation needs to be revised and updated with a more comprehensive information technology security policy.

DFS management realized the importance of protecting its computer systems through a comprehensive security program and requested information security staff at VITA to conduct an information security review, to prepare for assuming responsibility for the IT administrative functions July 1, 2006. The VITA security review report was issued in February 2006. This review provided recommendations for improving IT security and also acknowledged that DFS had many good IT security practices in place. Current IT security practices include the following:

- Industry standard firewalls with updated Operating Systems are maintained and installed at all points of entry from the outside (internet, all CJIS access points).
- All users are authenticated with a user ID and password. The authentication confirms the identity of any user trying to log on to a computer to access network resources.
- All main systems and selected user directories are backed up nightly and backups are taken off site weekly.
- All critical system data is stored on a Storage Area Network (SAN) with redundant and hot spare drives. All drives are actively monitored by DFS IT personnel and the SAN manufacturer via an automated "call home" function. The SAN provides high availability of critical system data.
- DFS maintains an automated, centralized anti-virus application/system to update and maintain current virus definition files on each workstation, laptop and server attached to the DFS network. The virus definition files are automatically updated and pushed out to the clients on a daily basis or as needed in an emergency situation.
- Additional anti-virus safe guards are in place on the DFS e-mail server which scans every incoming and outgoing e-mail message for viruses and notifies the system administrator of any viruses found. This application uses 4 different providers of virus definition files updated daily or as needed in an emergency situation.
- Operating System and application patch management is provide via an automated and centrally maintained system to ensure all approved service packs are distributed and applied automatically and in a timely manner.
- DFS has removed administrative computer account privileges for individual users and reserved this designation for IT staff only. This reduces the risk of viruses and Trojan horses from being installed or replicated, and prevents unauthorized software from being installed on agency computers.
- Access to DFS facilities is controlled with a security system which only allows access to authorized users. All employees must wear an ID badge which identifies them as a DFS employee. Any visitors to the buildings must wear a visitor badge and they must be escorted while in the building.

In response to concerns raised in the APA Special Review, DFS has asked VITA to review DFS current security measures to ensure no immediate changes need to be implemented before the Business Impact Analysis and Risk Assessment is completed. An initial meeting with VITA is scheduled for August 16, 2006.

In order to develop a Continuity of Operations Plan and a comprehensive IT security program to comply with the recently revised VITA standards, DFS plans to contract with an outside consultant to complete this effort for the agency. DFS has begun negotiations with a vendor to come to an agreement on the objectives, schedule, scope, and price of the work to be completed. Current estimates from this vendor indicate this project will take approximately 34 weeks to complete, not including implementation. Based on current progress made in negotiating the scope of work and work plan, DFS anticipates having a signed contract and beginning work in August 2006. The vendor is proposing to complete the work in three phases which will last 10 weeks, 10 weeks, and 14 weeks respectively. DFS will forward the completed product of each phase to the APA as each phase is completed.

DFS is evaluating the need for additional IT security personnel resources to support this effort and to plan for additional workloads that will need to be addressed on a permanent basis with the implementation of this enhanced security program and the expanded use of Information Technology in the agency. In light of this response, we request to meet with you again before your report is issued.

If we can provide any additional information at this time, please contact Ron Layne at (804) 786-2281.

Sincerely,

Paul B Ferrara

Paul B. Ferrara, Ph.D.
Director

wwa

c: The Honorable John W. Marshall
Secretary of Public Safety

APA Response

Based on our review of the Department's response and additional documentation they sent to us on August 11, 2006, we do not think an additional meeting is necessary.