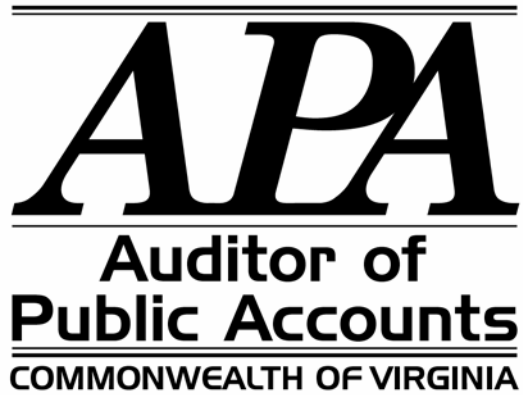
DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

RICHMOND, VIRGINIA

NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TEST REPORT

SPECIAL REPORT

MARCH 2004



AUDIT SUMMARY

Our network vulnerability assessment and penetration test of Department of Medical Assistance Services (DMAS) as of January 22, 2004 found:

- based on our assessment of the risks the systems face and the tests of the operating effectiveness of the controls developed by DMAS to alleviate those risks, overall information security controls in place at the time of the testing appear sufficient to protect critical and sensitive information; and

- certain areas where improvements can be made to enhance systems security. We have provided management of DMAS the details of our findings and recommendations in a separate report that is exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. This provision allows for the exemption from disclosure, information that describes the design, function, operation, or access control features of any security system.

Commonwealth of Virginia

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

Walter J. Kucharski, Auditor

March 8, 2004

The Honorable Mark R. Warner
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Lacey E. Putney
Vice Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

The **Department of Medical Assistance Services** (DMAS) requested the Auditor of Public Accounts (Auditor) to perform a vulnerability assessment and network penetration test. DMAS requested that the Auditor use its technical staff experienced in security control work and operations to perform an independent assessment of the risks the systems face (vulnerability assessment), and a test of the operating effectiveness of the controls (penetration test). We conducted the review as of January 22, 2004 and examined whether information systems management and administration had reasonably assessed risk, and that the controls placed into operation were effective in mitigating the assessed risks.

DMAS requires this type of test every other year to satisfy due diligence requirements for the federal Health Insurance Portability and Accountability Act (HIPAA) and internal policies. DMAS has created an information security controls environment that attempts to protect the areas where information systems management perceive risk, and has tailored the controls accordingly.

The Auditors used a variety of scanning software and techniques during the vulnerability and penetration test. Outside of the scope of this engagement were "social engineering" attacks. Social engineering attacks include posing as technical support staff to elicit responses from users designed to aid in network penetration, or searching desks to reveal notes with passwords and user IDs. This type of test typically identifies significant security weaknesses. However, we did not perform this type of test work because of the effect that these tests can have on employee confidentiality, property rights, and the relationship between users and information systems staff.

This project was limited to the DMAS network. This test work did not include any information housed for DMAS at the Virginia Information Technology Agency (VITA), or any of the information housed at First Health, DMAS' service provider for processing Medicare claims. This engagement did not have a goal of identifying all of the potential weakness that the systems could have been subject to.

Based on our assessment of the risks the systems face and the tests of the operating effectiveness of the controls developed by DMAS to alleviate those risks, overall information security controls in place at the time of the testing appear sufficient to protect critical and sensitive information. However, we noted certain areas where improvements can be made to enhance systems security. We have provided management of

DMAS the details of our findings and recommendations in a separate report that is exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. This provision allows for the exemption from disclosure information that describes the design, function, operation, or access control features of any security system.

We have not included management's response in this report because the information included in their response is also exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. However, management generally concurred with our recommendations and agreed to take appropriate corrective action.

EXIT CONFERENCE

We discussed this report with management at an exit conference held on March 8, 2004

AUDITOR OF PUBLIC ACCOUNTS

WJK:cam
cam:25