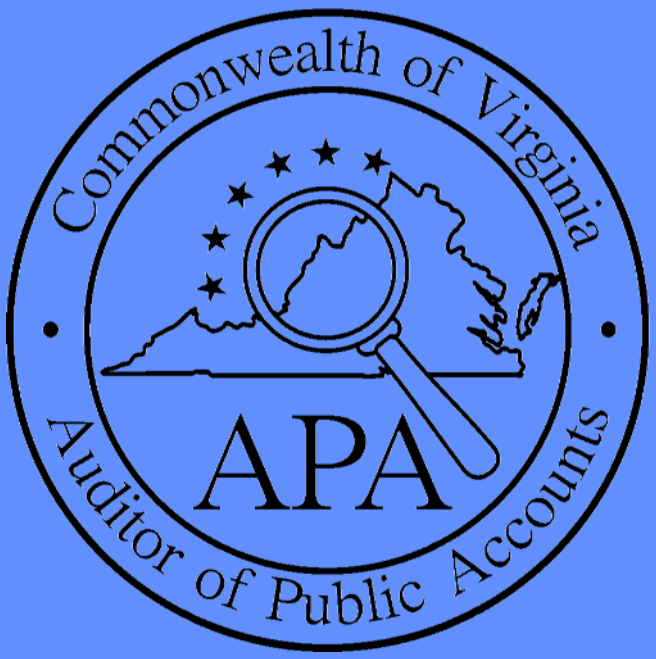

DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

VULNERABLILITY ASSESSMENT AND NETWORK PENETRATION TEST

AS OF

OCTOBER 2013

www.apa.virginia.gov | (804) 225-3350 | reports@apa.virginia.gov

Audit Summary

Our vulnerability assessment and network penetration test of the Department of Medical Assistance Services (DMAS) as of October 30th, 2013 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 mitigate those risks, overall information security controls in place at the time of the testing appear sufficient to protect critical and sensitive information from external and internal threats; and

- Certain areas where DMAS can make improvements to information security controls that protect critical and sensitive information from external and internal threats.

Recommendations regarding these improvements are part of a separate report that is exempted from public disclosure in accordance with Section 2.2-3705.2.3 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

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2013

The Honorable Robert F. McDonnell
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable John M. O'Bannon III
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

The **Department of Medical Assistance Services** (DMAS) requested that the Auditor of Public Accounts (Auditor) 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 October 15, 2013, 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 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 perceives risk and has tailored the controls accordingly.

The auditors used a variety of scanning software and techniques during the vulnerability assessment and penetration test. Not only did the review investigate the state of the network and systems, it also included the content of published data. The review of the published data checks for sensitive data and documents available to the public on the DMAS website.

Outside of the scope of this engagement were "social engineering" and "phishing" 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 and information housed for DMAS at the Commonwealth Enterprise Solutions Center (CESC). This engagement did not have a goal of identifying all of the potential weakness to which the systems could have been subject.

Based on our assessment of the risks the systems face and the tests of the operating effectiveness of the controls developed by DMAS to mitigate 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 DMAS can make improvements to enhance systems security. We have provided the management of DMAS the details of our recommendations in a separate report that is exempted from public disclosure in accordance with Section 2.2-3705.2.3 of the Code of Virginia. This provision allows for the exemption from disclosure of information that describes the design, function, operation, or access control features of any security system.

We discussed this report with management at an exit conference held on December 3, 2013. Management's response is included at the end of this report.

AUDITOR OF PUBLIC ACCOUNTS

GGG/clj

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CYNTHIA B. JONES
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
800/343-0634 (TDD)
www.dmas.virginia.gov

December 4, 2013

Ms. Martha S. Mavredes
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed your Special Review Report, *Information System Vulnerability Assessment and Penetration Test*, dated October 2013. We are in general concurrence with your recommendations and agree to take prompt action to fully address them. We would like to thank Goran Gustavsson and Matt Robinett for providing DMAS with a thorough review and report.

If you have any questions, please do not hesitate to contact our Director of Internal Audit, Paul Kirtz.

Sincerely,

Cynthia B. Jones

Cynthia B. Jones

DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

Cynthia B. Jones
Director