MLDS Center
Maryland Longitudinal Data System

Address 550 West Baltimore Street
Baltimore, MD 21201
Phone 410-706-2085
Email mlds.center@maryland.gov
Website www.MLDSCenter.org

Memorandum

TO: Members of the MLDS Governing Board

FROM: Tejal Cherry, Chief Information Officer
Ross Goldstein, Executive Director

DATE: August 31, 2018

SUBJECT: System and Security Updates

The purpose of this memorandum is to update the Governing Board on the completion of one year of the intrusion detection system, the annual review of the Data Security and Safeguarding Plan, and plans for an Independent Security Audit.

Intrusion Detection System (IDS)

Background

The Center entered into an agreement with Cyber Engineering Service, Inc. (Cyber) in August of last year. The process to fully plan and implement the IDS took until October 20, 2017, at which point the Center began receiving *Weekly Network Security Monitoring Reports*. Initial reports captured close to two million alerts, causing Center staff and Cyber staff to work to fine tune the reporting protocol to identify and eliminate "good" traffic. After the fine tuning, the number of alerts were reduced significantly, but upon further testing it was determined that Cyber wasn't detecting certain types of activity. In response, Cyber conducted a review of the Center's system architecture and firewall rules. This review resulted in a modification to Cyber's protocols for analyzing traffic to and from the system. It also produced several recommendations for improvements to the Center's network and firewall management, which staff implemented.

Review

The services provided by Cyber were inconsistent. For example, each weekly report contains a summary of the total number of alerts, broken out by those that were of high severity, medium severity, and low severity. The number of alerts varied greatly week to week and the classification of those alerts would changed. Center staff continued to work with Cyber to resolve these inconsistencies. Cyber was responsive to input and would make corrections as needed, but it remained a difficult process to work with and obtain actionable information.

Despite some of these issues the IDS added value to the Center. As discussed above, Cyber's review of the network architecture resulted in important fine tuning of the network and firewall rules. Also, staff learned a great deal about system monitoring and developed ways to use existing tools to create comparable monitoring. They also developed methods for analyzing the monitoring reports so that they can better assess and respond to potential issues.

Next Steps

While the IDS has been a worthwhile endeavor and learning experience, due to its cost and the ability to replicate much of the monitoring internally, we do not plan to continue this service.

Data Security and Safeguarding Plan

Section 1.2 of the Data Security and Safeguarding Plan (DSSP) requires that it be periodically reviewed and revised as necessary. During the past few months, Center staff have been reviewing the DSSP, with a specific focus on ensuring that it aligns to the Department of Information Technology (DoIT) security requirements. Staff has completed the review and identified the following topics that are not included in the DSSP:

1. Virtualization Technologies
2. Cloud Computing Technologies
3. Mobile Devices
4. Electronic Communications Policy
5. Social Media Policy

Of the topics, only Virtualization Technologies apply to the Center's data system. Staff will develop procedures addressing Virtualization Technologies and present it as a proposed revision to the DSSP for Governing Board review and approval at the December meeting.

Independent Security Audit - U.S. Department of Homeland Security

The National Cybersecurity and Communications Integration Center (NCCIC) under the Department of Homeland Security is charged with reducing the risk of systemic cybersecurity and communications challenges in its role as "the Nation's flagship cyber defense, incident response, and operational integration center." NCCIC, through its U.S. Computer Emergency Readiness Team (U.S. CERT), offers *National Cybersecurity Assessments and Technical Services (NCATS)*. All of the services are available at no cost to state and local government. The services include:

1. Cyber Hygiene: Vulnerability Scanning
2. Phishing Campaign Assessment (PCA)
3. Risk and Vulnerability Assessment (RVA)
4. Validated Architecture & Design Review (VADR)

Center staff have been making arrangements to take advantage of these free services to fulfill the annual audit requirement. Staff has been reviewing and completing a series of forms that needed to be signed and approved by the Center. The documents include:

1. Risk and Vulnerability Assessment Rules of Engagement
2. Authorization to Conduct Continuous Scans of Public-Facing Networks and Systems
3. Express and Certification Statement
4. Operational Assurance Assessment and Logistics Request Form
5. Service Request

Center staff is in the final process of submitting all paperwork so U.S. CERT can begin the audit services within next two to three months.