

Consulting Report

1908 myLASERS Security Review

March 9, 2022

Cindy Rougeou, LASERS Executive Director
The LASERS Audit Committee

BACKGROUND

This was a planned engagement on the fiscal year end (FYE) 2019 Audit Plan. The fieldwork for this engagement was completed on March 3, 2022.

Following the implementation of Optimus, LASERS customized Enterprise Content Management (ECM) system, the IT Division continued to plan for and implement initiatives related to disaster recovery and a redesign and rebranding of Member Self-Service, which is now known as myLASERS. MyLASERS was designed with new features and enhanced security. During the implementation, eForms were also introduced to myLASERS, allowing users to complete a selection of forms and electronically submit them to LASERS.

To better secure user access to myLASERS accounts, the following key examples of security updates were planned and implemented:

- A third-party vendor, Okta, was chosen as an Identity and Access Management (IAM) solution to improve the authentication process when members logon to myLASERS. IAM is the security and business discipline that enables the right individuals to access the right resources at the right times and for the right reasons. The integration of Okta and myLASERS added the following security enhancement examples:
 - Email validation to confirm that an email address is deliverable and valid.
 - Improved minimum password requirements to require a more complex and strong user account password (i.e., minimum length, alphanumeric, symbols).
 - Multi-factor authentication (MFA) method required to be setup and used at each login. MFA is an extra layer of security that requires not only a password and username (that which you know) but also something that only the user has on them (i.e., a onetime code the member has access to through something they have physically, such as a phone). Currently, myLASERS accomplishes

BOARD OF TRUSTEES:

Judge William Kleinpeter, *Chair*
Shannon Templet, *Vice Chair*
Thomas Bickham
Virginia Burton
Charles F. Castille

Comm'r Jay Dardenne
Byron P. Decoteau, Jr.
Rep. Phillip DeVillier
Ternisa Hutchinson
Amy A. Mathews

Barbara McManus
Sen. Barrow Peacock, *Designee*
Sen. Edward Price
Hon. John Schroder

Cindy Rougeou, *Executive Director*

LASERS Benefits Louisiana.

this by allowing the user to receive a one-time verification code via a SMS text message or voice call.

- Notifications are sent to the user notifying them of security related changes (i.e., when a sign-in occurs from a new device, password is changed).
- The member registration process was improved through validation of the member from SOLARIS information. After entering personal demographic information that matches an individual stored in SOLARIS, the user will begin the myLASERS PIN process. During the PIN process, they will be prompted with contact information stored in SOLARIS where a pin validation code will be sent to assist with further validating the identity of the user. The user can choose from SMS text message, voice call, email, or physical mail to receive the PIN code. Once the validation code is entered and confirmed, the user account is created.
- To provide additional protection, when certain areas containing critical/sensitive information are accessed after login, such as an eForm, the user is required to perform MFA again by entering a verification code sent via SMS text message or voice call to their registered device.

Implementation of myLASERS took place in a series of releases from December 2020 through July 2021. Requirements and tests were developed for each area of functionality planned for myLASERS. Before all releases went live, testing was performed by the myLASERS project team to help ensure that the applicable security requirements were met.

In conjunction with the release of myLASERS, LASERS developed WorkSpace. WorkSpace is a solution that contains information relating to a person stored in SOLARIS. When accessing WorkSpace, a customer service representative is able to search for individuals by their person details to determine if a myLASERS account has been created. If the user has not completed the necessary steps to connect the account to their person details (i.e., successfully completing the myLASERS registration process), the customer service representative can search for the member account and resolve the reported issues (Features Supported: registration, password reset, lock or unlock accounts, suspend or unsuspend accounts, block users from completing registration, and delete accounts).

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this engagement included a review of the primary and supportive security related components of myLASERS.

The primary objectives of this engagement were to determine if:

- The requirements established for security of myLASERS appropriately represented established business rules.
- Testing plans were effective in confirming the expected security of myLASERS.
- The myLASERS logging and monitoring processes were adequate and defined.
- The eForms implemented were secure and properly configured.
- The complementary Member Services and Fiscal processes aligned with the security enhancements to myLASERS.
- The requirements established for WorkSpace appropriately represented established business rules.
- Testing plans were effective in confirming the expected functionality of WorkSpace.

Procedures used to complete this engagement included:

- Reviewing vendor security documentation to confirm security standards.
- Reviewing the relevant requirements and testing plans as established by IT, Member Services, and Fiscal.
- Reviewing the process and procedures for customer services and member demographic updates.

- Independently performing testing of myLASERS and WorkSpace and verifying all security controls were implemented.
- Conducting other inquiries considered necessary to achieve engagement objectives.

This engagement was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the policies and procedures of the Audit Services Division.

EXECUTIVE SUMMARY

Audit Services participated in a consulting role in the implementation of myLASERS and the security enhancements made to protect user accounts and information. Audit Services performed the following key activities:

- Confirmed that the third party vendors utilized for myLASERS security (i.e., Okta) and eForms (i.e., Adobe Sign) met LASERS defined security requirements.
- Reviewed requirements and testing plans for myLASERS security and WorkSpace.
- Confirmed through independent testing that all myLASERS security and WorkSpace requirements were met.
- Analyzed the myLASERS logs and related processes.
- Reviewed the relevant components of operational processes that complement myLASERS security (i.e., customer service processes and member demographics processes).
- Verified that eForms are secure and PII is protected.

After completion of these activities, Audit Services confirmed that the implementation of myLASERS and WorkSpace was successful and that the complementary processes were aligned. One observation was identified which relates to the technical logging and monitoring of myLASERS activity. It is of note that logging was not a primary focus of this project; however, certain log components were introduced throughout the implementation.

OBSERVATION, RECOMMENDATIONS, AND RESPONSES

1. LOGGING REQUIREMENTS SHOULD BE FORMALLY DEFINED AND CORRESPONDING MONITORING IMPLEMENTED

OBSERVATION

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 92, logs are composed of entries that contain information related to a specific event that has occurred within a system or network. Some common types of information that can be logged include user authentication attempts, account creation steps, usage information, and actions completed by users. Logs are useful for resource management, application troubleshooting, and system monitoring. If properly monitored, detailed logs can alert an organization about malicious or fraudulent activity and help reduce the risk of fraud and prevent account compromise. Without sound processes for monitoring and analyzing logs, the value of the logs is significantly reduced.

As part of the myLASERS implementation, two components of myLASERS logs were created. Those related to the LASERS portion of myLASERS activity (i.e., registration steps, notifications, and application errors) and Okta activity (i.e., account creation and login). Prior to the myLASERS implementation, Member Self-Service had very basic and minimal logging that was limited by the technologies used to develop the application.

Therefore, for the LASERS portion of the myLASERS activity, LASERS established more extensive logging (i.e., logging to a folder/file, Windows Application log, and database) which is configurable and callable from anywhere. At this time, most of these logs are used by IT for application support, maintenance, and security needs. According to LASERS IT, all items at the time of the myLASERS implementation that seemed reasonable to be logged is currently being logged. Furthermore, staff confirmed that, during the project, there were no formal technical requirements established on which myLASERS activity can and should be logged. The process of establishing specific requirements would ensure that all technical activity is properly logged and available for monitoring. As for the logging of Okta activity, all activity is being logged.

In the instance that LASERS is notified of exceptions from Okta, the business, or other related activities, logs are reviewed accordingly. Regarding the monitoring of myLASERS technical logs, the LASERS portion is not formally being monitored on a real-time basis. Okta logs were previously being monitored on a real-time basis by IT staff utilizing Q-Radar, a Security Event Incident Management (SEIM) solution, which assists with helping to detect anomalies and security threats using logs. According to IT, the interface between Okta and Q-Radar was not working properly and was turned off. Also, LASERS has made attempts to reconfigure the interface but have not been successful. Furthermore, IT has recently learned that these vendors have stopped supporting the interface between the two products. Separate from the monitoring of Okta activity by LASERS SEIM solution, LASERS IT staff members review notifications generated from Okta that provide details of exceptions detected by Okta.

RECOMMENDATION #1

IT should evaluate the current environment to establish the requirements for the technical (non-operational) aspects of LASERS portion of myLASERS activity logging. This should include establishing what can be logged, how this can best be accomplished, and the retention of the logs. Upon completion, any identified gaps or weaknesses compared to current practice should be resolved.

DIVISION RESPONSE

IT agrees with this recommendation. IT will evaluate the technical aspects of logging in myLASERS based on the recommendation and resolve any gaps or weaknesses identified. Due to several ongoing security projects that currently have a higher risk or impact (i.e., Active Directory Remediation, Firewall Replacement, and Employer Self-Service project), this has been assigned a low priority with a re-evaluation date of July 1, 2023.

RECOMMENDATION #2

IT should implement a process to monitor the LASERS and Okta myLASERS activity logs on a real-time basis using LASERS SEIM solution. Furthermore, formal guidelines and procedures should be developed for the handling of exceptions generated by both the LASERS and Okta log monitoring processes.

DIVISION RESPONSE

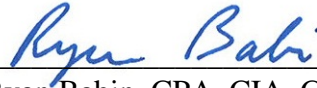
IT agrees with this recommendation. IT is manually reviewing Okta logs as needed and will evaluate the ability to automate this process in real-time using LASERS SEIM solution. IT will develop formal guidelines and procedures for log management. Due to several ongoing security projects that currently have a higher risk or impact (i.e., Active Directory Remediation, Firewall Replacement, and Employer Self-Service project), this has been assigned a low priority with a re-evaluation date of July 1, 2023.

FOLLOW-UP

A follow-up to this engagement will not be scheduled at this time. Audit Services will maintain this information on a tracking report. These items will be tracked until they are closed.



Reece Babin, CISA
Auditor



Ryan Babin, CPA, CIA, CISA
Audit Services Director

Cc: Trey Boudreaux
 Travis McIlwain
 Johnathon Sprouse
 Tricia Gibbons
 Artie Fillastre
 Eric Schoonmaker
 Wretha Drinnon
 Johnathan Drago