Assurance Report

1604 IT Security Management Review

April 5, 2016

Cindy Rougeou, Executive Director
The LASERS Audit Committee

EXECUTIVE SUMMARY

The following observations were noted during this review and are detailed below:

1. Not all computers and servers have LASERS approved antivirus software installed.
2. LASERS website filtering application and approval process should be reviewed.
3. Data logs are not effectively evaluated.
4. A comprehensive IT security assessment plan should be established.
5. An IT security incident response plan should be formally implemented.
6. Local administrator privileges were not removed timely.
7. IT security awareness training program should be formally implemented.
8. Not all computers have endpoint security software installed.
9. Not all network switches were updated according to procedure.
10. Procedure related to virtual private network (VPN) access not consistently followed.
11. VPN security validation software should be reviewed.
12. External user access to LASERS network could be managed more effectively.
13. Mobile device passcode not required for all devices utilizing the AirWatch application to access LASERS email system.
14. IT security oversight should be evaluated to increase effectiveness.
15. An overall IT governance and management framework does not exist.

BACKGROUND

This was a planned engagement on the fiscal year end 2016 Audit Plan. The fieldwork for this engagement was completed on March 31, 2016.

The effective management of IT security risks, threats, and vulnerabilities is an important role in the protection of LASERS systems and information. The rapid evolution of technology creates an ever changing landscape of security risks, threats, and vulnerabilities.

Key elements of LASERS IT Security Management Program consist of utilizing hardware, applications, and personnel for:

- Preventing an intrusion into LASERS network by an outside party.
- Virus and malicious programs prevention, detection, and remediation.
- Internal security roles.
- Data protection.
- Software and hardware patch updates.
- Securely connecting users to LASERS network.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this engagement was to review IT security management in the areas which are covered by the Security Administrator including network perimeter defense, internal and external vulnerability management, and incident management.

Due to complex subject matter and the vast amount of processes within these areas, testing was limited to the existence of controls, compliance with procedures and policy, and effectiveness of outlined processes. This review was based on risk and limited to what could be performed by the Audit Services Division staff with the time and resources allotted. It should not be considered as comprehensive as what could be performed by industry experts who provide independent vulnerability testing. Control effectiveness was tested when feasible. For example, the testing of antivirus software tested for the existence of the software only. A virus was not developed or obtained to be used in testing whether the antivirus software was effective at identifying viruses.

The primary objectives of this engagement were to determine if:

- The network perimeter defenses are adequate and operating effectively.
- Internal and external vulnerability management is effective and controls are implemented to minimize IT security risks.
- IT security incidents identified through the incident reporting system are adequately addressed.
- Approved IT security policies and procedures are in place and followed.

Procedures used to complete this engagement included:

- Interviewing LASERS staff.
- Review of IT security policies, procedures, processes and controls.
- Review of external security reports.
- Testing of security controls where possible.
- Researching various resources for best practices of IT security.

- 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.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. NOT ALL COMPUTERS AND SERVERS HAVE LASERS APPROVED ANTIVIRUS SOFTWARE INSTALLED

OBSERVATION

According to IT procedure, as new computers (desktops and laptops) are issued or servers are deployed, antivirus software should be installed, monitored, and updated on them. According to IT, the antivirus software approved for enterprise use on LASERS issued computers and servers is Symantec Endpoint Protection (Symantec). Symantec is an antivirus software that includes firewall, Intrusion Prevention System, and advanced protection technologies. An unprotected computer or server weakens a first line IT security defense that prevents viruses from being introduced into LASERS network environment which could have a critical impact to LASERS.

It was observed that 22 of the 173 active LASERS computers and 14 of the 87 servers did not have Symantec installed on them that should have. It should be noted that during the review IT took the necessary steps to ensure Symantec has been installed on these devices.

RECOMMENDATION

IT should develop and implement a process to ensure that all LASERS computers and required servers contain the LASERS approved antivirus software, that the software is up to date, and functioning as expected.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016. The corrective action plan for this item is noted below.

Immediate Remediation Action Plan (COMPLETED)

All workstations and servers have been reviewed and any deficiencies in antivirus software protection have been corrected. Two exceptions are documented that have an approved alternate antivirus solution installed.

Further Remediation Planned

IT plans to perform the following additional corrective action to address this item:

- A standard IT policy for governance of antivirus software along with applicable supporting procedures will be developed that will address, at a minimum, the following:
  - When and how antivirus software is used.
  - Allowable exceptions.
  - Exception process including documentation and approval process.

    - Validation of process.
    - Notification structure for failure to follow policy.
- Based on policy, antivirus software protection for workstations will be automatically installed on any workstation connected to the LASERS network domain if not already present. To verify installations are occurring, a weekly report will identify any workstations on the LASERS network domain that do not conform to this policy. Antivirus software installation will occur within one business day of discovery of a deficiency.
- Based on policy, antivirus software protection for servers will be manually installed on all servers. To verify installations are occurring, a weekly report will identify any servers that do not conform to this policy. Software installations will occur as soon as possible, but no later than the next scheduled maintenance window which occurs on Friday evenings. Written procedures will be developed related to this.
- Employee training will be incorporated into the annual security training plan discussing the roles of employees in relation to virus protection at work and at home when connecting to the LASERS network. This may be either a manual or electronic process or both.

2. LASERS WEBSITE FILTERING APPLICATION AND APPROVAL PROCESS SHOULD BE REVIEWED

OBSERVATION

LASERS website filtering provided by Barracuda is used by IT to manage which websites, online content, and software applications employees can access or download through the internet. A Safe Search function is also utilized to prevent inappropriate content and images from returning while using a search engine such as Google, Yahoo, and Bing. According to the LASERS Information Technology Policy, employees authorized for internet access are subject to LASERS web filter. If an employee needs access to a website that is currently blocked, a request for access is made with approval from their division management. IT will then temporarily provide the user access or if it is determined the user will need frequent access, then IT can make it permanently available with the approval of Executive Management.

According to IT and testing, it was determined that the aforementioned process was not being consistently followed as stated in the policy. For example, there were several websites where permanent access was granted without formal approval documentation available as prescribed per policy.

In addition to the testing of the process, Audit Services performed limited testing of the Barracuda application. Audit Services concluded from testing and conversations with IT that the application continues to produce inconsistent results from what is expected from IT. Audit Services feels that one source of this is due to the configuration process in which user groups are frequently adjusted because of issues with Barracuda that IT has experienced. According to IT, these issues cannot be effectively identified or explained. These are the key reasons why Audit Services testing was limited in scope and depth. A couple of examples identified during limited testing is as follows:

- Users were able to download a blocked application that they should not have been able to access. IT is currently working on blocking the application download and is in contact with Barracuda to assist with resolving this issue due to some encountered difficulties.
- While using a search engine inappropriate content was returned.

A web filter is a primary control that serves as the first line of defense in protecting LASERS from outside viruses and programs and if not functioning properly then this inherently increases the risk that users could access malicious websites whether intentionally or not.

RECOMMENDATION #1

IT should perform a thorough review of the application and process used to manage website control at LASERS and take corrective action accordingly. Additionally, a continuous monitoring and testing process should be implemented to ensure compliance with both policy and procedures in this area.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016.

IT plans to perform the following corrective action to address this item:

- All current web access requirement documents will be reviewed and matched to current documentation and access will be removed if no longer necessary.
- A standard IT policy for governance of the web filter along with applicable supporting procedures will be developed that will address, at a minimum, the following:
    - Standard site blocking.
    - Allowable exceptions.
    - Exception process including documentation and approval process.
    - Validation of process.
    - Notification structure for failure to follow policy.
- All exceptions to normal web access restrictions will be documented and approved according to policy.
- A product search will be conducted that will review current web filtering hardware and software solutions. A recommendation will then be made to stay with the current solution or move to a new and improved product. The process will include, at a minimum, the following:
    - Identifying industry best practices.
    - Documenting requirements.
    - Conducing search and review of available products.
    - Developing recommendations.
- Training will be incorporated into the annual security training plan discussing the roles of employees and supervisors in relation to safe web browsing and requirements of our web browsing policies. This may be either a manual or electronic process or both.

RECOMMENDATION #2 (THIS ITEM IS CLOSED)

IT should take the necessary steps to resolve the two examples cited above.

RESPONSE

IT agrees with this recommendation. The two examples listed in the audit report and referred to in recommendation #2 have been corrected.

3. DATA LOGS ARE NOT EFFECTIVELY EVALUATED

OBSERVATION

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-92, a log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.

A fundamental problem with log management that occurs in many organizations is effectively balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by several factors, including a high number of log sources; inconsistent log content, formats, and timestamps among sources; and increasingly large volumes of log data. Log management also involves protecting the confidentiality, integrity, and availability of logs. Another problem with log management is ensuring that security, system, and network administrators regularly perform effective analysis of log data.

Additionally, NIST recommends that organizations should:

- Establish policies and procedures for log management.
- Prioritize log management appropriately throughout the organization.
- Create and maintain a log management infrastructure.
- Provide proper support for all staff with log management responsibilities.
- Establish standard log management operational processes.

According to IT, the monitoring of logs only occurs if an issue arises that requires a review of the logs to help identify how the problem occurred. For IT to continuously monitor LASERS logs for potential security weaknesses and other issues, IT would have to currently perform this manually.

RECOMMENDATION

IT should evaluate the current environment and establish policies and procedures to create an effective log management program.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017. The corrective action plan for this item is noted below.

Immediate Remediation Action Plan (COMPLETED)

If there are reasons to believe that a security anomaly has occurred, the Adaptive Security Appliance (ASA) and anti-malware logs will be reviewed and anomalies will be addressed by the IT Security Administrator. Currently, this will remain a manual process. In addition, Malware reports will be generated weekly to identify ongoing security risks and will be followed up on by the IT Security Administrator.

Further Remediation Planned

IT plans to perform the following additional corrective action to address this item:

- A review will be done of the NIST infrastructure logging recommendations and a standard IT policy for governance of logging along with applicable supporting procedures will be developed that will address, at a minimum, the following:
  - What is monitored with logging software.
  - What is monitored without logging software.
  - Validation of process.
  - Notification structure for failure to follow policy.
- An evaluation and recommendation will be made of available software to effectively aggregate and manage logging based on current best practices.

4. A COMPREHENSIVE IT SECURITY ASSESSMENT PLAN SHOULD BE ESTABLISHED

OBSERVATION

Vulnerability testing is important to analyze the potential weaknesses of LASERS current security setup. Tests can vary from external penetration testing, internal controls testing (i.e., internal security testing), and social engineering testing. External security testing offers the ability to view the environment's security posture as it appears outside the security such as firewall and antivirus software with the goal of revealing vulnerabilities that could be exploited by an external attacker. Internal security testing reveals vulnerabilities that could be exploited by a trusted insider or an attacker who has penetrated the first line of defenses. It also focuses on system-level security to eliminate as many system security risks as possible. Social engineering tests identify potential weaknesses with the staff and the potential for LASERS information to be released.

Over the past several years, IT has utilized contracted services for vulnerability testing. According to IT, they perform this type of testing every 12 to 18 months. When reviewing the past several years it was observed that in May of 2009 a social engineering test was contracted and performed. In July 2012, December 2014, and March 2016 an external penetration testing was contracted and performed. An internal security test has not been performed.

A comprehensive IT security assessment plan to organize the various testing methods does not exist. A plan should identify risks and establish testing requirements. It would allow for a comparison of tests already performed and identify any gaps in the testing to ensure coverage of those areas in the future. This could also identify areas that could be tested by internal LASERS staff thus reducing the scope and the cost of future contracts or allow for the contractors to test more with the same budget.

RECOMMENDATION

IT should establish an overall vulnerability assessment plan. It should also include a method to review potential vendors to identify who can fill the vulnerability testing need. For example, the Department of Homeland Security (DHS) can provide various types of vulnerability testing at no cost to LASERS.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- An IT Security Assessment Plan will be developed that addresses schedules and types of tests for:
  - Manual vulnerability testing
  - Automated vulnerability testing
  - Validation of tests
- A risk analysis will be performed for the Department of Homeland Security assessment recommendation.

5. AN IT SECURITY INCIDENT RESPONSE PLAN SHOULD BE FORMALLY IMPLEMENTED

OBSERVATION

The approval and implementation of an IT Security Incident Response Plan is important to prepare LASERS to appropriately handle security incidents, provide training, and make employees and contractors aware of the incident reporting process and their responsibilities. According to NIST SP.800-61r2, a security incident response plan is one of the important items to have for creating an effective security incident response capability in an organization.   A creation of an incident response plan, policy and procedure are important parts of establishing a team to help ensure that an incident response is performed effectively, efficiently and consistently. Additionally, the plan, policy, and procedure must allow the team to be empowered to do what needs to be done to rectify an incident.
It should be noted that IT has developed a draft IT Security Incident Response Plan, but it has not been approved or formally implemented.

RECOMMENDATION

IT should evaluate the current draft Security Incident Response Plan and make any necessary adjustments and take the steps to formalize and implement this plan for LASERS.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- A standard IT Security Response Plan will be developed and approved that will address, at a minimum, the following:
  - Detection
  - Analysis
  - Recovery
  - Post-Incident
- A testing plan for the incident response will be developed that will be tested on an agreed upon testing period between IT and Audit for validation of process and improvements.
- Investigation will be made into having a vendor retainer for incident responses to ensure that the environment is ready for a security incident and that support would be available to respond timely.
- Investigation will be done into data breach notification laws for the state of Louisiana so that LASERS is aware of what our legal requirements are. Data breach insurance policies will also be investigated and an analysis conducted.

6. LOCAL ADMINISTRATOR PRIVILEGES WERE NOT REMOVED TIMELY

OBSERVATION

A user that is a local administrator of their computer allows them to have elevated privileges. A main privilege is that a user is able to install and uninstall applications on their LASERS computer with minimal restrictions. IT will grant an employee these privileges temporarily or permanently in order to perform job related tasks. These elevated privileges inherently reduce controls and increase the risk of a possibility for the computer and LASERS network to be impacted by a virus or some other malicious software, whether intentionally or unintentionally. Due to this risk, IT noted that they perform a weekly review of the list of employees that have local administrator privileges on their computer.

While reviewing a list of users, it was determined that 27 had local administrator privileges on their computer that should not have and IT has since taken the necessary steps to remove these privileges. When discussing the approval process with IT, it was determined that a formal policy and set of procedures to grant these privileges has not been established.

RECOMMENDATION

IT should establish a procedure for providing, monitoring, and removing administrator privileges for a user's computer similar to other processes that require special permissions. When providing access, IT should evaluate what level of administrator privileges should be granted based on the situation instead of providing all administrator privileges. Additionally, IT should perform a review of the current users with local administrator privileges and apply the newly developed procedure.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016.

IT plans to perform the following corrective action to address this item:

- All accounts that have local administrator access and should not have them will be corrected. All exceptions will be documented and formally approved.

- A standard IT policy for governance of local administrator access along with applicable supporting procedures will be developed that will address, at a minimum, the following:
  - Allowable exceptions.
  - Exception process including documentation and approval process.
  - Validation of process.
  - Notification structure for failure to follow policy.

7. IT SECURITY TRAINING PROGRAM FOR EMPLOYEES SHOULD BE ENHANCED

OBSERVATION

IT security related information is provided to all LASERS employees in two key ways. First, an IT security policy video is provided to newly hired employees during orientation. Second, IT security related items are communicated to employees on a periodic basis via email, employee newsletter, and agency wide staff meetings. This approach is a good way to increase the general level of IT security awareness, but there is no guarantee that employees will read the email, look at the newsletters, or understand the subject matter. A formalized plan to consistently inform LASERS staff of the ever changing security threats and actions they should take has not been documented.

RECOMMENDATION

IT should formalize and implement an organizational-wide IT security training program to ensure every employee knows how to recognize IT security red flags and how to respond accordingly.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- A training plan will be developed which will include, at a minimum, the following:
  - New hire training will be implemented that covers security topics.
  - Periodic and ongoing training provided to all staff which cover focused topics such as: virus and malware protection best practices, web surfing issues, typical email attacks, phone scams, and/or other data security related topics as they become available.
  - Security presentation to the LASERS board.
  - Recommendation will be made into the purchasing or development of online computer based security training that can be distributed on a regular basis and be required to complete by staff similar to other HR required trainings.

8. NOT ALL COMPUTERS HAVE ENDPOINT SECURITY SOFTWARE INSTALLED

OBSERVATION

LASERS utilizes Lumension endpoint security software which limits the user's ability to perform certain tasks on their computers such as, accessing external storage devices and writing files to CDs. Lumension helps reduce the opportunity for malicious programs to be introduced into LASERS network and confidential data to be copied from LASERS systems since it prevents an employee from connecting external drives to their computer. IT noted that procedures related to Lumension do not exist because it is a difficult software to trouble shoot and issues encountered are not consistent across all computers.

It was observed that 55 of the 173 active LASERS computers did not have Lumension installed on them and should have. It should be noted that during the review IT took the necessary steps to ensure Lumension has been installed on these devices. Furthermore, 70 of the 173 active LASERS computers were classified as being exempted from having Lumension installed on them. According to IT, these computers are exempted based on business need. However, there is no written procedure or divisional policy related to exempting computers from using Lumension.

RECOMMENDATION

IT should perform a thorough review of the Lumension application and the process used to manage endpoint protection at LASERS and take corrective action accordingly. This review should also include developing a methodology for providing exemptions to determine whether a complete exemption or a partial exemptions should be provided. A re-evaluation of the current exemptions should be performed using this new methodology. For those who still require complete exemption, then an evaluation of other possible controls to mitigate applicable risks should be performed and implemented accordingly. Lastly, a continuous monitoring and testing process should be implemented to ensure compliance with both policy and procedures in this area.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016. The corrective action plan for this item is noted below.

Immediate Remediation Action Plan (COMPLETED)

All workstations have been reviewed and any deficiencies in endpoint security software protection have been corrected. All exceptions are documented.

Further Remediation Planned

IT plans to perform the following additional corrective action to address this item:

- A standard IT policy for governance of endpoint security software along with applicable supporting procedures will be developed that will address, at a minimum, the following:
    - When and how endpoint security software is used.
    - Allowable exceptions.
    - Exception process including documentation and approval process.
    - Validation of process.

    - Notification structure for failure to follow policy.
- Based on policy, the endpoint protection product will be automatically installed on any workstation connected to the LASERS network domain if not already present. To verify installations are occurring, a weekly report will identify any workstations on the LASERS network domain that do not conform to this policy. Software installations will occur within one business day of discovery of a deficiency.

9. NOT ALL NETWORK SWITCHES WERE UPDATED ACCORDING TO PROCEDURE

OBSERVATION

A network switch is a computer hardware device that connects other devices together on a computer network. It forwards and controls data flowing across the network to specific devices that need to receive it instead of broadcasting the data to all connected devices. When new security vulnerabilities are identified, the vendor may decide to release a security update patch that needs to be installed on the affected device to reduce its exposure to those vulnerabilities.

LASERS IT procedure currently in place requires the network switch operating system (OS) to be evaluated for new updates on a bi-annual basis in June and December. If a new update is identified, then it is applied across all affected devices.

During this review, it was identified that five of the thirteen network switches in the LASERS environment were not updated to the current OS version in accordance with the outlined procedure notated above. It should be noted that during this review IT took the necessary steps to ensure these switches are on the current OS version.

RECOMMENDATION

IT should make the necessary changes to their monitoring process that will ensure the following:

- Real time notification when a new version of a network switch OS is released.
- Testing and installation of the new version is completed in a timely manner.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- A procedure will be established and followed to review switch and network device code on a quarterly basis and update as necessary. All exceptions to this process will be documented.
- The IT Security Administrator will submit a code summary and action plan report to the IT Tech Support Manager on a quarterly basis outlining the plans for the updates including reasons that these updates were not done. Note: There may be legitimate reasons to delay or cancel code updates.
- Investigation will be made into options for notification lists on all devices to ensure understanding when switch or network device updates becomes available.

10. PROCEDURE RELATED TO VPN ACCESS NOT CONSISTENTLY FOLLOWED

OBSERVATION

A VPN allows users to securely access LASERS systems while off-site through an internet connection which reduces the potential risk of exposing LASERS data compared to an open internet connection. According to IT procedure, VPN access is granted with an approved access request form. Furthermore, employees are required to submit a new approved form every year and failure to do so will result in their access being revoked. During testing, it was identified that four people had access to VPN, but did not have a VPN form on file. It should be noted that during this review the VPN access for the four users identified was revoked.

RECOMMENDATION

IT should develop and implement a process to ensure that VPN access is provided and maintained in accordance with procedure.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016.

IT plans to perform the following corrective action to address this item:

- The IT security administrator will reconcile the VPN access audit list to the VPN access form. The reconciled report will be turned into the IT Tech Support Manager. All exceptions will be documented.
- A standard IT policy for governance of VPN along with applicable supporting procedures will be developed that will address, at a minimum, the following:
  - When VPN access is allowed and how access is managed (including supported operating systems, acceptable virus software and acceptable levels of system updates required).
  - Allowable exceptions.
  - Exception process including documentation and approval process.
  - Validation of process.
  - Notification structure for failure to follow policy.
  - An annual review process will be performed of these VPN forms to ensure compliance.

11. VPN SECURITY VALIDATION SOFTWARE SHOULD BE REVIEWED

OBSERVATION

Before a user is allowed to establish a connection to LASERS VPN, a software will scan the computer trying to connect and ensure it has an approved virus protection software and that it is up-to-date with a recent virus definitions file. If the computer trying to connect does not meet this criteria, then the software will not allow the machine to connect. This is in place to further reduce risk to LASERS systems by ensuring the device connecting remotely has the latest protection from viruses and malware. During testing, it was observed that an authorized VPN user was able to successfully connect to LASERS network using a laptop with an outdated antivirus definition file.

According to IT, these requirements were temporarily disabled to allow a user to connect via VPN that was having issues connecting. At the time, IT was not able to identify why the user could not connect, so they disabled the control while attempting to identify the issue. IT stated that the control was re-instated and the issue of connecting to LASERS with an outdated virus definition file was rectified. However, during re-testing it was observed that an authorized user was still able to connect to LASERS VPN with an out-of-date virus definition file.

RECOMMENDATION #1 (THIS ITEM IS CLOSED)

IT should rectify the issue and identify why the user was allowed to connect with out-of-date virus definitions. While performing testing, all VPN control settings should be tested to ensure that no other control fails and allows a user to connect to LASERS VPN when they should not be allowed to.

RESPONSE

IT agrees with this recommendation. IT performed the following to verify this item has been addressed:

- The current VPN validation software was verified as enabled and was tested remotely by disabling antivirus and the connection was denied.
- An additional test was performed where the VPN validation rules were modified to require virus definitions be no more than one-day old. A computer with two day old definitions attempted access and was denied.
- An additional test was performed by disabling the firewall on the computer and attempted access was denied.

RECOMMENDATION #2

IT should develop and implement a process to ensure that VPN access settings are continuously enforced. A testing plan should be developed to ensure it is working as intended. If an issue arises with the software, a formalized process should be established to handle these types of situations. For example, access should be temporarily suspended until the issue is resolved or access is granted with IT management approval. Additionally, IT should evaluate the current VPN access control environment and determine if additional controls are necessary. For example, the addition of a security token to the validation requirements.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as high with a target completion date of December 31, 2016.

IT plans to perform the following corrective action to address this item:

- A standard IT policy for the governance of the VPN will be developed. See response to Observation 10, Recommendation 1.
- Testing of these controls will be completed according to the VPN policy.
- Regular testing of environment after any changes to ensure the antivirus definition and windows update functionality verification is still enabled and functional will be established according to policy.

- A product search will be conducted that will review VPN solutions. Based on results, a recommendation will be made to stay with the current solution or move to a new product. The process will include, at a minimum, the following:
  - Identifying industry best practices.
  - Documenting requirements.
  - Conducting search and review of available products.
  - Developing recommendations.

12. EXTERNAL USER ACCESS TO LASERS NETWORK COULD BE MANAGED MORE EFFECTIVELY

OBSERVATION

IT utilizes external parties (i.e., vendors) who may need remote LASERS VPN access as they perform contracted work for LASERS. According to IT, the process to provide access for external parties is outlined in the Security Account Process Review procedure. This procedure is the same for managing LASERS employee access and requires proper authorizations. Additionally, it was observed that in some instances, authorization was written into the contract allowing for a remote connection. However, this was not observed in all contracts nor was there specific people named in the contract identifying who shall be provided access. A formal procedure for requesting, approving, and monitoring third party VPN access does not exist.

During testing, the following was identified relating to external user account VPN access:

- Three instances where VPN access was established for an external user account and there was no provision in the contract authorizing remote access.
- Three external user accounts where VPN access was not disabled upon the completion of the contracted work.
- Three external user accounts were set up with VPN access without an expiration date.

It should be noted that during this review these exceptions were discussed with IT resulting in three external user accounts being disabled and the establishment of an expiration date for three accounts.

RECOMMENDATION

A policy and a process should be developed and implemented to authorize, grant, monitor, and timely remove the remote VPN access to LASERS systems for external parties.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- A standard IT policy for governance of external vendor VPN access along with applicable supporting procedures will be developed that will address, at a minimum, the following:
  - When external vendor VPN access is allowed and how access is managed.
  - Identify the LASERS role responsible for approval of vendor VPN access.
  - Frequency of access review.
  - Standard contract verbiage related to VPN access.

  - Validation of process.
  - Notification structure for failure to follow policy.
- The IT Security Administrator will report the status of all vendor remote access accounts to the IT Tech Support Manger on a weekly basis.

13. MOBILE DEVICE PASSCODE NOT REQUIRED FOR ALL DEVICES UTILIZING THE AIRWATCH APPLICATION TO ACCESS LASERS EMAIL SYSTEM

OBSERVATION

A LASERS employee can access their email on their mobile device in two ways. One way is to utilize the LASERS webmail website which requires them to log into their account the same way they would if they were at home using their computer. This can be tedious for users who frequently check their email. To solve this problem, LASERS IT implemented the AirWatch software that securely makes their LASERS email readily available on their mobile device. To utilize AirWatch, the user must be approved and also consent to allowing IT to utilize AirWatch to set controls on their device.

According to IT procedure**,** the AirWatch application is configured to require a device to have a passcode in order to connect to their LASERS email. This is an important control because without a passcode, if a device is lost or stolen, someone outside of LASERS would have instant access to LASERS information. To ensure security rules are enforced, IT uses the AirWatch management console to establish and monitor the security access and device controls for all approved users.

During this review, it was identified that the device passcode requirement was not enforced for 20 of the 26 devices enrolled in AirWatch. The lack of passcode enforcement does not mean that these devices did not in fact have a passcode, but simply the IT control to require a passcode was not enabled for all devices. It should be noted that during this review IT updated the AirWatch control to now require all devices to have a passcode.

RECOMMENDATION

IT should develop and implement a review and monitoring process to ensure all users and devices connected to LASERS via AirWatch are in compliance with the IT controls and requirements.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017. The corrective action plan for this item is noted below.

Immediate Remediation Action Plan (COMPLETED)

All AirWatch controls of requiring a passcode have been corrected. Email controls and the control to disallow “jailbroken” phones to connect to LASERS email has been verified. There were no exceptions noted. The term “jailbroken” refers to a process of removing software restrictions placed on the device by either the manufacturer or carrier/seller. Default restrictions are placed on devices by manufacturer and carriers to secure the core code and file system of the device against malicious activity. Breaking these default restrictions is called

"Jail Breaking" a device and can allow malicious and unsecure code or apps to run on the device.

Further Remediation Planned

IT plans to perform the following additional corrective action to address this item:

- A standard IT policy for governance of mobile devices on the LASERS network along with applicable supporting procedures will be developed that will address, at a minimum, the following:
    - When mobile devices are allowed on the LASERS network.
    - Required safeguards for LASERS data on mobile devices.
    - Allowable exceptions.
    - Exception process including documentation and approval process.
    - Validation of process.
    - Notification structure for failure to follow policy.
- A standard procedure for management of mobile devices will be developed to include, at a minimum, the following:
    - Pre-upgrade assessment of impact to LASERS environment.
    - Post-upgrade functionality regression testing which includes a post-upgrade report delivered to the IT Tech Support manager.
    - Notification to the IT Security Administrator of any changes made to the mobile device management system to ensure that all security policies with the system remain in effect.

14. IT SECURITY OVERSIGHT SHOULD BE EVALUATED TO INCREASE EFFECTIVENESS

OBSERVATION

The roles and responsibilities of overseeing LASERS IT security is currently divided between multiple employees at LASERS. This separation of duties is inherently riskier than having a centralized person to oversee the various security roles and processes. A decentralized security oversight increases the risk that the application of security policies and procedures will be inconsistent, thus increasing the difficulty of ensuring the security and protection of LASERS systems and information.

The security oversight could be centralized to one individual who would oversee the team and ensure that all policies are standardized, implemented, and adhered to; however, they may not necessarily perform all of the task they are overseeing. This person would have a holistic view of the IT security risks facing LASERS and be able to identify technologies and implement processes to help minimize those risks. This person would have an understanding of how this change would affect the overall IT security environment which is governed by the LASERS IT policy.

RECOMMENDATION

IT should evaluate the current security oversight management function and determine which IT staff manages each role, their responsibilities, and their authority. An analysis of this would help determine the necessary changes needed to increase the effectiveness of the IT security management oversight function.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017. IT plans to review the existing management structure and various IT security roles and responsibilities and changes will be recommended, as needed, to increase the overall effectiveness of IT security management and oversight.

15. AN OVERALL IT GOVERNANCE AND MANAGEMENT FRAMEWORK DOES NOT EXIST

OBSERVATION

IT has implemented an overall IT policy and has procedures for several areas of IT operations. However, some procedures are very detailed, some are more of an overview, and some do not exist. These inconsistencies create a potential for inconsistent application of the processes. Currently an overall IT governance and management framework does not exist. A framework could assist with addressing the observations noted in this report by setting a standard for all areas of IT as well as aid in the overall management of the IT division.

RECOMMENDATION

IT should review the various framework options available and consider adopting a comprehensive IT governance framework approach that best fits LASERS environment. A comprehensive framework could affect the organization as a whole; therefore, input from various organizational stakeholders is necessary.

RESPONSE

IT agrees with this recommendation. The priority to address this recommendation has been set as medium with a target completion date of June 30, 2017.

IT plans to perform the following corrective action to address this item:

- An IT governance policy for security management will be developed. This policy will address, at a minimum, the following:
    - Uses for security software and settings:
        - Antivirus
        - Endpoint security
        - Web filtering
        - Log monitoring
        - Security assessments
        - Local administrators
        - VPN access
        - Mobile device management
    - Standard exception process:
        - When exceptions are allowed.
        - Approval process.
        - Required documentation.
    - Standard validation.
    - Notification structure to follow policy.

- Internal review of current security hardware appliances and software security solution suites to reaffirm continued use or recommend replacement or upgrade options including testing and cost proposals.
- Policy will be reviewed on an annual basis.
- Frameworks will be investigated to identify a framework or blend of frameworks that works best for LASERS.

FOLLOW-UP

A follow-up to this engagement has been scheduled for fiscal year end 2017. Audit Services will maintain this information on a tracking report. These items will be tracked until they are closed.

Blake Lee, CISA
Audit Services Manager

Ryan Babin, CIA, CISA
Audit Services Director

Cc: Maris LeBlanc
Trey Boudreaux
Dan Bowden
Eric Schoonmaker
Greg Byrd
Brent Fitch