Executive Summary

The National Institute of Standards and Technology (NIST) defines patch management as the process for identifying, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware, and add new features including security capabilities.

Patch management is a vital portion of any institution's computer security program. The Department of Highway Safety and Motor Vehicle's (Department) Information Systems Administration (ISA) is responsible for administering the patch management program for the Department. There are two bureaus within ISA that deploy the patch management program: Service Support and Service Operations. ISA deploys patches to member workstations and field servers, while the Agency for State Technology (AST) deploys patches to Windows and managed servers.

Service Support is further broken down into two different sections: Client Services and Platform Systems. Client Services is responsible for Desktop Support, which provides workstation software installation and updates including patching in the Kirkman Headquarters building and the Technical Assistance Center which handles Department wide IT issues. Platform Systems is responsible for the field servers and workstations.

Service Operations provides support for the Department’s platforms, systems, network, storage, and telecommunications/phone infrastructure. This infrastructure is the foundation for the Department’s databases, applications, and software products. Service Operations works primarily with AST as many of the managed servers are located at and patched by AST.

The purpose of this audit was to review and evaluate the efficiency and effectiveness of the Department’s patch management. Overall, the Department maintains effective operations of the patch management process. However, our review noted key areas where ISA could implement improvement:

- The Department should have an active Service Level Agreement (SLA) with AST;
- A review of administrator access rights is needed to ensure security of our IT resources;
- Strengthening patch management procedures would enhance the patch management process; and
- Patch Deployment should be timely.
Background and Introduction

NIST defines patch management as the process for identifying, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware, and can also add new features including security capabilities. In the case of operating systems and computer server software, patches have the important role of fixing security vulnerabilities.

Rule 74-2, Florida Administrative Code, requires that each agency’s security policies, processes, and procedures are maintained and used to manage protection of information systems and assets. It further requires each agency establish a configuration change control process to manage upgrades and modifications to existing IT resources. This includes determining the types of changes that are configuration controlled such as emergency patches, releases, and other out-of-band security packages.

Patch management is a vital portion of any institution’s computer security program. The Department’s ISA, in coordination with AST, is responsible for administering the patch management program for the Department. There are two bureaus within ISA that deploy the patch management program: Service Support and Service Operations. ISA deploys patches to member desktops and laptops (workstations) and field servers, while AST deploys patches to Windows and managed servers.

Service Support

Service Support is further broken down into two different sections: Client Services and Platform Systems. Client Services is responsible for Desktop Support, which provides workstation software installation and updates including patching in the Kirkman Headquarters building and the Technical Assistance Center which handles Department IT issues.

Client Services uses the Microsoft System Center Configuration Manager (SCCM) to deploy patches to the workstations in the Kirkman headquarters building. Patches are downloaded using SCCM and are deployed using an automatic deployment rule. Once the rule is set, the patches will automatically download and install at defined intervals. Prior to the patches being deployed to the entire directory, they are sent to a pilot or test group to ensure the patch or update is compatible and has no malfunctions or issues.

Platform Systems is responsible for the installation, tuning, and maintenance of enterprise platform servers, hardware, operating system software, and infrastructure software environments for the field offices. Platform Systems uses the Windows Server Update Services (WSUS) program to download and deploy patches to the Department servers located in the field offices. Platform Services is currently transitioning from the
WSUS program to SCCM to patch the field workstations with the same properties as the Kirkman headquarters workstations.

**Service Operations**

Service Operations provides support for the Department’s platforms, systems, network, storage, and telecommunications/phone infrastructure. This infrastructure is the foundation for the Department’s databases, applications, and software products. Service operations works primarily with AST as many of the managed servers are located at and patched in conjunction with AST.

**Agency for State Technology**

AST was established in 2014 by the Florida Legislature to develop and publish information technology policy for the management of the state’s information technology resources. It oversees the state’s essential technology projects and manages the State Data Center. Section 282.201, Florida Statutes (F.S.), establishes AST as the State Data Center and defines the duties they shall provide to its customers.

The intent of AST is to provide efficient and effective means of quality utility data processing services to state agencies and to concentrate computing resources in quality facilities that provide proper security, disaster recovery, infrastructure, and staff resources. The responsibilities listed in Section 282.201, F.S., include entering into a SLA with each customer entity to provide the required type and level of service. AST’s responsibilities also include housing and patching the Department servers.

Each month, AST patches Department servers. AST and Department members communicate frequently and work together during the patching process to complete the updates and restart servers as needed. AST offers a customer portal that allows members to report incidents, request service, or view status of previously submitted tickets; including all patch updates that have been applied. The information included within the patch updates include: status of the patch, type of patch, priority, risk, and the expected downtime.

**Findings and Recommendations**

Overall, the Department maintains effective operations of the patch management process. However, our review noted key areas where ISA could implement improvement:
**Service Level Agreement**

**Finding No. 1:** The Department should have an active SLA with AST.

Section 282.201, F.S., establishes the state data center within AST to provide data center services for state agencies. It also requires AST to enter into a SLA with each customer entity to provide the required type and level of service. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease services.

During our review of the patch management process, we noted there is no SLA between the Department and AST. The Department previously had an SLA in effect for the state shared resource center prior to the Florida Legislatures’ establishment of AST in 2014; however, this SLA expired on October 31, 2015.

The SLA lists all of the services AST provides to the Department. Additionally, the SLA includes Department specific requirements for our technical environment. These customer specific requirements include: a right to audit clause, standard maintenance windows, security requirements for law enforcement and Criminal Justice Information Services, and roles and responsibilities that are necessary for the function of the day-to-day services the Department provides to the public.

**Recommendation**

We recommend ISA collaborate with AST to establish and enact a SLA.

**Management Response**

ISA continues to work with AST to finalize a SLA. The Customer Specific Attachment “B” was completed by ISA and sent to the AST SLA Coordinator on February 7, 2017. If AST concurs, the SLA will be sent to legal for review and then routed for signature.

**Access Rights**

**Finding No. 2:** A review of administrator access rights is needed to ensure security of IT resources.

The principle of least privilege states only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary. During our review of administrator access rights, we noted, as of October 2016, there were 56 users that have Domain Administrative access rights for the Department, including 39 AST members.
Section 282.201(2)(f), F.S., gives authority to AST as the state data center to have administrative access rights to IT resources housed at their facility; however, the number of users with administrator access rights is significant. Anyone with domain administrative rights has the ability to navigate throughout the networks.

**Recommendation**

We recommend ISA initiate a review of users, to include AST, with Department Domain/Server Administrator access to ensure the number of administrators is appropriate when using the principle of least privilege.

**Management Response**

ISA has reviewed access rights with AST and has reduced the number of users with Department Domain/Server Administrator access to 26.

**Procedures**

**Finding No. 3:** Strengthening patch management procedures would enhance the patch management process.

Written policies or procedures, which clearly define the responsibilities of employees, are essential to provide management and members with guidelines regarding the effective, efficient, and consistent conduct of business and the effective safeguarding of assets.

During our review of the patch management process, we noted there are limited procedures for the patch management process which do not cover all aspects of patch management. Patch management guidelines are in place for the field servers and ISA follows AST guidelines in coordination with AST for patching for the managed servers; however, they do not provide specifics for patching applications.

Patch management procedures for the Kirkman Headquarters workstations do not provide specifics on the following: use of SCCM, automatic deployment rule, administrative rights to deploy patches, pilot groups, monitoring, or back-out plans for corrupted or malfunctioned patches. There are currently no patch management procedures for field workstations.
Recommendation

We recommend ISA enhance their procedures to include at a minimum:
- Deployment of patches;
- Third party patches; and
- Back-out plans for patches.

Management Response

ISA will update and publish patch management procedures by the end of June 2017. These procedures will include the deployment of patches, third party patches, and back-out plans for patches.

Patch Deployment

Finding No. 4: Patch Deployment should be timely.

Applying patches significantly eliminates vulnerabilities which reduce the opportunity for exploitation. Patches are usually the most effective way to mitigate software vulnerabilities without negatively impacting functionality. If patches are not routinely deployed, the Department faces security vulnerabilities and concerns with functionality of applications and operating systems.

During our review of the patch management process we noted as of December 2016, field workstations have not been patched since August 2016. The patch management process for field workstations is being transitioned from WSUS to SCCM, causing delays in the deployment of patches for those workstations.

Additionally, our review of all field servers noted a total of 430 patches needed to be applied to 258 of 433 servers, and two servers had 44 failed patches as of December 12, 2016. Field servers had a rare occurrence for the November 2016 patches that caused a number of servers to need manual restarts; therefore, raising the number of needed patches. Finally, our review of compliance for Adobe Flash Player within SCCM noted 2,855 of 4,201 computers (67.96%) needed a patch as of September 2016.

During the course of our audit, as part of the Department’s IT risk assessment, EY performed a vulnerability scan between September and December 2016. The vulnerability scan consisted of approximately 20 percent of the Department’s infrastructure, including 30 servers managed and maintained by AST. Based on our review of the scan, vulnerabilities were identified with the Department servers maintained by AST.
Recommendation

We recommend ISA ensure patches for workstations, servers, and third party applications are deployed appropriately and timely.

We also recommend ISA implement a process to periodically monitor patch implementation across all Department servers and workstations, including those housed at AST.

Management Response

The bulk of the deficiency regarding timely patch management resides with the remote field offices. The ISA Bureau of Service Support has proposed reallocating an existing Service Support member to ameliorate “field office patch management.” ISA will remediate this portion of the finding within 120 days of implementing the reallocated position.

Many of the discovered vulnerabilities were “out of scope” for patching by AST staff. Discussions are ongoing with AST to plan a remediation strategy for patching existing vulnerabilities, and periodic monitoring for new exposures. This strategy will be executed by the end of August 2017.

Purpose, Scope, and Methodology

The purpose of this audit was to review and evaluate the efficiency and effectiveness of the Department’s patch management.

The scope of this audit included a review of the patch management process for Department computer systems, applications, software, and servers.

Our methodology included:

- Reviewing applicable Statutes, Rules, manuals, and procedures;
- Interviewing appropriate Department and AST members;
- Reviewing AST’s process for Department patching;
- Reviewing AST’s monitoring of Department patching;
- Determining Department process for deployment of patches;
- Determining who has the authority to deploy patches;
- Reviewing SCCM, WSUS, and Lumensions use;
- Sampling Department IT resources to determine if software patches are up-to-date;
- Reviewing the pilot group; and
- Reviewing the back-out plan for potential malfunction of patches.
Distribution, Statement of Accordance, and Project Team

Distribution

Terry L. Rhodes, Executive Director
Diana Vaughn, Deputy Executive Director
Jamie DeLoach, Chief of Staff
Boyd Dickerson-Walden, Chief Information Officer
Scott Bean, Chief of Service Support
Eric Brown, Chief of Service Operations

Melinda M. Miguel, Chief Inspector General
Sherrill F. Norman, Auditor General
Tabitha McNulty, Inspector General, AST

Statement of Accordance

Section 20.055, Florida Statutes, requires the Florida Department of Highway Safety and Motor Vehicles' Inspector General to review, evaluate, and report on policies, plans, procedures, accounting, financial, and other operations of the Department and to recommend improvements. This audit engagement was conducted in accordance with applicable International Standards for the Professional Practice of Internal Auditing published by the Institute of Internal Auditors and Principles and Standards for Offices of Inspector General published by the Association of Inspectors General.

Project Team

Engagement conducted by:
John Brancale, Auditor
Keaton Wilson, Auditor

Under the supervision of:
David Ulewicz, Audit Director

Approved by:

[Signature]
Julie M. Leffler, Inspector General
ATTACHMENT – Management Response

MEMORANDUM

DATE:  February 24, 2017

TO:  David Ulewicz, Audit Director

FROM:  Clayton B. Dickerson-Walden, Chief Information Officer

SUBJECT:  Information Systems Administration Response to the IT Patch Management Audit (Audit Report No. 201516-22)

The following is our response to the findings and recommendations presented in the report.

Finding 1. Service Level Agreement

The Department should have an active Service Level Agreement with the Agency for State Technology.

Recommendation

We recommend Information Systems Administration collaborate with the Agency for State Technology to establish and enact a Service Level Agreement.

Management Response

The Division continues to work with the Agency for State Technology to finalize a Service Level Agreement. The Customer Specific Attachment “B” was completed by the Division and sent to the AST SLA Coordinator on February 7, 2017. If the Agency for State Technology concurs, the Service Level Agreement will be sent to legal for review and then routed for signature.
Finding 2. Access Rights
A review of administrator access rights is needed to ensure security of IT resources.

Recommendation
We recommend Information Systems Administration initiate a review of users, to include the Agency for State Technology, with Department Domain/Server Administrator access to ensure the number of administrators is appropriate when using the principle of least privilege.

Management Response
The Division has reviewed access rights with the Agency for State Technology and has reduced the number of users with Department Domain/Server Administrator access to 26.

Finding 3. Procedures
Strengthening patch management procedures would enhance the patch management process.

Recommendation
We recommend ISA enhance their procedures to include at a minimum:
- Deployment of patches;
- Third party patches; and
- Back-out plans for patches.

Management Response
ISA will update and publish patch management procedures by the end of June 2017. These procedures will include the deployment of patches, third party patches, and back-out plans for patches.

Finding 4 – Patch Deployment
Patch Deployment should be timely.

Recommendation
We recommend Information Systems Administration ensure patches for workstations, servers, and third party applications are deployed appropriately and timely.

We also recommend Information Systems Administration implement a process to periodically monitor patch implementation across all Department servers and workstations, including those housed at the Agency for State Technology.

Management Response
The bulk of the deficiency regarding timely patch management resides with our remote field offices. ISA Bureau of Service Support has proposed reallocating an existing Service Support member to ameliorate field office patch management. ISA will remediate this portion of the finding within 120 days of implementing the reallocated position.

Many of the discovered vulnerabilities were “out of scope” for patching by AST staff. Discussions are ongoing with AST to plan a remediation strategy for patching existing vulnerabilities, and periodic monitoring for new exposures. This strategy will be executed by the end of August, 2017.