ATTACHMENT A

ORANGE COUNTY TRANSPORTATION AUTHORITY

Performance Audit of

OCTA's Patch Management Program

February 18, 2020

FINAL REPORT

Prepared by:
BCA Watson Rice LLP
Certified Public Accountants and Management Consultants

TABLE OF CONTENTS

CONCLUSION

Based on the audit, the Orange County Transportation Authority's Patch Management Program for the Windows operating system environment complies with industry standards and best practices; however, the program should be expanded to address areas outside the Windows environment. In addition, we have identified areas of improvement that will further enhance the program.

INTRODUCTION AND BACKGROUND

The Orange County Transportation Authority's (OCTA) Internal Audit Department contracted with BCA Watson Rice (BCAWR) to conduct a performance audit of OCTA's Patch Management Program (PMP). The purpose of the audit was to assess and test the adequacy of OCTA's PMP and to make detailed recommendations for improvement based on industry standards, best practices, economies, and efficiencies. The audit included testing of OCTA's compliance with its patch management policies and procedures and best practices including the National Institute of Standards and Technology (NIST) 800-53, Revision 4 Security Standards and NIST 800-40, Revision 3, titled "Guide to Enterprise Patch Management Technologies". BCAWR used its corporate knowledge of OCTA and its extensive knowledge of best practices to develop a detailed work plan to perform this audit as outlined in the methodology section of this report.

At the time of the audit, OCTA's PMP addresses the following components:

1. Approximately 950 individual user accounts;
2. Approximately 950 Windows workstations;
3. Approximately 90% of the workstations (which are run on Windows 10) with the remaining workstations running on Windows 7;
4. Approximately 200 Linux devices;
5. Approximately 900 network devices; and
6. 350 Windows Servers (Windows Server 2012 and 2016, currently migrating from the remaining 2008 Servers).

BCAWR affirms that it is independent of OCTA and conducted the performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and relevant best practices. GAGAS requires that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. BCAWR believes that the evidence obtained provides a reasonable basis for our findings and recommendations.

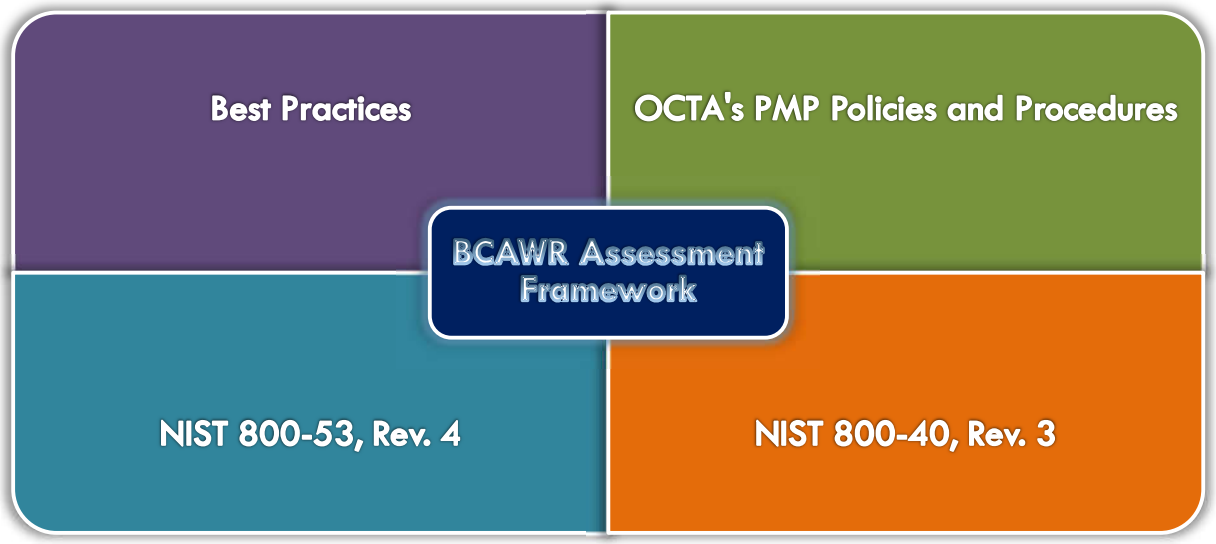
METHODOLOGY

This section contains the methodology used to assess OCTA's PMP based on the scope and objectives of this audit:

AUDIT STEPS	TESTING METHODOLOGY
Reviews and Observations	We requested and reviewed all relevant and existing PMP documentation. We observed, where possible, activities related to the PMP operations and overall management process.
Inquiries and Meetings	We made inquiries of management and corroborated responses with appropriate operations personnel. We also conducted inquiries of personnel responsible for carrying out distinct aspects of the PMP and corroborated responses with other personnel and documentation. Our inquiries included interviews and meetings with OCTA's PMP key stakeholders.
Examinations and Walk-Throughs	We inspected PMP documents and other related documentation to determine the adequacy and appropriateness of OCTA's PMP. We also determined whether the PMP development process was conducted in accordance with specific control policies and procedures, and any established industry standards. Our examination process involved reviewing and analyzing the PMP and related documents.
Substantive Testing	We conducted substantive testing of OCTA's PMP, where appropriate.

CRITERIA

To guide our audit and to adequately assess OCTA's PMP, our criterion was based on the requirements outlined in the agreement between OCTA and BCAWR, industry "Best Practices", and the relevant NIST Special Publications. BCAWR used these criteria as the framework for the development of our audit methodology, findings and recommendations. The audit was conducted in accordance with Generally Acceptable Government Auditing Standards. Below is a pictorial representation of the criteria used.


Best Practices
OCTA's PMP Policies and Procedures
BCAWR Assessment Framework
NIST 800-53, Rev. 4
NIST 800-40, Rev. 3

The remainder of this page is intentionally left blank.

DETAILED AUDIT RESULTS

OCTA's Information Systems Department has developed a PMP, supported by a Patch Management Policy that focuses on the Windows operating system environment. Management's strategy was to focus first on OCTA's highest risk area, the Microsoft Windows environment, and then expand the program to address other risk areas. The findings and recommendations described below, if implemented, would cause OCTA to leverage their success in the Windows environment across all platforms and systems.

Finding No. 1: OCTA's Patch Management Policy and Program should be expanded

To reduce the risk of security breaches, OCTA should expand the PMP to address all other operating systems software, hardware, and peripherals, and to incorporate all devices; including firewalls, Linux and Mac Operating systems, IoT devices, 3rd party devices, applications that communicate with the network, and other technology-based devices (e.g. field fuel stations).

Recommendation 1:

We recommend OCTA expand the PMP to address all software, hardware, peripherals, and devices; including firewalls, Linux and Mac Operating systems, IoT devices, 3rd party devices, applications that communicate with the network, and other technology-based devices.

Management Response:

Management agrees with the recommendation to expand the patch management program. The Information Systems (IS) Department will identify and develop a plan to comply with the recommendations that will focus on security and core infrastructure and applications first, and then continue to address all other areas. The additional resource as recommended in Finding #2, will play a critical role in this process.

Finding No. 2: OCTA should formalize plans to address patch vulnerabilities

Through regular scanning, OCTA identifies a high number of critical and severe vulnerabilities in the Windows environment. Many of the identified vulnerabilities have not been addressed and have been outstanding over 90 days. Management indicated that other operational activities, including relocation of the data center, have hampered efforts at remediating these vulnerabilities.

Recommendation 2:

We recommend that OCTA identify a dedicated operations staff person to coordinate with employees who have designated responsibility for remediating vulnerabilities. These employees should develop and document a Plan of Action with Milestones and create desktop procedures for patch management.

Management Response:

Management agrees with the recommendation to dedicate an operations staff person to coordinate with those responsible for remediating vulnerabilities and support the completion of the recommendations. The dedicated resource will document a plan of action with milestones and create desktop procedures.

Finding No. 3: Numerous workstations and servers are operating with end-of-life software and operating systems

OCTA vulnerability scans identify a number of devices with obsolete operating systems and/or software. Allowing these unsupported system components makes the network more vulnerable to attack and renders the system less reliable.

Recommendation 3:

We recommend that OCTA remove all obsolete operating systems and software from the network. Where operations currently require the use of obsolete software, we recommend that OCTA work with the vendors to acquire more secure software. In cases where the vendor is not able to supply more secure functionality, we recommend that OCTA develop plans to migrate to an alternative software solution and develop mitigating controls in the interim.

Management Response:

Management agrees with the recommendation to remove all obsolete Operating Systems (OS) and software from the network. This is a continuing process that will rely on cybersecurity to provide guidance to help the IS operational teams plan for the removal or upgrade of obsolete software. All obsolete OS and software that can't be removed due to business requirements will use alternative vulnerability remediation methods until removed. This process will continue the best practice of separation of duties as used in the recent removal of all Windows 7 machines.

Finding No. 4: Allowing for network workstations that are not managed by OCTA's Information System Department (ISD), and granting of local administrative access rights to users, increases exposure to the network

During our audit, we identified software on workstations that are not managed by OCTA's ISD. One department within OCTA has historically purchased and managed its own workstations.

In addition, we identified unsupported software, like iTunes, VLC player, and Wireshark (a tool used by hackers), installed on workstations. In most of the cases noted, the software was installed by users with local administrative access; which should be limited.

Recommendation 4:

We recommend that OCTA restrict users from installing unauthorized software and that the ISD be authorized to manage all OCTA workstations. Also, management should strictly enforce policies against installing unauthorized software on workstations. Any workstation that requires local administrative rights should be closely monitored by ISD.

Management Response:

Management agrees with the recommendation to restrict users from installing unauthorized software and that IS be authorized to manage all OCTA workstations. IS will continue to scan for new devices and software on the network. IS is aware of and in the process of taking back the management of found devices that are not IS managed, to include non-IS administrative accounts that will no longer be needed.

Finding No. 5: Patch testing should be strengthened and formalized

Use of formalized test scripts helps ensure system functionality after implementation of a patch, and is part of a mature patch management program.

As new patches are introduced, testing of basic functions is performed; however, formalized test scripts should be developed and implemented for each of the mission critical systems. Formalized test scripts identify critical functions of the particular system and provide a guide for testing after implementing a patch.

Recommendation 5:

We recommend that patch management test scripts be developed through collaboration between ISD and users of the mission critical systems. These scripts should mirror those used in the change management process.

Management Response:

Management agrees with the recommendation that patch management test scripts be developed for mission critical systems. IS and system/application owners will develop test scripts to follow the IS patching schedule for critical systems as defined in the Continuity of Operations Plan. As this is a continuous process, IS will implement and maintain the process for all defined systems.

February 18, 2020

BCA Watson Rice, LLP