Memorandum from the Office of the Inspector General

August 20, 2020

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2020-15717 – MANAGEMENT OF MAC® DESKTOPS AND LAPTOPS

As part of our annual audit plan, we audited the Tennessee Valley Authority's (TVA) management of Mac® desktops and laptops. Our objective was to determine if Mac® desktop and laptop patching and configuration management followed TVA policy. Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. Configuration management increases the security of individual computers, protects them from threats, and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties. We reviewed TVA's inventory of Mac® desktops and laptops and performed process walkthroughs of system inventory, patch management, and configuration management processes.

In summary, we found (1) TVA is at potential risk for compromise of Mac® desktops and laptops due to inaccurate inventory, (2) TVA was not patching Mac® systems in the designated time frames in TVA policy, and (3) TVA did not have a Mac® baseline as required by TVA policy. Specifics of the identified issues were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on May 19, 2020.

We recommend the Vice President and Chief Information Officer, Information Technology (IT):

1. Update Mac® device inventory for completeness and accuracy.

2. Patch Mac® devices to the latest macOS®[1] version or document and implement mitigation plans.

3. Establish and implement system baselines for Mac® desktops and laptops.

TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

[1] macOS® is the operating system used by Mac® desktops and laptops created by Apple Inc.

BACKGROUND

Patch management has been an area of concern in previous audits. In our 2014 FISMA audit,[2] we found patching timeliness for Security Patch Evaluation and Rating (SPEAR) alerts[3] were not tracked appropriately. In our 2016 FISMA audit,[4] we were unable to test the patch management process because it had not been fully implemented. In our 2016 audit[5] on cyber security patch management of high-risk desktops and laptops, the process used to manage Mac® desktops and laptops was not formally documented.

The National Institute of Science and Technology (NIST) states that "patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they mitigate software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation."[6]

Configuration management increases the security of individual computers, protects them from threats, and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties.[6] NIST states that "effective and well-tested security configurations mean that less time and money is spent eradicating malware, restoring systems from backups, and reinstalling operating systems and applications."[7]

According to the IT system of record for inventory, TVA has 200 Mac® desktops and laptops in use. TVA policy states that IT operates an asset management program to merge the physical, financial, and contractual functions required for the purchase and use of IT hardware. The IT Asset Administrator is responsible for keeping the IT system of record for inventory. Mac® desktops and laptops are managed through an enterprise management platform that controls device settings. This includes the configurations and settings related to patching the macOS® running on the desktop or laptop.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if Mac® desktop and laptop patching and configuration management followed TVA policy. The scope of this audit was limited to systems running macOS® that are managed by TVA's IT organization. Fieldwork was performed between March 2020 and May 2020.

[2] Audit Report 2014-15059, *Federal Information Security Management Act Evaluation*, January 13, 2015.

[3] SPEAR is a process TVA uses to evaluate and categorize security patches before installation.

[4] Audit Report 2016-15407, *Federal Information Security Management Act*, January 11, 2017.

[5] Audit Report 2016-15369, *Cyber Security Patch Management of High-Risk Desktops and Laptops*, July 19, 2017.

[6] Murugiah Souppaya and Karen Scarfone, "Guide to Enterprise Patch Management Technologies," *NIST Special Publication 800-40,* Revision 3, July 2013, page iii, <http://dx.doi.org/10.6028/NIST.SP.800-40r3>, accessed on June 1, 2020.

[7] Lee Badger, Murugiah Souppaya, Mark Trapnell, Eric Trapnell, Dylan Yaga, Karen Scarfone, "Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist", *NIST Special Publication 800-179,* December 2016, page 3, <https://doi.org/10.6028/NIST.SP.800-179>, accessed on March 27, 2020.

To achieve our objective, we:

- Obtained and reviewed TVA Standard Programs and Processes (SPP), IT policies, procedures, and work instructions (WI) including:
  - TVA-SPP-12.004, *TVA Cybersecurity Patch and Vulnerability Management Program.*
  - TVA-SPP-12.704, *Security Configuration Benchmark Standards.*
  - IT-SPP-09.003, *Configuration Settings Management.*
  - IT-WI-12.346, *Apple® and Mobile Device Patch Management.*
- Interviewed IT personnel and performed process walkthroughs to identify and obtain information on TVA's controls for management of Mac® desktops and laptops.
- Identified and tested controls in place related to inventory, patch management, and configuration management.
- Reviewed data from the system of record for inventory and reconciled it against the enterprise management platform.
- Reviewed macOS® versions in use against vendor patch release dates.
- Reviewed TVA's policies for patch and configuration management and compared them against TVA's practices to determine if policy was being followed.

Inventory, patch, and configuration management were identified as internal controls that were significant to our audit objective. As such they were included in our audit plan for testing. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

FINDINGS

We found (1) TVA is at potential risk for compromise of Mac® desktops and laptops due to inaccurate inventory, (2) TVA was not patching Mac® systems in the designated time frames in TVA policy, and (3) TVA did not have a Mac® baseline as required by policy.

TVA AT POTENTIAL RISK FOR COMPROMISE OF MAC® DESKTOPS AND LAPTOPS DUE TO INACCURATE INVENTORY

We reconciled the macOS® inventory listing from IT's enterprise management platform with the IT system of record for inventory and determined 164 devices from IT's enterprise management platform were in use. However, 5 of the 164 devices were not listed in the IT system of record for inventory. An incomplete inventory of Mac® desktops and laptops increases the risk of internal controls being improperly applied.

In addition, we found 37 of 200 devices in the IT system of record for inventory were not in the enterprise management platform. Therefore, for these 37 devices, we were unable to determine (1) the macOS® version running and (2) if patching was up to date. Further, according to TVA personnel, if a device is not procured through TVA supply chain processes and is not enrolled into the enterprise management platform, TVA IT cannot manage the configuration on those devices.

MAC® PATCHING NOT COMPLETED WITHIN DESIGNATED TIMEFRAMES

We found patches were not applied in the time frame required by policy, leaving systems in an operational status with unpatched vulnerabilities. In addition, TVA had no documented mitigation plans or business justifications to address older macOS® versions that were not patched.

TVA-SPP-12.004, *TVA Cybersecurity Patch and Vulnerability Management Program*, requires that internal nonhigh value asset[8] devices have critical vulnerabilities patched in 60 days, high impact vulnerabilities patched in 90 days, and moderate and low impact vulnerabilities are patched 'as available.' We found 140 out of 164 Mac® desktops and laptops did not meet the patching time frame found in TVA-SPP-12.004. IT-WI-12.346, *Apple and Mobile Device Patch Management,* requires high impact vulnerabilities to be patched in 7 days, moderate vulnerabilities in 30 days and low impact vulnerabilities 'as appropriate.' We found 163 out of 164 Mac® desktops and laptops did not meet the patching time frame found in IT-WI-12.346.

Further, TVA-SPP-12.004 requires a documented mitigation plan where patches cannot be applied. TVA had no mitigation plans for unpatched macOS® versions. IT-WI-12.346 requires documented business justifications for systems that cannot be patched, and we found TVA had not documented business justifications for unpatched macOS® versions.

TVA policy states that vulnerability management works to reduce or eliminate cyber vulnerabilities through patching or implementation of other remediation recommendations. Therefore by not applying timely patches or implementing mitigation plans, assets such as Mac® desktops and laptops are left vulnerable to cyberattack.

Specifics of the identified vulnerabilities were omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on May 19, 2020.

CONFIGURATION BASELINES NOT ESTABLISHED FOR MAC® DEVICES

We reviewed documentation and inquired with TVA management to determine if a macOS® standard configuration baseline existed in accordance to TVA's security configuration policies, TVA-SPP-12.704, *Security Configuration Benchmark Standards*, and IT-SPP-09.003, *Configuration Settings Management*. Both policies call for baselines to be established based off of national standards. We found TVA had not established a

[8] High value assets are "Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people."

standard baseline.[9] TVA policy states that the use of standardized baselines for Mac® desktop and laptops would provide a more secure infrastructure for IT that minimizes risks and reduces vulnerabilities, attacks, and malware.

RECOMMENDATIONS

We recommend the Vice President and Chief Information Officer, IT:

1. Update Mac® device inventory for completeness and accuracy.

2. Patch Mac® devices to the latest macOS® version or document and implement mitigation plans.

3. Establish and implement system baselines for Mac® desktops and laptops.

TVA Management's Comments – TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

- - - - - -

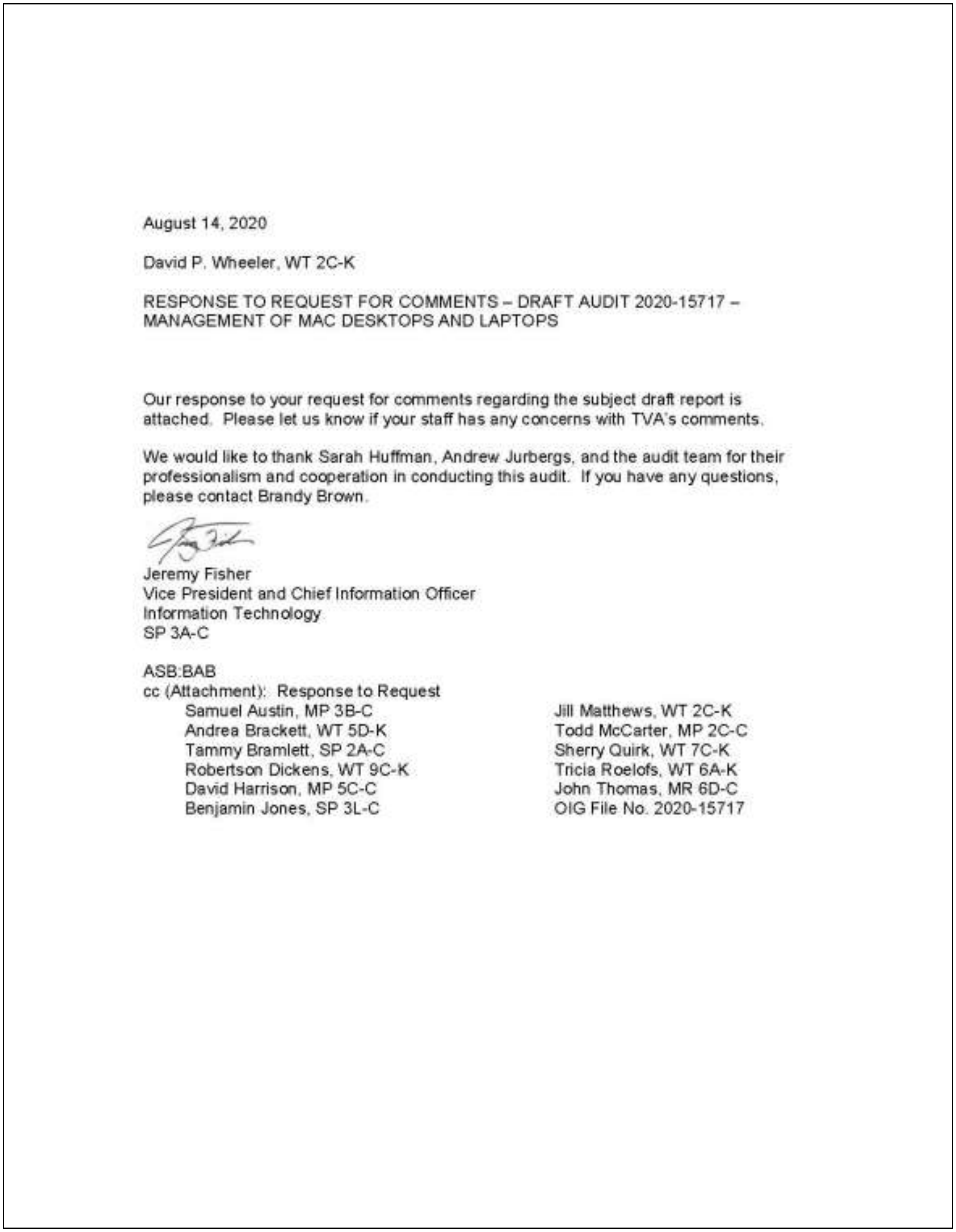
This report is for your review and management decision. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Andrew J. Jurbergs, Senior Auditor, at (865) 633-7393 or Sarah E. Huffman, Director, IT Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

AJJ:KDS
cc: TVA Board of Directors
Samuel A. Austin
Andrea S. Brackett
Jeffery J. Lyash
Justin C. Maierhofer
Jill M. Matthews
Todd E. McCarter
Sherry A. Quirk
John M. Thomas III
OIG File No. 2020-15717

[9] A baseline is a documented set of specifications for a system that has been formally reviewed and agreed upon.



August 14, 2020

David P. Wheeler, WT 2C-K

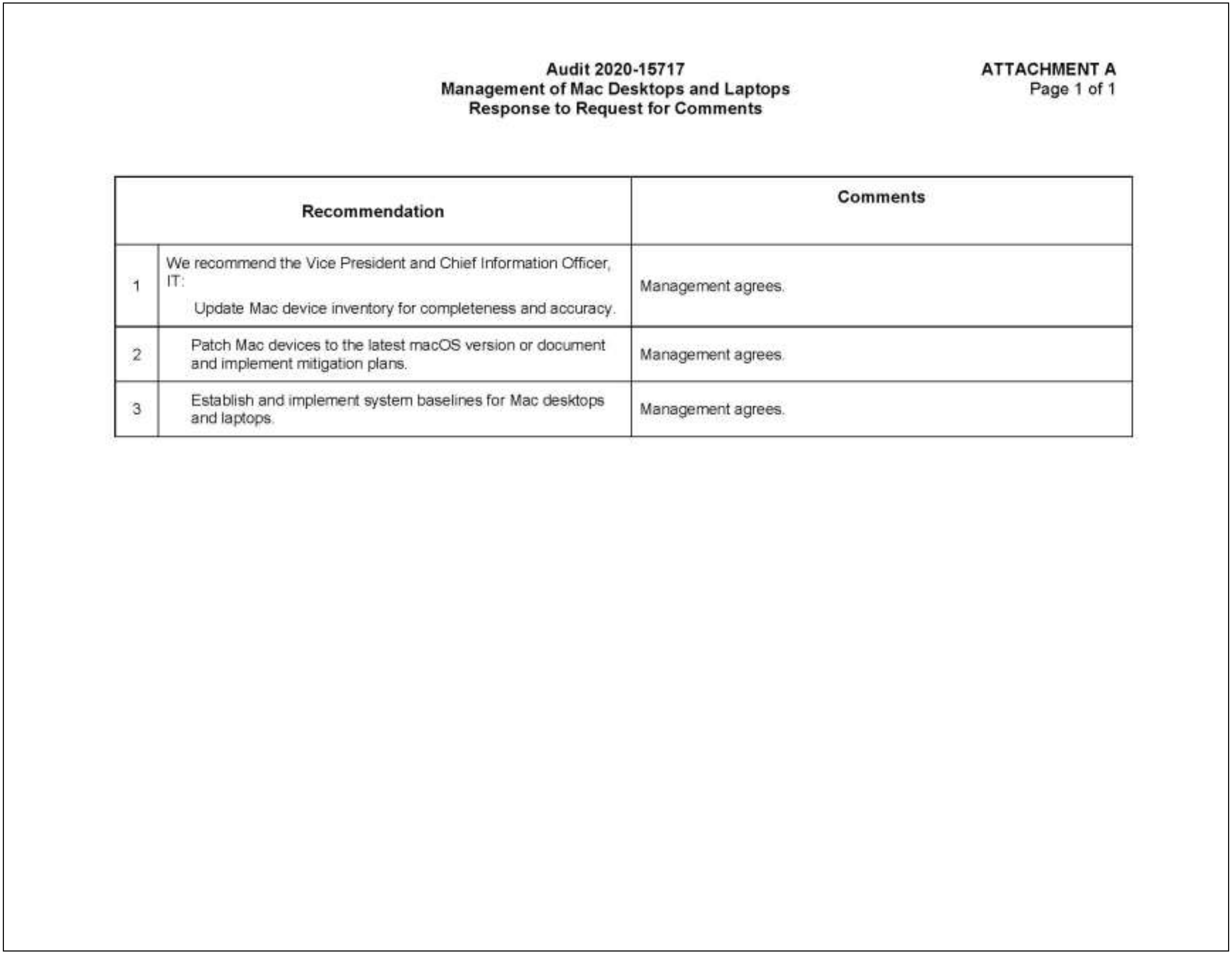
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2020-15717 – MANAGEMENT OF MAC DESKTOPS AND LAPTOPS

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Andrew Jurbergs, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brandy Brown.

Jeremy Fisher
Vice President and Chief Information Officer
Information Technology
SP 3A-C

ASB:BAB
cc (Attachment): Response to Request
Samuel Austin, MP 3B-C
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
Jill Matthews, WT 2C-K
Todd McCarter, MP 2C-C
Sherry Quirk, WT 7C-K
Tricia Roelofs, WT 6A-K
John Thomas, MR 6D-C
OIG File No. 2020-15717



Audit 2020-15717
Management of Mac Desktops and Laptops
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	We recommend the Vice President and Chief Information Officer, IT: Update Mac device inventory for completeness and accuracy.	Management agrees.
2	Patch Mac devices to the latest macOS version or document and implement mitigation plans.	Management agrees.
3	Establish and implement system baselines for Mac desktops and laptops.	Management agrees.