# Montgomery County, Maryland
# Office of the County Executive
# Office of Internal Audit

## Patch Management and Threat Detection Review

**January 30, 2026**

MCIA-26-1

# Highlights

## Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an audit of the Montgomery County Government's (County) Department of Technology and Enterprise Business Solutions (TEBS) focusing on Patch Management and Threat Detection.

MCIA performed this review to determine whether the County's processes for detecting cyber threats and applying system patches are operating effectively to protect critical data and technology assets. Strong threat detection and timely patching are essential to reduce vulnerabilities, prevent service disruptions, and safeguard information that supports County operations and public services.

TEBS is responsible for implementing and overseeing these activities across the County's information systems. By monitoring security events and maintaining current patch levels on endpoint devices and other technology assets, TEBS helps ensure the confidentiality, integrity, and availability of County data for residents, businesses, and the public.

The audit evaluated the design and effectiveness of the County's threat detection and patch management program, including its ability to identify and respond to cyber risks, analyze and correlate security events, and maintain compliance with industry standards and regulatory requirements. It also assessed whether existing controls sufficiently mitigate risks and whether gaps or vulnerabilities exist in the patching process.

This review was conducted by the accounting firm SC&H Group, Inc., under contract with MCIA.

**January 2026**

## Patch Management and Threat Detection Audit

## Technology and Enterprise Business Solutions (TEBS)

## What MCIA Found

TEBS units responsible for managing the County's threat detection and patch management processes have established internal controls to reduce cybersecurity risks. These controls support the protection of County systems, data, and technology assets.

However, opportunities exist to enhance the design and operational effectiveness of these controls to more effectively mitigate risks.

MCIA identified 5 areas where improvements would strengthen TEBS's processes and controls:

1. Administrator Activity Review
2. Firewall Rule Reviews
3. Device Enrollment
4. Vulnerability Management Plan Review
5. Legacy Server Patching

## *TABLE OF CONTENTS*

# Objectives

This report summarizes the results of an audit of Montgomery County Government's (County) patch management and threat management program (collectively, review). The audit was performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

The audit's objectives were to:

1. Assess an organization's ability to identify potential cyber threats by evaluating the effectiveness of their threat detection systems, processes, and procedures
2. Analyze the processes for collecting, analyzing, and correlating security events to identify potential malicious activity.
3. Assess areas where existing security controls may not be sufficient to detect potential threats.
4. Verify adherence to relevant industry regulations and compliance standards related to threat detection and incident response.
5. Assess the organization's patch management program to identify gaps and vulnerabilities in patching processes, and to improve patching processes.

# Background

## County-wide Information Technology Overview

The County manages hardware, software, and technology through both centralized and decentralized functions to support employees in delivering services efficiently and securely.

Technology and Enterprise Business Solutions (TEBS) provides county-wide IT support, including helpdesk services, IT asset management, data governance, information security, and access management for Active Directory (AD) and Oracle Enterprise Resource Planning (ERP).

## Patch Management and Threat Detection

Patch management responsibilities are distributed across three coordinated groups within TEBS:

- **Threat Detection Team:** In partnership with a vendor, the outsourced Security Operations Center (SOC), this team continuously monitors County information systems. They scan the environment 24/7, identify vulnerabilities, and issue patch recommendations.
- **Endpoint Patch Management Team:** Reviews alerts from the Threat Detection Team along with vendor advisories to evaluate endpoint vulnerabilities. They determine, test, and deploy patches for County workstations, laptops, and other endpoint devices.
- **Server Patch Management Team:** Performs the same functions for the County's server infrastructure, applying operating system and application patches to mitigate risks.

Together, these teams form the backbone of the County's patch management program. The process relies on continuous monitoring, coordination across functions, and timely deployment of vendor and internally recommended patches. This structure is critical for reducing security risks, maintaining system reliability, and ensuring compliance with cybersecurity standards.

Threat Detection Team

The Threat Detection Team is responsible for continuous monitoring of the County's IT environment and identifying vulnerabilities across systems and devices. The team operates within defined security policy levels (AP 6–7) and uses specific tools to scan endpoints, servers, and additional infrastructure such as printers and network devices. Findings are integrated into a tool to support risk prioritization, and results are shared through dashboards that provide departments with visibility into vulnerabilities and patch status.

To support detection and response, the team utilizes a layered toolset. Tools provide endpoint detection and response, capture firewall activity, and enable URL filtering. Remote access activity is monitored through a tool, which receives and logs VPN events. A tool is used for ticketing and remediation workflows, and device-blocking capabilities are available when threats are detected. These tools work together to provide comprehensive coverage and ensure vulnerabilities are addressed quickly.

In addition to daily monitoring, the team coordinates annual penetration testing for external-facing systems and performs ad hoc reviews to assess emerging risks. They also contribute to regional and national security collaboration by sharing intelligence with organizations such as MS ISAC, MD ISAC, and the Council of Governments (COG). Supplemental documentation, including incident response procedures and network diagrams, ensures structured and repeatable processes are in place. Through these capabilities, the Threat Detection Team provides 24/7 oversight of the County's IT environment and delivers actionable intelligence to support patching and remediation efforts.

Endpoint Patch Management Team

The Endpoint Patch Management (EM) Team is responsible for patching and maintaining end-user devices across the County. Their scope includes all computers managed at the Active Directory department or computer directory level, covering nearly all County staff devices, with the exception of Public Safety Data System endpoints, the MC311 call center, and other non-MCGOV domain endpoints. In addition to device management, the team proactively manages enterprise applications and major browsers across the County environment.

As of September 22, 2025, the team manages approximately 10,375 PCs, 20 Mac devices, 790 iOS/iPads, 17 Android devices (including conference room telecom equipment), and 6,430 mobile devices through a tool. This broad coverage ensures that the County's distributed workforce remains up to date with required security patches and enterprise application updates.

The EM Team employs a comprehensive toolset to support patching and monitoring activities. These tools allow for patch deployment, compliance tracking, vulnerability reporting, and customized application deployments for County departments. The team's responsibilities also include incident ticket management, ongoing maintenance of patching tools and policies, vulnerability analysis, and processing departmental requests for specialized deployments.

By combining centralized patching tools, proactive vulnerability monitoring, and enterprise-wide application management, the Endpoint Patch Management Team plays a critical role in maintaining a secure endpoint environment. Their work reduces device-level risks and ensures the County's IT infrastructure remains protected against evolving cyber threats.

Server Patch Management Team

The DevOps and Server Support Team is responsible for maintaining the County's core server infrastructure and ensuring secure and reliable operations. Their scope covers patching and

maintenance of approximately 750 Windows and Linux systems, management of 10 Nutanix clusters hosting more than 600 virtual machines, and oversight of 100+ resources in a tool. In addition to patching, the team supports critical enterprise services such as Single Sign-On (SSO), SQL and Oracle databases, Red Hat Linux deployments, antivirus enablement, SSL certificate lifecycle management, application deployments, and domain renewals. These responsibilities make the team central to the County's ability to provide secure IT services to staff and citizens.

To support these functions, the team leverages multiple tools and processes. A tool serves as the primary platform for patch management, streamlining what was previously a manual process. Another tool is used as the inventory database for tracking servers and related devices, ensuring accurate visibility into the environment. Patch approvals are coordinated and documented through email communication, while a dedicated QA server provides a space for patch testing prior to deployment, though results are not always formally documented. The team also employs Power BI dashboards to monitor vulnerabilities, track remediation status, and provide leadership with visibility into security posture.

Through these capabilities, the Server Support Team plays a pivotal role in the County's patch management program. Their ability to coordinate with the Threat Detection and Endpoint teams allows for timely remediation of vulnerabilities, reducing exposure to security risks. By managing both on-premises and cloud infrastructure, while maintaining critical identity, database, and application services, the team ensures the County's IT environment remains resilient, compliant, and aligned with cybersecurity best practices.

# Scope and Methodology and Approach

## Scope

The audit was performed in accordance with the Statement on Standards for Consulting Services (SSCS) issued by the American Institute of Certified Public Accountants (AICPA). In addition, the NIST Special Publication (SP) 800-53 IT governance framework was used to supplement the review over patch management and threat management practices.

The audit was conducted from April 2025 through October 2025 and focused on assessing the current state of implementation and effectiveness of the County's patch management and threat management programs. These programs are managed and overseen by the County's Department of Technology and Enterprise Business Solutions (TEBS), which is responsible for identifying, testing, and deploying software patches, as well as monitoring for potential cyber threats and vulnerabilities.

The scope focused on the following:

1. **Threat Detection and Management**
   a) Monitoring and analysis of system activity, logs, and alerts for potential threats.
   b) Evaluation of controls designed to detect and respond to emerging threats.
   c) Identification and prioritization of vulnerabilities and risks based on criticality.
   d) Review of processes for correlating and analyzing security events to identify malicious activity.
   e) Verification of adherence to industry regulations and compliance standards.

2. **Patch Management**
   a) Processes for identifying, testing, and deploying software patches across County systems.
   b) Evaluation of gaps or vulnerabilities in patch management practices.
   c) Assessment of whether patching ensures security, compliance, and system performance.
   d) For endpoint patch management, the review was limited to the Montgomery County Government (MCGMD.gov) domain, which is managed by TEBS and included in scope. Two additional domains, the Public Safety Sector and the Library, were considered out of scope. The MCGMD.gov domain is the primary domain used to administer endpoint devices across the County and therefore represents the majority of endpoint operations reviewed.

## Methodology and Approach

The review was conducted using a three-phased approach:

1. Phase 1: Planning
2. Phase 2: Fieldwork
3. Phase 3: Reporting

### Phase 1: Planning

Planning consisted of gaining an understanding of the threat detection and patch management process, as well as preliminary review of process specific policies, procedures, and documentation and performance of observation walkthroughs.

#### Process Understanding

SC&H performed the following procedures to gain an understanding of the County's threat detection and patch management processes for endpoints and servers, as well as the associated risks and controls:

1. Conducted interviews and walkthroughs with personnel responsible for threat detection, endpoint patch management, and server patch management to document current processes, practices, and team responsibilities.
2. Obtained preliminary documentation, including policies and procedures governing the threat detection and patch management processes.
3. Observed the systems and tools in use to support threat detection and patch management activities.

#### Creation of Audit Program

Based on the procedures performed during the planning phase, SC&H developed an audit program with steps to address the objectives, which was reviewed and approved by the MCIA Manager prior to implementation.

### Phase 2: Fieldwork

Fieldwork consisted of testing the design and operating effectiveness of internal controls identified during process understanding, and evaluating alignment and compliance with related policies, procedures, and governance requirements.

Based on the risk assessment and process walkthroughs performed during planning, SC&H identified three functional teams responsible for patch management and threat detection: Threat Detection, Endpoint Patch Management, and Server Patch Management. SC&H conducted interviews and walkthroughs with these teams to document processes, clarify responsibilities, and confirm how practices align with County policies and requirements.

Sample Selection
SC&H judgmentally selected samples to validate patching and monitoring activities. These samples included:

- Endpoint and server patch deployment records.
- Threat detection system logs.
- Vulnerability scan results.
- Firewall rule configurations.
- Privileged user activity related to security systems.

Sample selection was designed to provide coverage across operating systems, devices, and security tools most critical to County operations.

Internal Controls Testing
SC&H performed inquiry, observation, and sample based internal control testing to evaluate policies, procedures, and controls related to:

1. Identification and prioritization of vulnerabilities.
2. Patch testing, approval, and deployment processes.
3. Monitoring of endpoint and server compliance.
4. Logging and monitoring of security events.
5. Access and activity of privileged users within threat detection systems.
6. Firewall and network device configuration management.

Compliance Testing
SC&H performed test procedures to evaluate compliance with County policies, TEBS procedures, and NIST SP 800-53 Rev. 5 control requirements governing patch management and threat detection activities.

Validation
Preliminary test results were compiled, discussed and agreed upon with the responsible TEBS teams and presented to the MCIA Manager for confirmation and validation of factual accuracy.

# Findings and Recommendations

The following five categories of findings and related recommendations represent the key observations identified during the audit. These recommendations are intended to strengthen and enhance the County's threat detection capabilities and patch management practices. Findings are presented from the perspective of the team responsible: Threat Detection, Endpoint Patch Management, and Server Patch Management.

Due to the sensitive nature of the detailed results, certain information has not been included in this public report. Specific findings and recommendations have been communicated directly to each team within TEBS. Each responsible team is required to develop corrective action plans to address the recommendations in a timely and complete manner. The summary-level findings are outlined below without attribution to sensitive system details.

Implementation of these recommendations will strengthen the County's ability to mitigate cybersecurity risks, improve operational resilience, and maintain compliance with leading industry standards.

## Threat Detection:

| Finding 1: Lack of Review of Administrator Activity across two systems. |
|---|
| **Finding**<br>Review of logged administrator activity was not defined across two sampled systems, limiting accountability for privileged actions.<br><br>**Risk**<br>Without review of administrator activity, inappropriate or unauthorized actions could occur without detection. This increases the risk of accidental system misconfigurations, malicious insider activity, or compromised privileged accounts leading to unauthorized changes or data breaches.<br><br>**Recommendation**<br>TEBS should implement a formal process for reviewing administrator activity across the two systems as well as document and retain the results of the review. |

| Finding 2: Firewall Rule Review Documentation |
|---|
| **Finding**<br>Review of firewall rules and actions taken as part of the review are not consistently and formally documented.<br><br>**Risk**<br>Without formal documentation of firewall rule reviews and related actions, there is a risk of incomplete follow-up on security issues, lack of accountability, and reduced ability to provide evidence of control effectiveness. This could result in outdated or unnecessary firewall rules remaining in place, increasing the County's exposure to unauthorized access or other security vulnerabilities.<br><br>**Recommendation**<br>TEBS should establish a formal process to record and document completion of periodic firewall reviews, including actions taken and approvals. |

## Endpoint Patch Management:

| Finding 3: Device Not Initially Enrolled in an IT management tool |
|---|
| **Finding**<br>One sampled device was not initially enrolled in the County's patch management system, though enrollment of the identified device was promptly resolved through automated procedures prior to deployment.<br><br>**Risk**<br>Devices not enrolled in the IT management tool may be excluded from patch deployment and compliance monitoring. This increases the risk of missed patches, unaddressed vulnerabilities, and reduced visibility over the County's endpoint environment. Even a single unmanaged device could present an entry point for attackers or introduce compliance gaps.<br><br>**Recommendation**<br>TEBS should perform regular reconciliations to ensure all active devices are properly enrolled in patch management and documented. |

**Server Patch Management:**

| Finding 4: Server Vulnerability Management Plan Not Reviewed |
| --- |
| **Finding**<br>The Server Vulnerability Management Plan was not reviewed in accordance with annual requirements.<br><br>**Risk**<br>Failure to periodically review and update the Server Vulnerability Management Plan may result in outdated procedures or overlooked vulnerabilities. This increases the risk that critical systems are not adequately protected against emerging threats, and it may also limit the County's ability to demonstrate compliance with internal policies and industry standards.<br><br>**Recommendation**<br>TEBS should establish and enforce a recurring review cycle for the plan, with documentation and management approval of updates. |

| Finding 5: Unpatched AccessMCG and Certain Servers |
| --- |
| **Finding**<br>A sample of legacy servers were identified as unpatched due to system limitations or lack of vendor support. Migration to supported platforms is currently in process.<br><br>**Risk**<br>Unpatched or unsupported servers increase the risk of security vulnerabilities being exploited by attackers. This may lead to service disruption, unauthorized access, or compromise of sensitive systems and data. Extended reliance on legacy or unsupported platforms also makes it more difficult to maintain compliance with cybersecurity standards and industry best practices.<br><br>**Recommendation**<br>TEBS should continue prioritizing migration of unsupported servers, while maintaining interim controls until the process is complete. |

# Comments and MCIA Evaluation

The draft report was shared with TEBS for review and comment. TEBS stated that they had no formal comments, and that they would address the findings and process recommendations identified in the report. MCIA did not make any changes to the draft report.

# APPENDIX A – Department Comments


**DEPARTMENT OF TECHNOLOGY AND ENTERPRISE BUSINESS SOLUTIONS**

*Marc Elrich*
*County Executive*

*Gail M. Roper*
*Chief Information Officer/Director*

**MEMORANDUM**

January 20, 2026

TO: Michele El-Gamil, Internal Audit Manager
Office of the County Executive

FROM: Gail M. Roper, CIO/Director *Gail M. Roper*
Department of Technology and Enterprise Business Solutions

SUBJECT: TEBS Formal Comments—Internal Audit

Thank you for sharing the Draft Final Report and Internal Management Advisory Letter (IMAL) on Patch Management and Threat Detection. We appreciate the time and effort invested by the Internal Audit team throughout this review process and the opportunity to provide our formal management response.

After careful review, the department acknowledges the findings as outlined in the report. Based on our assessment, we believe that the identified issues can be effectively remediated through the implementation of periodic system reviews, enhanced documentation review processes, and completion of ongoing projects. These measures will help ensure ongoing compliance and reinforce existing controls.

We appreciate the collaborative approach taken during this audit and look forward to continued partnership in strengthening our patch management and threat detection environment.

**Office of the CIO**
101 Monroe Street, 13th Floor, Rockville, Maryland 20850
240 777-2900 FAX 240 777-2831