Agenda Item No: 16.A

STAFF REPORT

Report To: Board of Supervisors **Meeting Date:** October 6, 2022

Staff Contact: Sheri Russell, Chief Financial Officer

Agenda Title: For Possible Action: Discussion and possible action regarding recommendations of the Carson City Audit Committee to approve the completed remediation plans and remove findings from the Audit Findings Tracking Summary Report. (Sheri Russell, srussell@carson.org)

Staff Summary: The completed remediation plans for various recommendations and findings have been presented and approved by the Audit Committee. Upon approval by the Board of Supervisors, the completed recommendations and findings will be considered closed and removed from the Audit Findings Tracking Summary Report maintained by the internal auditor and City staff.

Agenda Action: Formal Action / Motion **Time Requested:** 10 minutes

---

Proposed Motion
I move to approve the Audit Committee's recommendation as presented.

Board's Strategic Goal
Efficient Government

Previous Action
N/A

Background/Issues & Analysis
Eide Bailly has been contracted by Carson City to provide internal auditor services starting July 1, 2022 through June 30, 2025.

Staff has addressed the recommendations and/or findings contained in the Audit Findings Tracking Summary Report with remediation plans. The internal auditor has validated remediation as requested, and the Audit Committee is recommending closure of the following findings:

- IT Vulnerability Audit - All items are recommended for closure. An updated findings report has any uncorrected errors included.
- Social Media - All items are recommended for closure.
- Community Development - Item #8 is recommended for closure.
- Wireless Assessment - All Items are recommended for closure.
- End Point User Internal Audit - All Items are recommended for closure.

Applicable Statute, Code, Policy, Rule or Regulation
N/A

Financial Information
Is there a fiscal impact? No

If yes, account name/number: N/A

Is it currently budgeted? No

Explanation of Fiscal Impact: N/A

Alternatives
Do not accept the recommendation and/or provide alternative direction to staff.

Attachments:
Audit Findings Summary 9-7-2022.pdf

Carson City Wireless Assessment 2022 - Obfuscated Report.docx

Board Action Taken:

Motion: _____	1) _____	Aye/Nay
	2) _____	_____
		_____
		_____
		_____
		_____

_____
(Vote Recorded By)

Carson City
Internal Audit Summary
Updated - 9/14/2022

Carson City - Audit Findings Tracking Summary Report (revised 9/14/2022)

Report Name	Report Submittal	AC/BOS Report Approval	Reporting Entity	Report Findings	Completed Findings	AC Approval	BOS Approval	Notes
Payroll Internal Controls Testing	7/27/2016	12/21/2017	Internal Auditor	2	2	8/8/2016	11/15/2018	
P-card Internal Controls Testing	7/27/2016	12/21/2017	Internal Auditor	2	2	8/8/2016	11/15/2018	
Small Works Projects Review	2/17/2017	12/21/2017	Internal Auditor	4	4	2/14/2017	12/21/2017	
Public Guardian Review	5/1/2017	12/21/2017	Internal Auditor	13	13	5/9/2017	11/15/2018	
Purchasing and AP Internal Controls Testing	7/6/2017	12/21/2017	Internal Auditor	12	12	7/12/2017	11/15/2018	
HTE Access Controls Testing	9/26/2017	12/21/2017	Internal Auditor	7	7	10/3/2017	12/21/2017	
FY 2014 CAFR	12/18/2014	12/18/2014	External Auditor	5	5	3/22/2016	12/18/2014	
FY 2015 CAFR	12/17/2015	12/17/2015	External Auditor	5	5	3/22/2016	12/17/2015	
Capital Projects Process Review	5/3/2018	8/20/2020	Internal Auditor	8	8	6/15/2020	8/20/2020	
Grants Audit	6/30/2018	9/30/2018	Internal Auditor	1	1	6/15/2020	8/20/2020	
Public Guardian Follow Up Review	5/3/2018	3/7/2019	Internal Auditor	8	8	5/10/2018	3/7/2019	
FY 2017 CAFR and Single Audit	11/30/2017	12/21/2017	External Auditor	4	4	5/10/2018	8/20/2020	
FY 2018 CAFR and Single Audit	12/6/2018	12/6/2019	External Auditor	3	3	6/15/2020	8/20/2020	
Temporary Staffing Audit	5/9/2019	5/6/2019	Internal Auditor	5	5	6/22/2021	10/3/2019	
Fire Department Overtime Audit	5/9/2019	10/3/2019	Internal Auditor	2	2	5/9/2019	10/3/2019	
FY2019 CAFR and Single Audit	12/5/2019	12/5/2019	External Auditor	1	1	6/15/2020	8/20/2020	
Cash Handling 2019	12/3/2019	1/6/2020	Internal Auditor	20	20	6/22/2021	8/20/2020	
Social Media Study	11/25/2019	1/6/2020	Internal Auditor	13	13	6/22/2021		#13 recommended for closure
HR Administration - Eligible EE Group Ins.	12/3/2019	1/6/2020	Internal Auditor	4	4	6/15/2020	8/20/2020	
AP and P-Card Audit Program	4/1/2020	3/4/2021	Internal Auditor	4	4	8/4/2020	3/4/2021	
IT Vulnerability Audit	10/30/2020	12/8/2020	Internal Auditor	10	10	3/8/2022		All items recommended for closure
Fleet Audit	3/30/2021	3/30/2021	Internal Auditor	6	6	3/8/2022	7/7/2022	
Revenue and Receivables Audit	5/25/2021	6/22/2021	Internal Auditor	3	3	12/7/2021	7/1/2020	
Payroll Internal Controls Testing	11/22/2021	12/7/2021	Internal Auditor	3	3	3/8/2022	7/7/2022	
Community Development Department	6/29/2022		Internal Auditor	8	1	7/12/2022		#8 recommended for closure
IT Vulnerability Retest Report	7/12/2022		Internal Auditor	6	0			
Wireless Assessment (see separate report)	4/30/2022		Internal Auditor	1	1			One item immediately remediated
Endpoint Security Assessment	4/30/2022		Internal Auditor	2	2			All items recommended for closure
Prelim Risk Assess. Body Worn Camera Prog.	9/1/2022		Internal Auditor	4	0			
Total (including archived reports)				166	149			

Legend:
- Report Submittal = date report submitted to City
- BOS Report Approval = date report adopted by BOS
- Reporting Entity = organization that prepared the report
- Report Findings = number of findings in the report
- Completed Findings = number of findings completed by management
- AC Approval = Audit Committee approval of completed findings
- BOS Approval = Board of Supervisors approval of completed findings
- Notes = notes about findings

Finding Corrected?

Y	Findings Addressed - Audit Committee closed
P	Partially Addressed items
N	Not yet addressed
Y	For Discussion today

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
13		The City does not have an Information Security Response Plan	Create an Information Security Response Plan to include procedures for responding to security incidents, communication protocol and determine system impact.	*Y*	6/30/2022	6/30/2022	N	CIO will create an Information Security response Plan. **UPDATE:** Plan is complete.

Carson City
IT Vulnerability Audit
October 30, 2020

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
		NOTE: 12 Findings - External						
1		Update all systems that are currently running on outdated software: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's perimeter network.	Staff is actively working on updating outdated systems and adjusting operations to be in line with industry best practices, such as automatic updates based on how critical a system is. Some legacy systems that cannot be updated will be isolated using a combination of identity based access rules and network security zones to mitigate the risk of their ongoing operation. Some of these systems may be decommissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	*Y*	3/31/2022	6/13/2022	Y	Staff is making progress on resolving issues. IT has been updating systems on a continuous basis. Some systems will require funding to stay current, extended support has been purchased for endpoint security to protect legacy systems. Maintenance will be performed with approval from the affected department(s). **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
2		System hardening processes should be in place across all systems: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.	Most issues identified in the external test were expected. Some sites do not use encryption as they don't warrant it with their purpose, others host apps that there are very few options for replacing/updating. Staff has implemented system hardening processes on many systems and will continue to expand on those efforts. Staff is working towards robust change management procedures that could prevent a misconfiguration from occurring as a standard risk management step. Staff's current approach requires a scope of work and review by at least two employees when performing work on critical infrastructure.	*Y*	3/31/2022	6/13/2022	Y	Staff has continued to make progress on system hardening, changing default accounts and passwords and change management including the use of automated deployment tools and templates. Work is being conducted to update patch deployment systems. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
3		Web development processes: Ensure coding of website and web applications follow OWASP standards. The OWASP Top 10 is a standard awareness document for developers and web application security. Carson City should adopt this document and start the process of ensuring that their web applications minimize these risks.	External findings that would fall under OWASP guidelines are Commercial Off The Shelf (COTS) applications under which the City has little control over development. The City can add OWASP as a procurement requirement for COTS applications, however this may limit the scope and range of options for the City as a whole when considering vendors of specialized software, such as the software from which this item stems. Staff will review this recommendation and consider how to implement it.	*Y*	3/31/2022	6/13/2022	Y	Staff does not have the recommendation yet, but has begun to approach new vendors with this requirement. **Update:** Staff will work with external vendors to ensure that these standards are being followed for the Carson City websites they host. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
4		Recommend remediation scanning be performed: Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.	Carson City systems are regularly scanned and most by MS-ISAC / CIS as part of a federal program intended to harden local government systems. Most issues identified by the external audit were also identified by the MS-ISAC / CISC scanning effort and were known/expected. Staff will either remediate or document exceptions to all findings.	*Y*	3/31/2022	6/13/2022	Y	In the December 2020 Audit Committee meeting, it was decided to re-test in August 2021. This was pushed to the last quarter of FY22, as we have a new CIO. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
		NOTE: 103 Findings - Internal						
1		Update all systems that are currently running on unsupported operating systems: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's infrastructure and data.	Staff is actively working on updating outdated systems and adjusting operations to be in line with industry best practices, such as automatic updates based on how critical a system is. Some legacy systems that cannot be updated will be isolated using a combination of identity based access rules and network security zones to mitigate the risk of their ongoing operation. Some of these systems may be decommissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	*Y*	3/31/2022	6/13/2022	Y	Staff is making progress on resolving issues; **Current Status 11.24.2021**: IT has been updating systems on a continuous basis. Some systems will require funding to stay current, extended support has been purchased for endpoint security to protect legacy systems. Maintenance downtime will be performed with the approval from the affected department(s). **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**

2		Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.	Most issues identified in the external test were expected. Some sites do not use encryption as they don't warrant it with their purpose, others host apps that there are very few options for replacing/updating. Staff has implemented system hardening processes on many systems and will continue to expand on those efforts. Staff is working towards robust change management procedures that could prevent a misconfiguration from occurring as a standard risk management step. Staff's current approach requires a scope of work and review by at least two employees when performing work on critical infrastructure.	*Y*	3/31/2022	6/13/2022	Y	Staff is continuing to make progress on system hardening and change management including the use of automated deployment tools and templates. **Update:** A new application is being setup to track all changes and approvals within the environment. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
3		Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.	Staff has deployed tools such as inventory, deployment, and recently endpoint management software (EMS) to assist with this effort. Inventory and deployment systems allow staff to track and update software. EMS allows staff to scan endpoints for known security issues that require a patch and force the patch to be installed as part of network policy. Staff is continually working towards further automating and integrating these tools into our workflow. At last count our inventory of applications has more than 6251 software packages and components, which makes this an evergreen maintenance item for staff, requiring much in the way of time and resources.	*Y*	3/31/2022	6/13/2022	Y	A new application is being setup to track all managed systems within the environment. These managed systems will have regular patching cycles based on the manufacturer's recommendations. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
4		Change default credentials upon installation: To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.	Staff will change the identified systems with default credentials where possible. Some examples identified by the audit do not support credentials for their regular operation. For these devices, staff is working towards isolating in a similar fashion to devices that cannot be reasonably patched as a compensating control.	*Y*	3/31/2022	6/13/2022	Y	An existing application is being utilized to ensure default credentials are changed on all managed systems. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
5		Conduct regular vulnerability assessments: As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended, and producing the desired outcome. Consult NIST 800-30 for guidelines on operating an effective risk management program.	Staff believes that regular third party auditing of IT systems is valuable and will contribute to increased security of Carson City systems and data. Performing audits such as this one regularly would likely require additional resources to obtain the audit and then act upon the results of the audit in a timely fashion.	*Y*	3/31/2022	6/13/2022	Y	A new application is being utilized to conduct vulnerability assessments on an established cadence. Staff expects to be able to demonstrate significant progress at the time of the audit follow-up. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**
6		Recommend remediation scanning be performed: Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.	Some issues identified in this report require a small effort to remediate and staff will remediate them in a timely fashion. Others are systemic issues that have already been identified by staff and require large-scale efforts to address in the long term. Additional resources would contribute towards addressing all of the identified issues in a more timely fashion.	*Y*	3/31/2022	6/13/2022	Y	Staff expects to be able to demonstrate progress at the time of the re-test. **Update:** Using the results from the new vulnerability scanning application, critical and high vulnerabilities will be able to be addressed. Legacy systems are still planned for a migration to more modern operating systems with the permission of each department. **UPDATE 6/13/2022 - VALIDATED ALL FINDINGS COMPLETE, NEW REPORT WAS PRESENTED TO AUDIT COMMITTEE 7-12-2022.**

Note: In this audit staff gave maximum access to the auditors to simulate an attacker gaining access to a sensitive area of the network. Many of the identified issues were discovered because we bypassed our usual security controls to allow the penetration tester greater access. The findings are valuable, but do not necessarily represent vulnerabilities that could be exploited from any part of the City network. FINDINGS ARE OBFUSCATED, AS TO NOT PROVIDE A ROAD MAP TO WHERE ISSUES ARE; THEREFORE, TOTAL FINDINGS ARE NOTED, BUT SUMMARIZED HERE.

Item No.	BOS Closure	Finding	Recommendation	City - Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
1		Entergov has tripled the amount of data entry involved in processing a business license when compared to the legacy system. A poorly executed customer interface on the portal coupled with the inability to require payment prior to permit issuance caused the shutting down of the customer portal. Business licenses issued can be issued without payment and credits to potentially fictitious customers can go undetected, creating an opportunity for fraud and potential lost revenue for the City.	The City should continue to work with Energov to determine if the necessary updates can be made to improve efficiency, incorporate preventative controls, and features that will help effectively service customers. Alternatively, if there is no resolution with Energov, then the City should look into alternative software solutions.	Community Development has met with IT and IT is currently working with Energov to determine if resolution of the issues is feasible. If not, the staff will investigate alternative systems. Staff has underfilled a position to hire a consultant in anticipation of not being able to resolve issues. Community Development has set a date of January 1, 2023 and the Director will be the lead in working with the consultant.	N	1/1/2023			
2		Business license fees list on the website is not complete per CCMC 4.04.020, it is missing Fictitious Filing Fees $20 and Technology Fees of $5.	The Director should work to provide an updated list of business fees to the customers for transparency on the website.	The fees can be added to the portion of the website that addresses business license fees as well as included on other materials associated with business license fees. Planning Manager will be responsible.	N	1/1/2023			
3		There is a lot of great information in the full report. This finding has to do with whether or not the City should continue to outsource with Charles Abbott (CAA). There isn't enough data regarding time CAA spends on their services to fully understand all the costs of each Building Permit.	Recommendation is that the City should use the benchmarking data as well as obtain further data on the number of hours each permit takes to process from intake, plan review, permit issuance, inspections, re-inspections, etc., in order to determine if we should continue outsourcing, move to a hybrid approach, or insource all together.	The current contract will expire in August 2024. By July 2023 the Director should provide an analysis to the City Manager/ Board of Supervisors relative to the recommendation to insource, continue outsourcing, or utilizing a hybrid approach. This will provide the City with a year to determine the preferred structure.	N	7/1/2023			
4		It was noted that there was a lack of monitoring of performance metrics as required by the City's contract with CAA. For example: permit transaction reports are attached to monthly invoices, however, the City does not monitor for timeliness of permit related activities or accuracy of the Permit fee calculations. There is also no formal customer feedback process or means of sharing unsolicited feedback with the Director.	Director should enforce the contract requirement for CAA to provide monitoring information to the City. The City and CAA should establish a customer feedback loop. Additionally the City should consider an independent audit of the consultants performance. Lastly, a quarterly or annual trend analysis of reported issues should be created and shared with the Director.	CAA typically does not have sole responsibility for a building permit's review. The delay could come from a City department. Director will work with City Manager's office on customer survey's both internal and external to the City. Reporting and surveys will be Director's responsibility.	N	1/1/2023			
5		Reinspection fee was not charged for FY 2021 and 2022 resulting in losses to the City of $33,000 and $17,000 respectively. There were many instances where the Final Inspection was performed, but the permit was canceled, and auditor was unable to determine the cause for such a late cancelation.	Director should require that re-inspection fees are charged to ensure the City receives payment for work performed. Director should also determine why there were 199 permits in 2021 and 84 permits in 2022 that a final inspection was noted, but no permit was issued.	Director will work with CAA to ensure they start charging the reinspection fee. Director also agrees to look into the canceled permits where inspections occurred by September 30, 2022 and report out to the City Manager, and Audit Committee.	N	9/30/2022			
6		Building Division has not evaluated the cost of its services in 15 years to determine if the fee fully covers the costs. There is currently no reliable data on how much in employee and CAA time it takes to issue a Permit. National Association of Home Builders has stated that construction permit fees are typically 1.7% of total project cost, but City per Permit cost only came to .48% of total project costs.	As an enterprise fund building permit fees should be designed to cover all direct costs. City should use the information contained in the report to help with a cost of service study. A review of expenses should also be done to determine that appropriate and legitimate expenses are properly reported.	Community Development staff does not have the skill set to pursue this recommendation, and we would need to outsource a consultant to pursue this task. Director is watching the fund closely to make sure that non-building related activities are not paid out of this fund.	N	1/1/2023			

Item No.	BOS Closure	Finding	Recommendation	City - Remediation Plan (Course of Action & Expected Benefits)	Finding corrected? (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Validation (Y,N)	Status Comments
7		CAA contract states that the Building Official with CAA is to provide building code enforcement. Based on interviews and discussions with Director and Building Official, CAA is not providing building code enforcement.	Director and possibly DA should enforce the contract language related to code enforcement and work to come to a resolution with CAA.	Director, DA's office and Building Official are scheduled to meet in August 2022 to further discuss.	N	11/1/2022			
8		Final Plan Review doesn't include all Department Final Sign-off, which causes plan delays when inspectors note that final reviews were not signed off.	Process workflow should be implemented to address version controls, for resubmittals of the plans to all plan reviewers to ensure a newer version of the plan is rerouted to all relevant parties for final review.	Director will request that CAA implement a workflow process that addresses the version controls and final reviews sign-off.	*Y*	9/1/2022	8/6/2022		Community Development has reviewed the workflow in energov to verify no one is dropped off the review and the permits techs are implementing

Carson City
IT Vulnerability Update Internal Audit
April 2022

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
		NOTE: 103 - Original Report - RETEST - 27 Remediated, 73 partially remediated, only 2 not remediated.						
1		Update all systems that are currently running on unsupported operating systems: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's infrastructure and data.	Staff is actively working on updating outdated systems and adjusting operations to be in line with industry best practices, such as automatic updates based on how critical a system is. Some legacy systems that cannot be updated will be isolated using a combination of identity based access rules and network security zones to mitigate the risk of their ongoing operation. Some of these systems may be decommissioned if our customer agency's business needs support this outcome. This will increase security, availability, and integrity of Carson City's infrastructure and data.	P	6/30/2025			Decision needs to be made by the System / Software owner for a replacement. Funding will be needed to replace systems and the infrastructure to support any new system. Some systems do not have upgrade path leading to a full replacement. Some systems have be scheduled for replacement in 2025. Example: Tiburon
2		Implement and enforce implementation of change control across all systems: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.	Most issues identified in the external test were expected. Some sites do not use encryption as they don't warrant it with their purpose, others host apps that there are very few options for replacing/updating. Staff has implemented system hardening processes on many systems and will continue to expand on those efforts. Staff is working towards robust change management procedures that could prevent a misconfiguration from occurring as a standard risk management step. Staff's current approach requires a scope of work and review by at least two employees when performing work on critical infrastructure.	P	12/31/2022	1/31/2022		Change Control Policy and Processes implemented January of 2022. Current records state process began in January 2022 within Manage Engine.
3		Implement a patch management program: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.	Staff has deployed tools such as inventory, deployment, and recently endpoint management software (EMS) to assist with this effort. Inventory and deployment systems allow staff to track and update software. EMS allows staff to scan endpoints for known security issues that require a patch and force the patch to be installed as part of network policy. Staff is continually working towards further automating and integrating these tools into our workflow. At last count our inventory of applications has more than 6251 software packages and components, which makes this an evergreen maintenance item for staff, requiring much in the way of time and resources.	P	6/30/2025			Current process is Patch, Reboot, and Scan is performed on the end units the last Thursday of each month and servers the last Wednesday of each month. There are exclusions for high risk and Public Safety units and servers. Reference recommendation #1 for High Risk Legacy systems.
4		Change default credentials upon installation: To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.	Staff will change the identified systems with default credentials where possible. Some examples identified by the audit do not support credentials for their regular operation. For these devices, staff is working towards isolating in a similar fashion to devices that cannot be reasonably patched as a compensating control.	P	6/30/2022	7/26/2022		SOP Created - System Hardening Process has been established which contains Peer Review. Policy is in Policy Tech.

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
5		Conduct regular vulnerability assessments: As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended, and producing the desired outcome. Consult NIST 800-30 for guidelines on operating an effective risk management program.	Staff believes that regular third party auditing of IT systems is valuable and will contribute to increased security of Carson City systems and data. Performing audits such as this one regularly would likely require additional resources to obtain the audit and then act upon the results of the audit in a timely fashion.	P	11/1/2021	11/1/2021		SOP Created - System Hardening Process has been established which contains Peer Review. Policy is in Policy Tech.
6		Recommend remediation scanning be performed: Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.	Some issues identified in this report require a small effort to remediate and staff will remediate them in a timely fashion. Others are systemic issues that have already been identified by staff and require large-scale efforts to address in the long term. Additional resources would contribute towards addressing all of the identified issues in a more timely fashion.	P	4/30/2022	4/30/2022		Comment - This is the retest - 1 year after initial report.

Note: In this audit staff gave maximum access to the auditors to simulate an attacker gaining access to a sensitive area of the network. Many of the identified issues were discovered because we bypassed our usual security controls to allow the penetration tester greater access. The findings are valuable, but do not necessarily represent vulnerabilities that could be exploited from any part of the City network. FINDINGS ARE OBFUSCATED, AS TO NOT PROVIDE A ROAD MAP TO WHERE ISSUES ARE; THEREFORE, TOTAL FINDINGS ARE NOTED, BUT SUMMARIZED HERE.

Carson City
End Point User Internal Audit
April 2022

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
		NOTE: 11 Findings - 5 High Risk, 5 medium risk, 1 low risk.						
1		Remediate the vulnerabilities identified in the City workstation and user account during the Endpoint Security Assessment to address the following high risk findings: undetected virus; security changes by users; disabled networks security controls; unquoted service paths; and unsecure ciphers.	Staff is actively working on noted recommendations, starting with High Risk areas.	*Y*	6/30/2022	8/1/2022		Hardening processes are in place. Current antivirus has been notified on virus gaps and have updated their virus signatures / definitions. Google has been locked down to meet the Security Changes within the Audit. Unsecure Ciphers removed.
2		Remediate the following medium and low risk findings noted on the Endpoint Security Assessment: enforce BitLocker; implement new versions of TLS; require signing on remote services; upgrade the remote host; apply vendor recommended settings for remote host; implement best practice web browsing solution (noted in report).	Staff is actively working on noted recommendations, starting with High Risk areas.	*Y*	6/30/2022	8/1/2022		Items have been remediated.

Item No.	BOS Closure	Recommendation	Remediation Plan (Course of Action & Expected Benefits)	Finding corrected (Y, N, Partial)	Expected Compl. Date	Actual Compl. Date	Auditor Verified? (Y, N)	Status Comments
1		The Sheriff's Office should establish a process that ensures all officers responding to 911 dispatch calls and all self-initiated activities requiring dispatch notification have a BWC video. Additionally, performance metrics and goals should be established for Body Worn Camera ("BWC") activation.	Sheriff is reviewing Axon and other performance products, and will need to build performance metrics and goals.	N	7/1/2023			
2		The Sheriff's Office should update their BWC policy to address when the video upload and categorization is to occur. Additionally, the Sheriff's Office should perform routine monitoring of the uploads and the categorization of videos for completeness and accuracy. Lastly, performance metrics and goals should be established for BWC uploads and categorization of videos.	Sheriff's office agrees and will incorporate into policy instruction when to upload and categorize video from a BWC.	N	10/30/2022			
3		The Sheriff's Office should continue to roll out the BWC program's Early Warning Policy to comply with NRS 289.823. Furthermore, the policy should implement a system and methodology to monitor the BWC video for compliance with the BWC program and policy, and identification of opportunities for improvement to include all uniformed personnel with BWC devices, including the Jailors. This should include an evaluation of the total reviews that need to be completed in order to be statistically significant in comparison to the total of BWC footage of each uniformed personnel with a BWC device or other means of how supervisors chose videos for review, such as utilizing the feature within the Axon software that aids in the random selection of the videos for review. Lastly, the supervisor's monitoring of the videos should also be reviewed for compliance with set methodology and intent of the program and related policies.	The Sheriff's Office has established policy to address the Early Warning Policy, as per NRS 289.823. The implementation of Performance Measures will address the recommendations above. Detention officers are not required to have BWC; however, they have been issued to provide additional audio/visual documentation and record of events. An internal work group will address and publish a policy for camera use within the jail.	N	7/1/2023			
4		Review and update the current BWC policy to reflect current operating practices and alignment with NRS 289.830. Specifically, the policy should be updated to include disciplinary actions.	BWC policy is currently in review as a natural course of implementing the in-car camera as well as the early warning polices. Although not specifically mentioned in the BWC policy, it is a violation of Standards of Conduct for an employee's, "Failure to operate a portable recording device as required by the Office and/or editing or erasing any portion of a recording". See policy 339.5.8.(J). Discipline for the violation can range from a warning up to and including termination.	N	10/30/2022			

Carson City

Wireless Assessment – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nouguier – CISSP, PMP
Director, Cybersecurity Services

Overview

Carson City contracted Eide Bailly to conduct a Wireless Assessment. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization. The goal of the Wireless Assessment was to identify what vulnerabilities are present throughout Carson City's wireless networks.

Efforts were placed on identifying and exploiting security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The assessment was conducted with the level of access that a guest user would have. The assessment was conducted following industry best practices and standards, with all tests and actions being conducted under controlled conditions.

This report documents the Wireless Assessment performed on Carson City's wireless networks, conducted from April 25 to April 28, 2022.

Scope

The scope of this assessment was limited to Carson City's wireless networks and infrastructure as well as publicly available information. Eide Bailly tested the wireless networks in both the Carson City City Hall and Carson City Courthouse.

Summary of Results

Based on the testing performed, Eide Bailly determined that Carson City properly segments its wireless networks by using an open guest network that is separate from its secured corporate networks. None of the networks identified within scope had WPS or other vulnerable extensions enabled. Eide Bailly found that all of Carson City's secured networks are using WPA2. This protocol is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. Eide Bailly also noted that Carson City's wireless networks use the MGT-CCMP encryption mechanism, which is the security standard used with WPA2 wireless networks.

Additionally, Carson City's wireless networks require both a username and password in order to successfully authenticate and obtain network access. By requiring a username and password combination, rather than simply requesting only a password, Carson City implements an extra layer of wireless network security.

Overall, Eide Bailly identified one (1) low-risk finding throughout the Wireless Assessment. This issue was brought to the Carson City IT team immediately and the issue was remediated.

The technical details of this assessment's results, including a full technical writeup of the testing performed, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real-world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. As demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to more closely mimic real-world situations, enabling customers to have increased access to industry-recognized expertise, all while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.