



**Risk Advisory Services  
Network Testing Executive Summary**

October 2020

**CARSON CITY**

**Submitted By:**

Eide Bailly LLP  
Nathan Kramer, CEH  
Associate, Risk Advisory Services

Joe Sousa, CISA, CEH  
Manager, Cybersecurity and information Assurance

Eric Pulse, CISA, CISM, CRISC, GSEC, CFSA  
Principal-in-Charge of Risk Advisory



October 19, 2020

James Underwood  
Chief Information Officer  
Carson City Information Technology  
Carson City, Nevada

Dear James:

This report contains our findings and recommendations relating to the network testing Eide Bailly performed for Carson City in 2020.

No assessment of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, application and control environments are extremely dynamic in nature and our assessment of your controls, security methods, and procedures are conducted and documented as of the following specific period in time.

Assessment Service	Start Date	End Date
<b>External Network Penetration Assessment</b>	09/14/2020	09/23/2020
<b>Internal Network Vulnerability Assessment</b>	09/21/2020	10/01/2020

As a result, the projection of any conclusions, based on our assessment, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, Eide Bailly takes no responsibility for any lack of specific control failures, breach of security, or other errors of fraud related to any part of your operational environment other than those controls and security measures specifically tested and for any period of time other than the period specifically covered by our assessment conducted. Any subsequent control or security issues that may arise within those areas assessed or any control or security issues that are present at the time of this assessment, but that are outside the scope of this assessment, are solely the responsibility of Carson City.

We appreciate the courtesies and cooperation extended to us during this project, and appreciate the opportunity to be of service to Carson City. If you have any questions or need anything additional, please contact me at 605.367.6713 or [jsousa@eidebailly.com](mailto:jsousa@eidebailly.com).

Sincerely,

Joe Sousa, CISA, CEH  
Manager, Cybersecurity and information Assurance

## Executive Summary

### Summary of Results

The table below contains a summary of the results for the area assessed during our assessment of Carson City.

Area Assessed	Rating	Results
External Network Penetration Assessment	<b>Elevated</b>	Eide Bailly identified five (5) high, five (5) medium and two (2) low risk findings.
Internal Network Vulnerability Assessment	<b>Elevated</b>	Eide Bailly identified twenty-two critical (22), sixteen (16) highs, and sixty-five (65) medium risk findings.

### External Network Penetration Assessment

Eide Bailly was contracted by Carson City to conduct an External Penetration Test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization with the goals of: Identifying if a remote attacker could penetrate the organizations defenses and determining the impact of a security breach of confidentiality of the organization’s private data, internal infrastructure and availability of the organization’s information systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in PTES (Penetration Testing Execution Standard) with all tests and actions being conducted under controlled conditions.

### Methodology

Eide Bailly utilized the PTES which defines the process related to a penetration testing. From the initial communication and information gathering, it also covers threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization through vulnerability research, exploitation and post exploitation.

The PTES consists of seven phases:

1. **Pre-engagement Interactions** - In this phase, we prepare and gather the required tools, operating systems, and software to start the penetration testing. Selecting the tools required during a penetration test depends on several factors such as the type and the depth of the engagement. Some of the tools include:
  - WHOIS
  - DNSEnum
  - Nessus
  - Nmap
2. **Intelligence Gathering** - In this phase, the information or data or intelligence is gathered to assist in guiding the assessment actions. The information gathering process is conducted to gather information about the employee in an organization that can help us to get access, potentially secret or private “intelligence” of a competitor, or information that is otherwise relevant to the target.

3. **Threat Modeling** - Threat modeling is a process for optimizing network security by identifying vulnerabilities and then defining countermeasures to prevent or mitigate the effects of threats to the system. Threat modeling is used to determine where the most effort should be applied to keep a system secure. This is a factor that changes as applications are added, removed, or upgraded or user requirements are evolved.
4. **Vulnerability Analysis** - Vulnerability Analysis is used to identify and evaluate the security risks posed by identified vulnerabilities. The Process of vulnerability is divided into two steps, Identification and Validation.  
  
Identification: Discovering the vulnerability is the main task in this step.  
Validation: In this step, we reduce the number of identified vulnerabilities to only those that are actually valid.
5. **Exploitation** - After finding the vulnerabilities, we try to exploit those vulnerabilities to breach the system and its security. For the Exploitation, we use different framework and software that are recommended for exploitative purpose and are freely available. Some of the most recommended tools include:
  - Kali Linux
  - Metasploit
  - Burp Suite
6. **Post Exploitation** - In the Post-exploitation phase, we determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machine's usefulness in further compromising the network.
7. **Reporting** - In this phase, we report the findings in a way that is understandable and acceptable by the organization that owns that system or hardware. It includes the defects that allow an attacker to violate an explicit (or implicit) security policy to achieve some impact (or consequence). In particular, defects that allow intruders to gain increased levels of access or interfere with the normal operation of systems are vulnerabilities.

Our external network penetration assessment was designed to answer the following questions for Carson City:

- **Was Eide Bailly able to compromise Carson City's external network security?**

**No.** During the conduct of our testing, we were not able to compromise Carson City's external network security. We were also unable to obtain any sensitive information or gain sufficient access to any of Carson City's servers to gain control of those servers.

- **Did Eide Bailly identify any issues that Carson City should be aware?**

**Yes.** Our testing did identify some security issues related to Carson City's external network. These issues are documented in "Carson City External Pen Test Report 2020.pdf" report provided to IT management.

- **What is Eide Bailly's assessment of Carson City's external network security?**



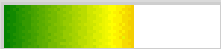


Based on the expertise and experience of Eide Bailly, the recommendations and best practice guidelines identified in this report will provide a foundation to improve the security of the external network environment. Eide Bailly experts understand the implications of the challenges facing governments daily, and that security is a process, not a destination. As such, an external penetration assessment is the first step in securing internal, external, and DMZ resources. Eide Bailly understands organizational and operational needs and is committed to providing world class, quality service. Due to the constantly changing threat environment, we recommend an external penetration analysis be performed at least annually. Additionally, Eide Bailly security experts are also available on a

consultation basis to assist in remediation of any findings.

Eide Bailly assigns a risk level to each identified issue discovered during the assessment. We base this risk level on an expert analysis of the issue, its environment, and the severity of the identified issue. We derive the suggested remediation timeline from the potential for system compromise, overall damage to the environment/system, and criticality of information theft.

**Twelve (12) findings** were identified during the internal vulnerability assessment of the addresses provided. These findings are summarized below by risk (the risk ratings are defined in the Scope section of the report). We were able to assess the organization’s performance through the vulnerability scanning and testing activities.

Based on our testing, we determined that we would rank the organization’s external network risk as Elevated in the areas assessed.

Risk Level	Description
Critical 	Risk of immediate exploitation or critical level of exposure that can lead to system or application compromise or information theft. Remediation should be conducted immediately or as soon as possible.
High 	Significant risk of severe impact to system or application security. Remediation should be prioritized or within (1) month.
Elevated 	Risk of an elevated nature that may expose sensitive information or may be used in conjunction with other issues aiding in exploitation. Remediation should be prioritized based on the criticality of the system and information exposed or within (3) months.
Moderate 	Risk of a less critical nature that may potentially lead to information theft or misuse. Remediation should be included in the next security update or within six (6) months.
Minimal 	Risk of a non-critical nature that may lead to misuse or stability loss or enhancement features, which will improve security. This issue should be noted for reference; however, remediation is not strictly necessary.

## Recommendations

Due to the impact to the overall organization as uncovered by our testing, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention.

1. **Update all systems that are currently running 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 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 perimeter network.
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.
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.
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.

## Internal Network Vulnerability Assessment

Eide Bailly LLP conducted an internal vulnerability assessment to establish a comprehensive view of the Carson City's network as it appears from the inside. This allowed us to identify potential security weaknesses within the network configuration which could allow an intruder to gain unauthorized access or cause network disruptions. The assessment consisted of a semi-blind internal assessment where Eide Bailly was provided the internal network IP addresses. The scanning system utilized by the Eide Bailly consultant for testing was placed in a server VLAN which allowed access to each subnet and host without restrictions. Without this, Eide Bailly would have been placed on the user network and would have had limited access to scan hosts based on the level of segmentation in place.

## Methodology

Efforts were placed on the identification and exploitation of security weaknesses that could allow an attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in PTES (Penetration Testing Execution Standard) with all tests and actions being conducted under controlled conditions.

For this security assessment, Eide Bailly followed a custom methodology patterned after actual attacks organizations are facing from hackers.

- Internal Infrastructure Foot printing
- Port Scanning and System Fingerprinting
- Vulnerability and Exploit Research
- Manual Verification of Identified Vulnerabilities

Our internal network vulnerability assessment was designed to answer the following questions for Carson City:

- **Could Eide Bailly compromise Carson City’s internal network security?**

**Yes.** During the conduct of our testing, we were able to compromise Carson City’s internal network security. Systems were accessible with either default or no credentials. Systems were missing critical patches that could enable attackers to perform remote code execution on internal systems. Out-of-date systems and operating systems are running within the network. We were not able to obtain any sensitive information but did gain access to internal systems via multiple attack vectors.

- **Did Eide Bailly identify any issues that Carson City should be aware of?**






**Yes.** Our testing did identify some security issues related to Carson City’s internal network. These issues are documented in “Carson City Internal Vulnerability Report 2020.pdf” report provided to IT management.

- **What is Eide Bailly’s assessment of Carson City’s internal network security?**

Eide Bailly LLP conducted an internal vulnerability assessment to establish a comprehensive view of the Carson City’s network as it appears from the inside. This allowed us to identify potential security weaknesses within the network configuration which could allow an intruder to gain unauthorized access or cause network disruptions. The assessment consisted of a semi-blind internal assessment where Eide Bailly was provided the internal network IP addresses.

**103 findings** were identified during the internal vulnerability assessment of the addresses provided. These findings are summarized below by risk (the risk ratings are defined in the Scope section of the report). We were able to assess the organization’s performance through the vulnerability scanning and testing activities.

Based on our testing, we determined that we would rank the organization’s internal network risk as **Elevated** in the areas assessed.

Risk Level	Description
Critical 	Risk of immediate exploitation or critical level of exposure that can lead to system or application compromise or information theft. Remediation should be conducted immediately or as soon as possible.
High 	Significant risk of severe impact to system or application security. Remediation should be prioritized or within (1) month.
Elevated 	Risk of an elevated nature that may expose sensitive information or may be used in conjunction with other issues aiding in exploitation. Remediation should be prioritized based on the criticality of the system and information exposed or within (3) months.
Moderate 	Risk of a less critical nature that may potentially lead to information theft or misuse. Remediation should be included in the next security update or within six (6) months.
Minimal 	Risk of a non-critical nature that may lead to misuse or stability loss or enhancement features, which will improve security. This issue should be noted for reference; however, remediation is not strictly necessary.

## Recommendations

Due to the impact to the overall organization as uncovered by our testing, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention.

- 1. Update all systems that are currently running 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.
- 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.
- 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.
- 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.
- 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.
- 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.