LEGAL SERVICES CORPORATION
OFFICE OF INSPECTOR GENERAL

Information Technology Vulnerability Assessments of Select Legal Services Corporation Grantees: 2024 Summary of Results and Key Recommendations to Strengthen Information Technology Security

June 3, 2024

Executive Summary

In March 2021 the Legal Services Corporation (LSC) Office of Inspector General (OIG) contracted with Securicon LLC (Securicon) to perform vulnerability assessments on grantee information technology (IT) systems. For the most recently completed contract year, Securicon scanned and assessed the network security of six grantees over a five-month period (November 2023 – March 2024). The objective of the vulnerability assessments was to determine if the assessed grantees' networks have vulnerabilities that can be exploited to compromise the integrity of the IT system or data or allow the theft and unauthorized manipulation of data and resources.

The results of the scans in this contract period were not improved over prior years. The last two years' assessments found that LSC grantees need to take immediate steps to address security vulnerabilities, as well as make plans to address other recommendations that will improve their information security posture in the long term. The results of all the IT Vulnerability Assessments were in the **unacceptable range**, which is the lowest possible rating.

This report includes recommendations that all LSC grantees can implement to quickly reduce the risk of information security attacks.

Objectives and Methodology

A vulnerability assessment provides grantee management and system and security administrators visibility to potential issues in the target network environment. These vulnerabilities may provide malicious actors an opportunity to exploit, compromise, modify or damage grantee data, information systems, or reputation. Identifying grantee information system vulnerabilities is essential to address known risks as part of a risk management program.

The objective of the vulnerability assessments was to proactively determine whether the grantees' networks have vulnerabilities that can be exploited to compromise the integrity of the system or data or allow the theft and unauthorized manipulation of data and resources.

Based on an OIG risk assessment selection process, Securicon scanned and assessed the network security of six grantees. Using the assessment results, Securicon assigned composite vulnerability security ratings to each grantee based on the likelihood of exploitation and potential impact of certain vulnerabilities that they found. Findings and observations identified during the remote assessments pertain only to hosts scanned at the time of the assessments.

Grantees could be classified as being in one of four categories: outstanding, excellent, acceptable, and unacceptable.

Results of the IT Security Assessments

The results of each assessment were shared with the individual grantees. This summary report lists recommendations and industry best practices to mitigate vulnerabilities and strengthen network security.

The six grantees varied widely in their security postures. However, all six grantees were rated unacceptable. This indicates the need for immediate and enhanced management attention on adopting policies and practices to reduce the risk and potential impact of cybersecurity incidents.

The OIG advises all grantees to adopt the near-term and longer-term recommendations and best practices that Securicon identified. Specifically, Securicon identified near-term recommendations that could immediately improve a grantee's security posture, such as applying software updates on all systems and removing unnecessary or unsupported software. Securicon also identified recommendations that could improve a grantee's security posture in the long term, such as implementing a patch management program and keeping an inventory of devices that belong on the network.

Finally, Securicon identified the following best practices: regularly performing vulnerability scans, implementing a defense strategy that uses multiple security measures (such as complex passwords and firewalls), and adding additional security layers to minimize risk (such as two-factor authentication and encryption).

Recommendations and Security Best Practices

Grantees could improve their security posture by simultaneously adopting several near-term recommendations, and implementing strategic recommendations that would position them to prevent or mitigate cybersecurity incidents in the longer term. Securicon recommends that grantees take the following actions:

Implement Near Term Recommendations to Immediately Improve Cybersecurity

Near-term recommendations are intended to immediately improve a grantee's security posture, if implemented. These recommendations can also be thought of as "quick wins" requiring minimal cost, resources, or effort to implement. Near-term recommendations support long-term recommendations whenever possible.

Securicon recommended that grantees:

1. Apply operating system and software updates on all systems.
2. Update and/or patch third party firmware and software. If the systems cannot be patched due to vendor constraints, enable a host-based firewall to block or filter connections to affected services.
3. Remove unnecessary or unsupported software, when possible.
4. Segment network boundaries using a firewall or router and apply firewall rules or access control lists to allow or deny traffic between zones as required.
5. Develop and maintain an approved port, protocols, and services whitelist and close any undocumented open ports.
6. Create inventory asset lists and network architecture diagrams that are maintained on a regular basis.

Develop and Implement Plans to Adopt Long-Term Recommendations to Maintain Improved Cybersecurity

Long-term recommendations define longer term initiatives and implementing processes. The goal is to prevent identified vulnerabilities from recurring. These initiatives may need to be addressed through formal security engineering efforts and may require substantial resources, budget, and time to implement.

Securicon recommended that grantees:

1. Implement a vulnerability scanning system which can securely and routinely (monthly or quarterly) conduct authenticated scans and report on all grantee IT assets. Grantees should not rely on host-based security tools or segmentation to obscure vulnerabilities (e.g., using host-based firewalls to hide operating system service vulnerabilities).
2. Implement a comprehensive patch management program to apply all available patches, firmware, and software updates. To prevent downtime or a negative impact on business operations, grantees should create a test and evaluation network which includes systems similar to those found in production networks. Patches should be installed first in this environment to test for negative impact on systems and applications before installing the updates on production hosts. Alternatively, patches and updates may be scheduled outside of business hours to minimize business interruptions.
3. Ensure that all communications at the external managed interfaces, including cloud and/or publicly available system components, and at key internal managed interfaces, are properly monitored in accordance with the organization's overall security architecture.

4. Research and if possible employ modern zero-trust architectures and controls. Zero-trust acknowledges the need to eliminate reliance on a singular authentication and control boundary to effectively mitigate risks.
5. Conduct routine manual and automated device inventories. If device inventories identify unknown devices, determine whether they should be added to the inventory or removed from the system.
6. Implement network segmentation to separate assets according to their risk or level of control. For example, move IP phones into a network separate from servers or desktop systems.
7. Establish clear physical and logical separation between static authorized systems and transitory non-grantee-controlled devices (e.g., personally owned digital devices).

Embrace Best Practices to Improve an Organization's Cybersecurity Posture

These best practices will improve an organization's information security posture. We encourage implementing as many as possible.

1. The foundation of robust IT security is knowing what devices reside in the environment. Take an asset inventory that is maintained on a regular basis. The asset inventory documentation should be supported by network diagrams that give a visualization of the network landscape and how data flows in and out of the environment.
2. Implement a defense-in-depth strategy that leverages multiple security measures to protect an organization. The core layers should include:
    a. Strong, complex passwords
    b. Antivirus software
    c. Secure gateway
    d. Firewall
    e. Patch management
    f. Backup and recovery
    g. The principle of least privilege, or giving a user the minimum access level or permissions needed to do their job
3. Adding additional security layers to further minimize risk such as:

a. Two-factor authentication (2FA) or multi-factor authentication (MFA)
b. Intrusion detection and prevention systems
c. Endpoint detection and response (EDR)
d. Network segmentation
e. Encryption
f. Data loss prevention
g. Virtual Private Networks (VPN)

Information Technology Security Resources for Grantees

Additional LSC and OIG guidance to help you strengthen your information technology security posture is available on the OIG Website:

- Cyber Security Resources
- LSC OIG Fraud Alerts and Best Practices
- LSC's Technology Baselines (Issued by LSC President, Ron Flagg in August 2023; security best practices are in Chapter 3)