Office of Inspector General
Legal Services Corporation

Inspector General
Jeffrey E. Schanz

3333 K Street, Nw; 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

Memorandum

TO: All Executive Directors

FROM: Jeffrey E. Schanz, Inspector General

DATE: March 28, 2017

SUBJECT: Results of Information Technology Vulnerability Assessments

We are pleased to provide the attached Management Analysis Report that summarizes recent information technology assessments on selected Legal Services Corporation (LSC) grantees conducted by InfoReliance, a contractor for LSC Office of Inspector General (OIG). The assessments performed were not audits of grantee systems, but were considered non-audit services to assist grantees in maintaining a secure information technology environment. The attached report is a high-level summary of vulnerability tests and scans that examined grantee networks from both an external and internal perspective. While each grantee we reviewed was different in size and complexity in regards to network configurations, our contractor provides a list of common security issues noted as well as best practices to mitigate these vulnerabilities. The issues noted are not all encompassing but are intended to provide insight into what common areas may affect LSC grantees and can focus their attention to strengthen their network security to minimize the potential for system compromise.

This report is intended for you to use to evaluate and compare your current information technology architecture, software and network settings to the broader results of the scans across the grantee population. It is also intended to make you aware of common deficiencies and provide solutions to the issues identified in the assessments. The report discusses industry best practices and standards to enhance your awareness of both and to enable you to implement them.

Section 8(a) of LSC grant conditions require grantees "...to have an information security system that ensures confidentiality and security of its operations, assets, data, and files." You can also refer to the April 2015 technology letter found at http://www.lsc.gov/sites/defaulUfiles/TIG/pdfs/LSC-Technology-Baselines-2015.PDF. Discussion of information technology security begins on page 24 and includes information on the tools, policies and practices that should be in place. If you should have any questions or comments, please contact John Seeba, Assistant Inspector General for Audit at 202-295-1581 or email at jseeba@oig.lsc.gov.

Attachment

LEGAL SERVICES CORPORATION – OFFICE OF INSPECTOR GENERAL (LSC–OIG)

LSC–OIG Grantee Site Vulnerability Assessment

Management Analysis Report

Date: January 30, 2017

Contract Year: 2016

Prepared by

INFORELIANCE

www.inforeliance.com

[Intentionally Blank]

Table of Contents

List of Figures

List of Tables

1.0 Executive Summary

As part of contracted work between the Legal Services Corporation-Office of Inspector General (LSC-OIG) and InfoReliance Corporation, the InfoReliance Vulnerability Assessment Team (IVAT) assessed the network security of six (6) Grantee sites over a 10-month period. Grantees were geographically dispersed across the continental United States and its territories. They differed in the number of sub-sites that comprised their network environment, as well as the way in which their network architecture was set up.

The assessment team conducted vulnerability testing of target networks from numerous perspectives. Examinations from the open Internet represented unprivileged external access, whereas analysis from the network space represented privileged internal access. The assessment team performed activities and tests necessary to identify vulnerabilities, flaws, and weaknesses in the architecture, technologies, and processes that could potentially compromise the target systems. Findings and observations identified during each Grantee site's onsite or remote assessment, pertained only to hosts scanned at the time of the assessments.

2.0 Assessment Findings

The security posture of all Grantee sites were similar to those typically found in small to mid-size businesses. Of the assessments performed, Grantee sites generally did not present a high level of risk of exposure from outside their networks. There were no critical or high-level vulnerabilities found in the external boundary of any network space. Open ports were standard to common services and necessary operations for those particular Grantee sites. Additionally, no Malware vulnerabilities were found during the scan window on any clients or servers with internal access to the network.

The more critical vulnerabilities discovered at each Grantee site were internal to the network environment and resulted from out-of-date Operating Systems (OSs), patches, and updates. Almost every site either had plans in place or were in the process of upgrading unsupported components. All sites had multiple systems missing Microsoft and third-party software updates. However, since the completion of their site assessments and out-briefs, many Grantees have initiated remediation of these updates.

The following sections provide greater insight into the common vulnerabilities found across the Grantee sites and detail the scores resulting from each assessment:

- Common Security
- Grantee Site Assessment Scores

2.1 Common Security Vulnerabilities

Some common security vulnerabilities discovered on the Grantee networks presented significant risk to the security of their infrastructure and information. The following security vulnerabilities found required correction and/or mitigation:

Finding	Risk Rating	Description
Unsupported OSs	Critical	OSs that no longer receive mainstream vendor support were in use on each Grantee's network and may not receive security updates and patches. Computer systems running unsupported software are exposed to an elevated risk of cybersecurity dangers, such as malicious attacks or electronic data loss.
Authorized Device Management	High	Complete and accurate lists of recognized and authorized devices were not maintained across all sites. Additionally, there were no standard naming conventions for authorized devices, which presents vulnerabilities in terms of client management and authentication.
Hardwired Network Authentication	High	No hardwired authorized device authentication was in place at several sites. This presents a vulnerability in that rogue devices could be connected to unmonitored ports and gain access to the system.
Domain Password Strength	Medium	There were instances were passwords did not meet "Strong" password industry best practices. "Strong" passwords are defined as: • at least eight (8) characters, • one (1) uppercase and one (1) lowercase character, • one (1) digit, • one (1) special character, if allowed, and • not easily inferred (i.e., organization name).
Current Patches and Updates	High	Numerous patches and software updates were not current and/or were missing across Grantee networks. Many Microsoft Security Bulletins, Oracle Java, and Adobe vulnerabilities were discovered on each Grantee network, with patching and updates several years out-of-date.
Weak and Untrusted Certificates and Encryption	Medium	Weak or untrusted client and server certificates vary depending on application requirements. These vulnerabilities require research by responsible parties for appropriate mitigation.
Virtual Host Server	Medium	Unpatched virtual hosting environments presented vulnerabilities that could compromise the integrity of the guest systems.
Policy Configuration Settings	High	The following policy configuration settings presented high risk vulnerabilities: • Allowing anonymous logon users to identify all account names and shared resources • Auto-play configurations allowing the immediate reading of a drive as soon as the media is inserted • Solicited remote assistance configurations allowing for remote access by unauthorized users • Elevated privileges for standard user accounts. Standard user accounts must be restricted to prevent

	🟧	the elevation of privileges for users while installing software. This can allow malicious persons and applications to gain full control of a system.

Table 1: Common Security Vulnerabilities

2.2 Grantee Site Assessment Scores

Site assessment scores were aggregated for each Grantee from scan results of systems tested at each site. Based on U.S. Government assessment criteria, scoring was calculated from findings discovered on four separate scans. Taking into consideration industry best practices, business and budget constraints, data sensitivity, and overall risk, the grading scale, as shown on the right side of **Figure 1** below, was implemented to provide realistic measures for success.

From the results of the scanned systems and the IVAT's observations, Grantees were individually assessed the following scores:

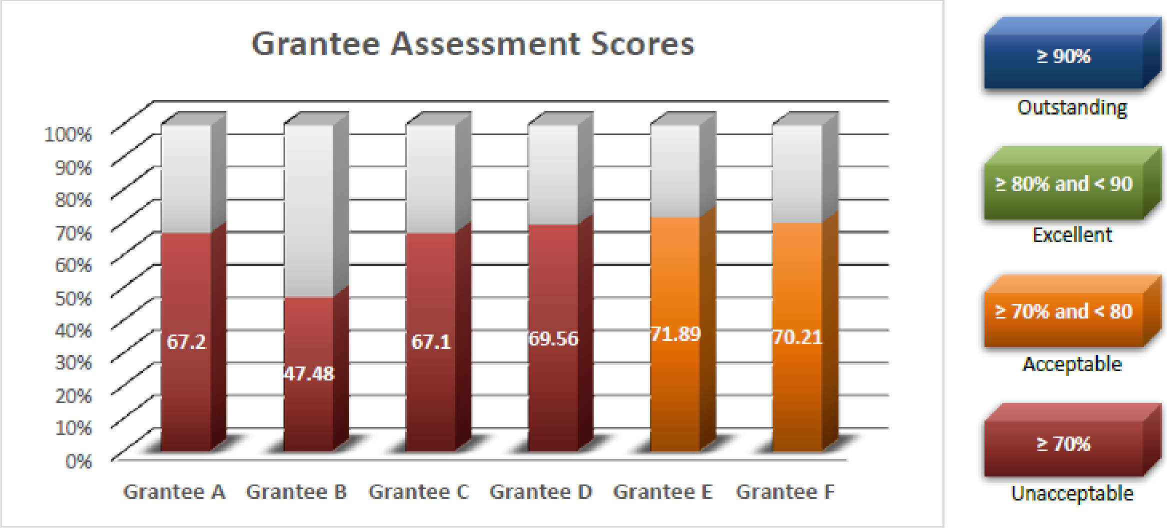

Figure 1: Individual Grantee Assessment Scores and Grading Scale

A regular and consistent patch management plan that covers OEM and third-party software, along with regular self-assessment scans, should result in an improved security posture and ultimately a higher score for Grantee sites. Additionally, implementing appropriate configuration management of network settings will aid in achieving a security baseline in line with Information Technology (IT) best practices.

3.0 Basic Security Best Practices

The protection of information and an organization's IT assets is a careful balance between security and risk. It is always best to first identify what information to protect and then develop a desired "end-state" or security objectives. An organization's security objectives should be a set of realistic goals that balance the principles of security – confidentiality, integrity, and availability.

Organizations will often take a singular technical approach to security, which usually leads to an unbalanced security posture that exposes vulnerabilities. A sound cybersecurity plan will be a holistic approach that encompasses not only technology, but also processes and procedures employing physical, administrative, and technical controls to establish layered defense-in-depth protection, as shown in **Figure 2**.

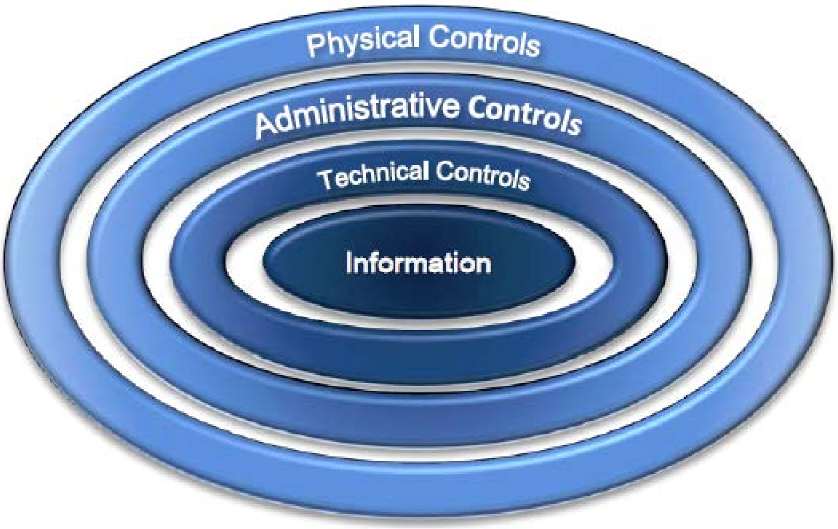

Figure 2: Layered Defense-In-Depth Protection

The following sub-sections describe the recommended minimum cybersecurity best practices for any small- to mid-sized organizations with an IT infrastructure.

- Physical Security Control Requirements
- Administrative Security Control Requirements
- Technical Security Control Requirements

3.1 Physical Security Control Requirements

Physical controls are measures put in place to protect personnel, facilities, and resources. At a minimum, we recommend that each Grantee implement the following physical security controls:

- Restrict office spaces from unauthorized personnel
- Install security and monitoring systems in office spaces
- Disable network wall jacks that are not in use

3.2 Administrative Security Control Requirements

Administrative controls are measures put in place to optimize the management of the policies and procedures that can prevent and detect security threats. At a minimum, we recommend that each Grantee implement the following administrative security controls:

- Ensure Wi-Fi and domain passwords are strong. “Strong” passwords are defined as: at least eight (8) characters – one (1) uppercase, one (1) lowercase, and one (1) special character, if allowed – one (1) digit, and not easily inferred (i.e., organization name).
- Maintain a list of authorized devices on the network and enforce network access through Media Access Control (MAC) address filtering
- Change the default credentials on all routers and switches
- Implement (or update) a patch management plan to identify all software requiring patches and to prevent exploitation of easily-countered vulnerabilities. It is very important that a software list is maintained. Microsoft-based patching solutions, like Windows Server Update Services (WSUS), may not provide patching for all software installed on your network. Additionally, software that is unaffiliated with Microsoft, such as Oracle Java or Adobe, need to be included in your patch management plan, so that they are tracked and managed manually.
- Establish basic cybersecurity awareness training for all Grantee staff that outlines healthy Internet usage, enabling them to detect and avoid potentially compromising situations. Recommended areas of study are below and can be found for free online (http://www.pbs.org/wgbh/nova/labs/lab/cyber/1/1/, for example):
    - Social engineering
    - Phishing attempts
    - Malicious links
    - Personally Identifiable Information (PII) – Identify Theft Prevention
    - Safe Internet Browsing

3.3 Technical Security Control Requirements

Technical security controls are hardware- and software-oriented measures and configurations that are put in place to secure IT infrastructure and protect information. At a minimum, we recommend that each Grantee implement the following technical security controls:

- Employ the Wi-Fi Protected Access 2 - Pre-Shared Key (WPA-2) Wi-Fi security protocol instead of the Wired Equivalent Privacy (WEP). WEP is an outdated security protocol and can easily be penetrated within a few minutes.
- Upgrade all servers and client OSs to current vendor-supported versions or other Cloud-based services. There are software vendors and service providers in the marketplace who offer migration assistance from an outdated system to a currently supported OS or Software as a Service (SaaS)/Infrastructure as a Service (IaaS) products and services. Computer systems running unsupported software are exposed to an elevated risk of cybersecurity dangers, such as malicious attacks or electronic data loss. Organizations that are governed by regulatory obligations may find they are no longer able to satisfy compliance requirements while running outdated systems.
- Employ WSUS, or a like service, which enables IT administrators to deploy the latest Microsoft product updates, to computers that are running the Windows OS. By using WSUS, administrators can fully manage the distribution of updates released through Microsoft Update to computers in their network.

- Establish and maintain a consistent backup plan for all data and regularly test
- Regularly conduct anti-malware scanning, such as Malwarebytes (https://www.malwarebytes.org/). This provides a low-cost, but robust solution, to combating malicious software.
- Those organizations that operate a firewall should employ the following best practices:
    - Review firewall policies regularly
    - Close all unnecessary ports
        - As a good common practice, you should only open the ports that clients and servers need to communicate with other networks and the Internet.
        - Special attention should be paid when opening Transmission Control Protocol (TCP), port 25 (i.e., Simple Mail Transfer Protocol [SMTP] port), to the Internet. Whenever possible, close this port for all clients and servers except the mail server. All clients and servers should relay their email to the Internet through central SMTP servers. Doing this will go a long way toward helping prevent infected clients on corporate networks from distributing unsolicited emails.
    - Back up your firewall regularly
    - Update firewall firmware
- Disable Telnet/Terminal Services – Telnet enabled at all times on any device poses significant risk to a network and should be disabled when not in use. Terminal Services transmits data in plain text. As a result, this capability should be upgraded to Remote Desktop Services (RDS) with Network Level Authentication (NLA).

Appendix A: Acronyms

All of the acronyms used in this document appear in **Table 2**. All acronyms are also fully defined the first time they appear in the document.

Acronym	Definition
IaaS	Infrastructure as a Service
IT	Information Technology
IVAT	InfoReliance Vulnerability Assessment Team
LSC	Legal Services Corporation
MAC	Media Access Control
NLA	Network Level Authentication
OIG	Office of Inspector General
OS	Operating System
PII	Personally Identifiable Information
POC	Point of Contact
RDS	Remote Desktop Services
SaaS	Software as a Service
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
WEP	Wired Equivalent Privacy
WPA-2	Wi-Fi Protected Access 2 - Pre-Shared Key
WSUS	Windows Server Update Services

Table 2: Acronyms