**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 31, 2020

**SUBJECT:** Results of Information Technology Vulnerability Assessments

---

In light of the COVID-19 crisis, we are aware that many of you have additional demands placed on your information technology systems as you incorporate telework and other remote methods to provide services critical to clients during this time of increased need. It is our hope that this report will aid you in meeting those demands and mitigating the associated risks as you stay vigilant with your network security.

The attached Management Analysis Report summarizes the results of recent information technology assessments on selected Legal Services Corporation (LSC) grantees conducted by ECS Federal, LLC, a contractor for the LSC Office of Inspector General (OIG). It is a high-level summary of vulnerability tests and scans that examined grantee networks from both an external and internal perspective. It provides insight into common security issues noted across grantee sites and best practices to mitigate these vulnerabilities and strengthen network security.

This report is intended to help you 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.

For additional guidance on information technology security, you can also refer to the April 2015 technology letter found at: https://www.lsc.gov/sites/default/files/TIG/pdfs/LSC-Technology-Baselines-2015.PDF. Discussion of information technology begins on page 24 and includes guidance on the tools, policies, and practices that should be in place. Should you have any questions or comments, please contact Roxanne Caruso, Assistant Inspector General for Audit at 202-295-1582 or rcaruso@oig.lsc.gov.

Attachment

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

## LSC-OIG Grantee Site Vulnerability Assessment Management Analysis Report

Date: December 31, 2019

Reporting Period(s): 2018 / 2019

Prepared by

ECS

http://ecs-federal.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 ECS Federal (formerly InfoReliance Corporation), the ECS Federal Vulnerability Assessment Team (EVAT) assessed the network security of eight (8) Grantee sites over a 16-month period. Grantees were geographically dispersed across the continental United States. They differed in the number of sub-sites that composed their network environments as well as the way in which their network architectures were designed.

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 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 limited numbers of critical- or high-level vulnerabilities found in the external boundary of any network space. Ports were primarily discovered in filtered or closed states. Any open ports were generally standard to common services and necessary operations for those particular Grantee sites.

The more critical vulnerabilities discovered at each Grantee site were internal to the network environment and primarily resulted from out-of-date Operating Systems (OSs) and applications as well as absent software patches and updates. Almost every site had multiple systems missing Microsoft and third-party software updates. Additionally, instances of configurations susceptible to malware were found during scan windows at approximately half of the assessed Grantee sites.

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
- Annual Assessment Trends

## 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 / Applications** | **Critical** | OSs and applications that no longer receive mainstream vendor support were in use on all Grantee networks 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. |
| **Bring Your Own Devices (BYODs) Management** | **Critical** | BYODs not isolated and unmanaged by IT support diminish inherent security mechanisms between critical business systems and potentially compromised devices. |
| **Authorized Device Management** | **High** | Complete and accurate lists of recognized and authorized devices were not maintained across all sites. Grantees in which asset inventories were maintained did not appear to be audited regularly. There were also inconsistent 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. |
| **Outdated Antivirus and Endpoint Protection** | **High** | Outdated antivirus and endpoint definitions leave clients susceptible to multiple exploitation attacks posing a serious risk to networks. Attackers can take advantage of these vulnerabilities and cause significant harm to the security posture. |
| **Current Patches and Updates** | **High** | Numerous patches and software updates were not current and / or were missing across several Grantee networks. Many Microsoft, Oracle, Java, and Adobe vulnerabilities were discovered on Grantee networks, with patching and updates several years out-of-date. |
| **Weak Encryption for Secure Web Access** | **Medium** | Weak encryption ciphers and Secure Sockets Layer (SSL) configurations were found on Web access and Virtual Private Network (VPN) tools at more than half of the assessed sites. This common vulnerability allows for the SWEET32 cyber-attack, which allows hackers to “hijack” a user’s Web browsing or VPN session. |
| **Flat Network Architecture** | **Medium** | A flat network configuration model was present on almost all Grantee networks. All devices, within a given sub-site, were found to be on the same logical subnet to include servers, clients, and / or network infrastructure devices. Assignment of all network devices on a single subnet presents vulnerabilities to network propagation of worms, viruses, and malicious attackers. Configuring subnets in this manner eliminates the security barrier between potential rogue devices and compromised clients and network servers and infrastructure devices. |
| **Ports Open to Public Internet** | **Medium** | Ports found open to the public Internet ranged anywhere from one (1) to six (6) on a given assessed Grantee network. Open, unfiltered ports increase security risks when not required for day-to-day operations. |

| | | |
|---|---|---|
| **Malware Susceptibility** | **Medium** | Weak configurations were discovered at half of the assessed Grantees. Weak configurations do not necessarily imply confirmation of malware, but identify potential exposures by which an attacker can infect the network environment. |
| **Remote Desktop Protocol (RDP) Man-In-The-Middle (MITM) Weakness** | **Medium** | An RDP server stores a hard-coded Rivest-Shamir-Adleman (RSA) private key in a library designated on a given system. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this MITM attack. |

**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. To provide realistic measures for success, the EVAT implemented a grading scale – as shown on the right side of **Figure 1** – that takes into consideration industry best practices, business and budget constraints, data sensitivity, and overall risk.

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

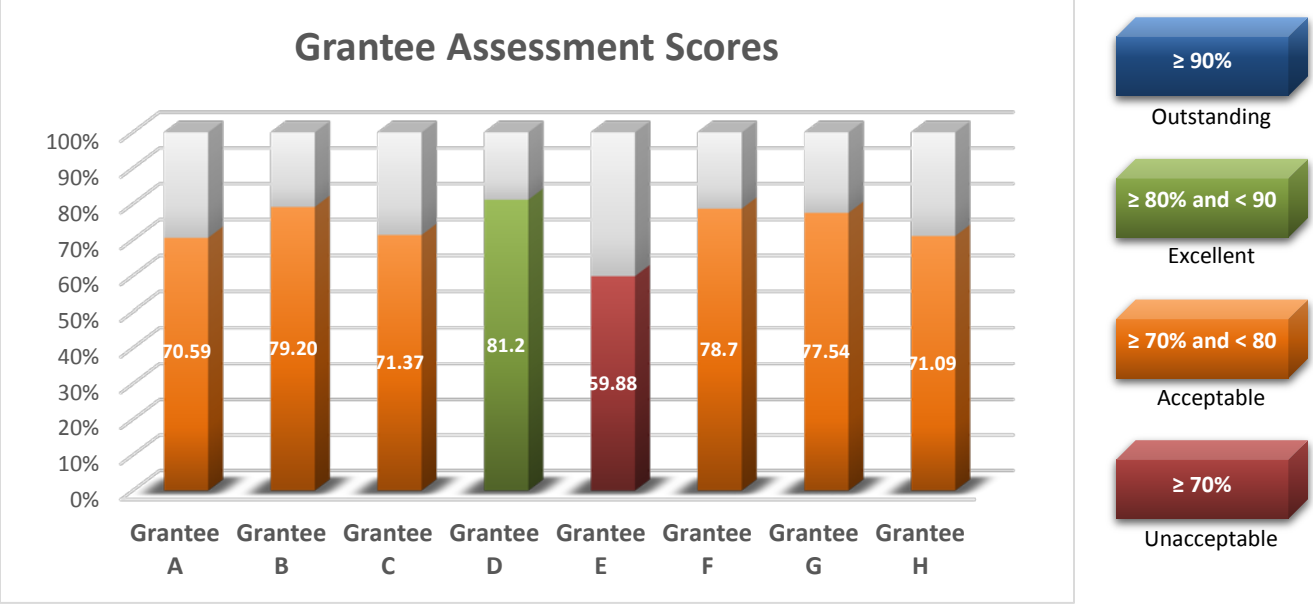


**Figure 1: Individual Grantee Assessment Scores and Grading Scale**

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 as well as proper logging and administration of authorized devices and BYOD networks will aid in achieving a security baseline in line with IT best practices.

## 2.3 Annual Assessment Trends

On average, Grantees assessed during the 2018 and 2019 calendar years performed approximately 5.5 percent and 2 percent (respectively) lower than Grantees assessed in the second year of the program and approximately 7 percent and 10 percent (respectively) higher than Grantees assessed during the initial year of the program, as shown in **Figure 2**. Grantees assessed in 2018 and 2019 tended to have fewer vulnerabilities exposed to the open Internet or external to the Grantee networks. However, assessed Grantees trended towards more vulnerabilities internal to the Grantee networks with more instances of out-of-date or unsupported OS, application, and Web browser software as well as configurations vulnerable to malware. Additionally, while Grantees generally maintained asset inventory lists, timely and consistent audits of authorized devices were not in place.

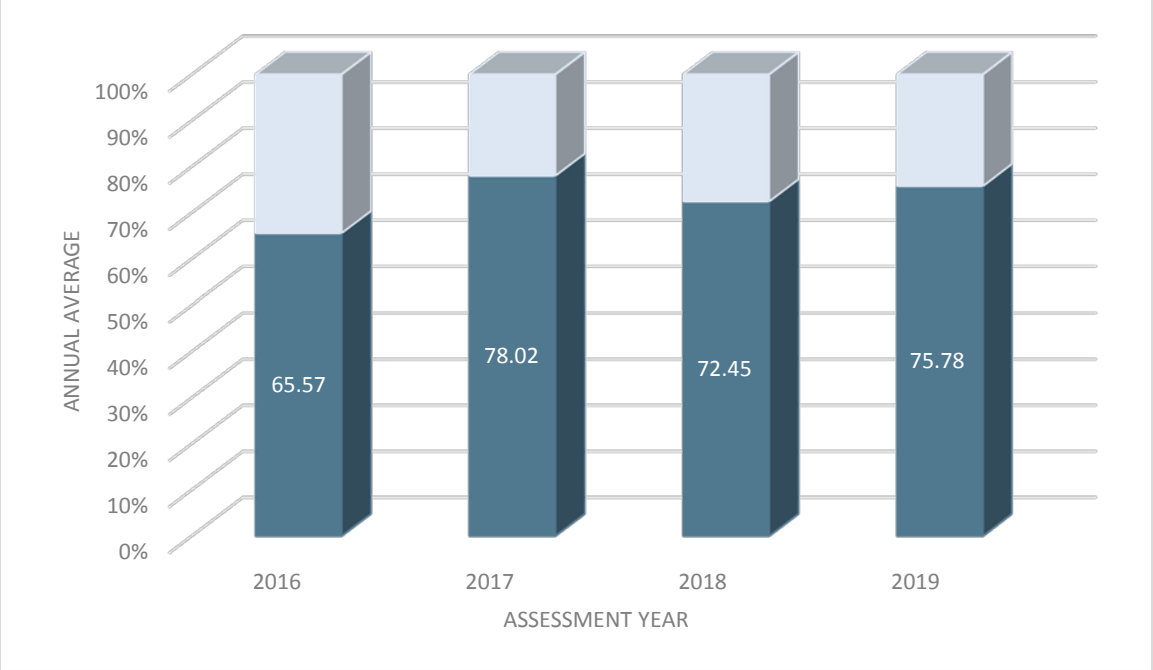


**Figure 2: Annual Assessments Comparison**

# 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 3**.

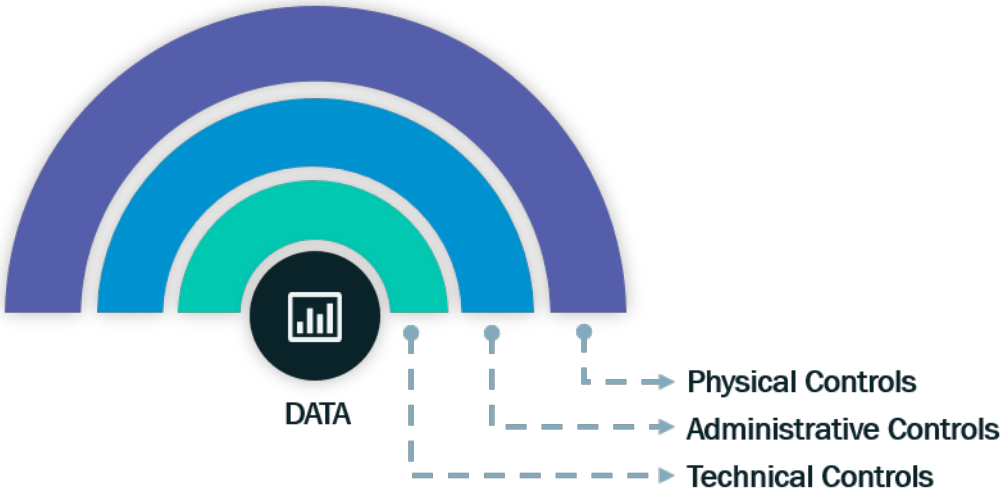


**Figure 3: Layered Defense In-Depth Protection**

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 and server rooms 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

- If BYODs are allowed on the network, ensure they are logically separated from your network domain resources or that proper security controls are in place. This can be achieved through a variety of solutions, such as:
    - Only allowing BYODs on a "Guest" network
    - Logically separating BYODs from the rest of your network
    - Implementing a Mobile Device Management Technology (MDMT) solution
    - Enacting Network Access Controls (NACs) to ensure all software is updated before access is granted
- 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 devices on 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 towards 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 |
|---|---|
| BYOD | Bring Your Own Device |
| EVAT | ECS Federal Vulnerability Assessment Team |
| IaaS | Infrastructure as a Service |
| IT | Information Technology |
| LSC | Legal Services Corporation |
| MAC | Media Access Control |
| MDMT | Mobile Device Management Technology |
| MITM | Man-in-the-Middle |
| NAC | Network Access Control |
| NLA | Network Level Authentication |
| OIG | Office of Inspector General |
| OS | Operating System |
| PII | Personally Identifiable Information |
| POC | Point of Contact |
| RDP | Remote Desktop Protocol |
| RDS | Remote Desktop Services |
| SaaS | Software as a Service |
| SMTP | Simple Mail Transfer Protocol |
| SQL | Structured Query Language |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| VPN | Virtual Private Network |
| WEP | Wired Equivalent Privacy |
| WPA-2 | Wi-Fi Protected Access 2 - Pre-Shared Key |
| WSUS | Windows Server Update Services |

**Table 2: Acronyms**