Office of Inspector General
Legal Services Corporation
3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660
www.oig.lsc.gov

FRAUD CORNER
23-0089-A-FA

TO: Executive Directors

FROM: Roxanne Caruso
Acting Inspector General

DATE: March 13, 2023

SUBJECT: Personally Identifiable Information

Introduction

In a continuing effort to assist grantees and subgrantees in preventing cyber threats, the Office of Inspector General (OIG) for the Legal Services Corporation (LSC) is providing the following guidance to assist grantees in protecting personal data from a cyber-attack. Specifically, the OIG is providing this guidance to help enhance the security of electronically shared personally identifiable information (PII). PII includes information such as name, address, social security number, birth date, bank account and bank routing numbers, and driver's license numbers. Much of this PII is contained in client case files.

Like all employers, LSC grantees maintain PII belonging to their employees and their immediate family members, and as legal service providers, LSC grantees maintain extensive PII for clients. As a result, grantees must ensure that they have mechanisms in place to protect all PII from internal and external threats. In addition, grantees must ensure that they have a response plan in place if a breach of their systems results in the release of PII.

A breach of systems, files, or unintended sharing of PII could result in many damaging effects, including financial loss, identity theft, weakening client confidence and diminished grantee reputation. Between 2020 and 2022, the OIG hotline received information that LSC grantees were victims of nine ransomware attacks resulting in the breach or attempted breach of PII. These numbers may be even higher than those reported above, as some attempts and attacks go unreported.

LSC Requirements and Guidance Related to PII

Due to the large amount of PII stored within grantee databases and systems, LSC is invested in safeguarding those systems and has provided guidance related to protecting this information. The LSC Case Service Report (CSR) Handbook[1], requires grantees to request and record sensitive PII client information, such as financial information, and information related to legal issues. The OIG suggests that grantees adopt sufficient policies and oversight practices that ensure the security of client information from internal and external threats.

LSC requirements involving client PII can also be found within LSC performance area 4, criteria 3 and the new LSC Financial Guide. Criteria 3 seeks to ensure the program has a proper written Information Technology (IT) security program to include robust IT security policies and procedures regarding protecting client and case data. Additionally, the criteria questions whether the grantee has security policies and procedures for protecting client and case data, sensitive personal and personnel data, and all communications from loss or unauthorized intrusion.

Section 2.5.3 of the new LSC Financial Guide requires grantees to establish policies that specifically address cybersecurity and the risks from cyber incidents such as data breaches, business interruption, and network damage. One of the cyber incident examples provided is unauthorized access and/or disclosure of PII. LSC recommends grantees obtain guidance from qualified experts in data and records security, including cybersecurity.

How to Protect PII

The Cybersecurity and Infrastructure Security Agency (CISA) released a fact sheet related to protecting PII.[2] CISA recommends that organizations:

1. Know what personal and sensitive information is stored on your systems and who has access to it. Limit the data by only storing information you need for business operations. Ensure data is properly disposed of when no longer needed.

---

[1] See Part 1611, Client Eligibility, and Chapter III of the LSC Case Service Report (CSR) Handbook

[2] "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches." *Cybersecurity & Infrastructure Security Agency*, www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf. Accessed 21 Feb. 2023

2. Implement physical security best practices. CISA recommends visiting Federal Trade Commission (FTC): Protecting Personal Information: A Guide for Business and FTC: Security for Small Business
3. Implement cybersecurity best practices by:
    a. Identifying the computers or servers where sensitive personal information is stored. Note: Do not store sensitive or personal data on internet-facing systems or laptops unless it is essential for business operations. If laptops contain sensitive data, encrypt them and train employees on proper physical security of the device.
    b. Encrypt sensitive information at rest and in transit.
    c. Implement firewalls to protect networks and systems from malicious or unnecessary network traffic.
    d. Consider applying network segmentation to further protect systems storing sensitive or personal information.
4. Ensure your cyber incident response and communications plans include response and notification procedures for data breach incidents. Ensure the notification procedures adhere to applicable state laws. (Refer to the National Conference of State Legislatures: Security Breach Notification Laws for information on each state's data breach notification laws.)

For additional information on protecting PII, CISA recommends FTC: Start with Security: a Guide for Business.

For additional cybersecurity resources, please refer to the OIG's cybersecurity site found here.

If you have any questions or would like additional information about this or any other fraud prevention article, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 295-1651, or by email at dorourke@oig.lsc.gov.

If you would like to stay current with our most recent alerts and advisories, please follow the directions on our homepage, "Sign Up for Email Updates" to subscribe to the LSC OIG website.