Office of Inspector General
Legal Services Corporation

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

FRAUD CORNER

TO: LSC Grantee Executive Directors, Chief Fiscal Officers, and Board Chairs

FROM: Daniel O'Rourke *Daniel O'Rourke*
Assistant Inspector General for Investigations

DATE: May 5, 2022

SUBJECT: FBI Warns "Ransomware Attacks Straining Local US Governments and Public Services"

As part of its Fraud Corner Series, the Office of Inspector General (OIG) is providing Legal Services Corporation (LSC) grantees with the following information and resources relating to ransomware attacks.

On March 30, 2022, the Federal Bureau of Investigation (FBI) warned local governments and public services of continued ransomware attacks that have resulted in a disruption of operational services, risks to public safety, and financial losses. The FBI urges local governments and public services to take steps to prevent and recover from ransomware attacks. The OIG also believes that ransomware has been and will continue to be a threat to LSC grantees. As a result, the risks identified by the FBI in the Private Industry Notification (PIN) apply equally to other organizations such as nonprofit businesses. Please review this alert and the FBI warning to ensure that your program has taken the steps necessary to minimize operational disruptions in the event of a ransomware attack.

Link to FBI Warning - PIN: 220330.pdf (ic3.gov)

The FBI PIN alerts local governments and public services of the top three origins of ransomware infections in 2021 occurred from phishing emails, remote desktop protocol exploitation, and software vulnerability exploitation.

The FBI PIN highlights the importance of initiating a proactive contingency plan. The contingency plan allows for operational continuity if systems become inaccessible due to a ransomware attack. "For example, re-routing emergency communications of local dispatch centers, alternative communication mechanisms for residents and personnel (if systems typically rely on electronic communications or VoIP), or alternative methods to conduct administrative services (such as bill pay, reporting on utility issues, etc.)."

In addition to a proactive contingency plan, the FBI PIN provides the following recommendations to prevent ransomware attacks from disrupting your services (please review the PIN for additional details related to each of these recommendations):

- Keep all operating systems and software up to date.
- Implement a user training program and phishing exercises.
- Require strong, unique passwords for all accounts with password logins.
- Require multi-factor authentication (MFA).
- Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration.
- Ensure all backup data is encrypted.
- If you use Remote Desktop Protocol (RDP) or other potentially risky services, secure and monitor them closely.
- Protect cloud storage by backing up to multiple locations, requiring MFA for access, and encrypting data in the cloud.
- If using Linux, use a Linux security module (such as SELinux, AppArmor, or SecComp) for defense in depth.
- Segment networks.
- Enforce principle of least privilege through authorization policies.
- Implement time-based access for privileged accounts.
- Disable unneeded command-line utilities; constrain scripting activities and permissions, and monitor their usage.
- Reduce credential exposure.
- Implement end-to-end encryption.
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network-monitoring tool.
- Document external remote connections.
- Collect telemetry from cloud environments.

The FBI urges businesses to report ransomware incidents as soon as possible to your local FBI field office, www.fbi.gov/contact-us/field-offices.

In addition, the OIG encourages grantees to report incidents of cybercrime to the FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/.

In addition, under LSC Grant Terms and Conditions (17), grantees must notify the LSC OIG Hotline within two business days of discovering that you have been the likely victim of a cyber incident.

Prior OIG warnings on ransomware attacks against grantees:

Hotline Advisory: Recent Phishing and Ransomware Attacks (July 13, 2021).

Hotline Advisory: Grantee Mitigates Impact of a Ransomware Attack (May 06, 2021).

Fraud Alert: Ransomware Attacks Fraud Alert (October 02, 2020).

If you have any questions or would like additional information about this or any other Fraud Corner 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.