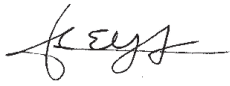




## **FRAUD ADVISORY 24-0045-A-FA**

**TO:** Executive Directors and Board Chairs

**FROM:** Thomas E. Yatsco  
Inspector General 

**DATE:** February 5, 2024

**SUBJECT:** CISA Alerts Can Help Legal Aid Organizations Prevent Cyberattacks

---

- The Cybersecurity & Infrastructure Agency (CISA) is a resource for learning about vulnerabilities to your information technology (IT) systems.
- CISA issues news alerts on imminent cybersecurity threats and ways to defend against them.
- The Legal Services Corporation (LSC) Office of Inspector General (OIG) urges your IT Departments to sign up to receive alerts from CISA.

Ransomware and other cyberattacks pose significant threats to the LSC grantee community. To assist LSC grantees and subgrantees in detecting and preventing these threats, the OIG encourages grantee IT departments to subscribe to CISA's email updates. CISA's notifications provide information about the most up-to-date security threats and solutions, such as recommended security patches.

We have seen examples of serious cyberattacks involving LSC grantees. Recently, an LSC grantee was the victim of a ransomware attack involving a virus named "Akira." This virus penetrated the grantee's network and halted its operations for multiple weeks. Prior to this attack, CISA had issued an alert on this specific virus and offered a solution to safeguard IT systems. It is possible, had the grantee received this CISA alert, they could have taken corrective action (completed security

---

patches) to prevent this virus from corrupting their network and temporarily hindering their ability to provide services to their clients. If your organization contracts with a managed IT service provider, you may consider asking if they subscribe to the CISA alerts. If they do not, suggest they do so.

The Joint Ransomware Task Force, co-chaired by CISA and the Federal Bureau of Investigation recommends<sup>1</sup> that by “engaging with peer organizations and CISA, IT departments will receive critical and timely information and access to services for managing ransomware and other cyber threats.”

### **How to Subscribe to CISA Alerts**

CISA alerts may prove invaluable to your organization’s cyberattack prevention efforts. If you do not already do so, it is highly recommended that all grantee IT departments subscribe to CISA vulnerability alerts by clicking [here](#).

### **Questions and Contacts**

If you have any questions or would like additional information about this or any other issue, please contact Daniel O’Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 441-9948 or by email at [dorourke@oig.lsc.gov](mailto:dorourke@oig.lsc.gov).

### **Sign Up for LSC OIG Alerts & Advisories**

If you would like to stay current with our most recent OIG fraud alerts and advisories, please follow the directions on our homepage at <https://oig.lsc.gov/>, see “Sign Up for Email Updates” to subscribe to new LSC OIG website postings.

---

<sup>1</sup> [https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3\\_1.pdf](https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf)