OFFICE OF INSPECTOR GENERAL
LSC America's Partner for Equal Justice
LEGAL SERVICES CORPORATION

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

**FRAUD ADVISORY**
**24-0143-A-FA**

**TO:** Executive Directors and Board Chairs

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

**DATE:** August 7, 2024

**SUBJECT:** Mitigating the Growing Risk of Cyber Attacks: New Guidance to Help Nonprofits

---

# How to Protect Your Legal Aid from Cyber Attacks

- We are making you aware of new guidance that could help your organization avoid being the victim of cyber-attacks. The Cybersecurity & Infrastructure Agency (CISA) has recently released guidance on mitigating cyber threats that is specific to civil society organizations, which include nonprofit and advocacy organizations.
- CISA, and the co-authoring agencies, provided a joint guidance report, which states that civil society organizations, including nonprofits, and their employees are targeted by state-sponsored threat actors who conduct extensive research and gather information about their potential victims to obtain login credentials, support social engineering, and use malicious software for surveillance and monitoring.
- CISA and the National Security Agency (NSA) also released five joint Cybersecurity Information Sheets (CSIs) to provide organizations with recommended best practices and mitigations to improve the security of their cloud environments.
- LSC-OIG recommends that your IT Departments review the new guidance released by CISA on Mitigating Cyber Threats with Limited Resources and the CSIs related to cloud security.

## Nonprofits Are Increasingly a Target for Cyber Attackers, but Following CISA Guidance Could Help Mitigate Your Cyber Risks

Nonprofit organizations and their staff are at an increased risk of being targeted by malicious cyber actors. The joint guide, developed as part of CISA's High-Risk Community Protection (HRCP) initiative, provides mitigation measures for nonprofit organizations to reduce their risk to common cyber threats. Recommended cyber risk prevention actions for organizations and individuals are summarized in the table below.

| | CISA Recommendations Summary |
|---|---|
| **Nonprofits** | |
| | Keep software updated on user devices and IT infrastructure. |
| | Implement phishing-resistant multifactor authentication (MFA). |
| | Audit accounts and disable unused and unnecessary accounts**.** Remove needless accounts to reduce access vectors that actors can use to get into the system. |
| | Disable user accounts and access to organizational resources for departing staff. |
| | Apply the Principle of Least Privilege and remove any unnecessary permissions or access. |
| | Exercise due diligence when selecting vendors, including cloud service providers (CSP) and managed service providers (MSP). |
| | Review contractual relationships with all service providers to ensure cybersecurity compliance. |
| | Manage architecture risks by auditing and reviewing connections between customer systems, service provider systems, and other client enclaves, such as cloud services. |
| | Use a dedicated VPN to connect to MSP infrastructure. |
| | Implement basic cybersecurity training to cover concepts such as account phishing, email and web browsing security, and password security. |
| | Develop and exercise incident response and recovery plans. |
| **Individuals** | |
| | Use strong passwords on accounts and implement MFA. |
| | Limit exposure of publicly available information, such as social media accounts. |
| | Verify contacts, be aware of social engineering, and exercise caution before clicking on links or attachments. |
| | Use encryption measures to protect communications when interacting with online services. |
| | Select apps carefully by using trusted app stores, thoroughly check app details, and developer information. |
| | Regularly review and restrict app permissions. |
| | Keep applications and OS updated. |
| | Consider rebooting your mobile device weekly. |
| | Secure browsing habits and digital footprint management to ensure privacy and online security. |

For detailed explanations related to CISA's recommendations and the additional resources provided, you may review the guide in its entirety at Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society (cisa.gov).

**Adopting Cloud Security Best Practices Should Be Considered**

CISA and NSA address the following cloud security topics in their recently released CSIs, which can be found in their entirety here.

- Use Secure Cloud Identity and Access Management Practices
- Use Secure Cloud Key Management Practices
- Implement Network Segmentation and Encryption in Cloud Environments
- Secure Data in the Cloud
- Mitigate Risks from Managed Service Providers in Cloud Environments

For additional cybersecurity resources, please refer to the OIG's cybersecurity site, which includes a cybercrimes fraud awareness presentation and a multitude of cybercrimes prevention resources and articles. We also encourage you to share this advisory broadly within your organization—particularly your IT staff or contractors— and within your professional network.

**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.

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

If you would like to stay current with our most recent 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.