

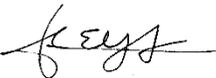


Office of Inspector General
Legal Services Corporation

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660
www.oig.lsc.gov

FRAUD ADVISORY **23-0214-A-FA**

TO: Executive Directors and Board Chairs

FROM: Thomas E. Yatsco 
Inspector General

DATE: September 28, 2023

SUBJECT: Grantees Should Consider Establishing Cyber Incident Response Plans

Introduction

As the digital landscape evolves and malevolent cyber actors continue to proliferate, the Legal Services Corporation (LSC) and its grantees are increasingly vulnerable to cyber threats. Since 2018, LSC and its grantees have been the victims of at least 48 cyberattacks, some of which resulted in monetary losses and compromised data. To mitigate the impact of a cyber incident, we strongly urge grantees to establish a comprehensive Cyber Incident Response Plan (CIRP). By developing and implementing a comprehensive CIRP, grantees can mitigate the impact of security breaches, protect sensitive data, and prevent potential losses, including loss of confidence by external stakeholders and clients.

In a continuing effort to assist grantees and subgrantees in proactively mitigating risks and preventing fraud and destructive cyber incidents, the Office of Inspector General (OIG) for LSC is providing the following guidance related to the process of establishing an effective CIRP to safeguard your operations and reputation. In addition to the guidance below, the OIG maintains an ongoing OIG Information Technology Vulnerabilities Assessment program.¹ The OIG also offers multiple cyber security prevention resources on its webpage found [here](#).

¹ The Information Technology Vulnerabilities Assessment tests for potential vulnerabilities in computer network architecture, technologies, and processes.

Cyber Incident Response Plans: LSC Guidance for Grantees

[Section 3.9 of the updated LSC Technology Baselines](#) urges grantees to implement an incident response plan before the organization becomes a victim of a cybersecurity incident. The incident response plan should include:

- information detailing roles and responsibilities of staff,
- reporting requirements, and
- communication strategies.

Incident response testing should take place at least once every year with simulated incidents to ensure that the plan remains effective. LSC notes that the plan typically includes procedures for detecting and analyzing different types of security incidents, as well as the systems and data that may have been compromised.

Steps for Creating a Cyber Incident Response Plan

Guidance from the Cyber Security and Infrastructure Security Agency (CISA), the Federal Trade Commission (FTC), and the National Institute of Standards and Technology (NIST) suggest, at a minimum, organizations should follow these steps when creating a CIRP:

1. Conduct a thorough assessment of your program's digital infrastructure. Identify critical systems, valuable data, and potential vulnerabilities. This includes identifying where any employee or client personally identifiable information (PII) may be stored.
2. Assemble a cyber incident response team responsible for managing cyber incidents. Include individuals with expertise in IT, legal matters, public relations, as well as senior management. The plan should assign specific roles and responsibilities to each team member to ensure clear lines of communication and efficient decision-making during an incident. The outcome of a cyber incident often depends on the ability to act immediately.
3. Develop a CIRP that outlines the step-by-step procedures to be followed in the event of a cyber incident. Key components of the plan should include:
 - A process for detecting and reporting cyber incidents promptly. You should encourage employees to report cyber incidents and related suspicious activity to your Information Technology Department, the Executive Director, law enforcement, the OIG hotline, and your cyber insurance company. Please be reminded that LSC Grant Terms and Conditions require a grantee to notify the LSC OIG Hotline within two business days of discovering they have been the victim of a cyber incident.

- Protocols for containing the incident to prevent further damage and mitigating the immediate impact. This may include isolating affected systems, disabling compromised accounts, or blocking unauthorized access.
 - Procedures for collecting and preserving evidence related to the incident to assist in the forensic investigation. You could contract with experts if necessary to conduct a thorough forensic investigation to determine the extent of the breach and identify potential vulnerabilities. Cyber insurance often covers the cost of these investigations.
 - Guidelines for communicating with external entities and individuals, including donors, partners, clients, and regulatory bodies. You should ensure that you are following your state’s data breach notification laws. A good resource to identify those requirements can be found at [Security Breach Notification Laws \(ncsl.org\)](https://www.ncsl.org/legislation/data-breach-notification).
 - A plan for restoring systems, data, and services affected by the incident.
 - Post-incident reviews or “post-mortems” to identify weaknesses in the response plan and make necessary improvements, to include lessons learned. You should regularly update the plan to incorporate emerging threats, lessons learned, and evolving best practices.
4. Conduct regular training sessions to educate employees about cyber risks, prevention techniques, and their roles in the incident response plan. You should create and nurture a culture of vigilance and encourage employees to report any potential security concerns promptly.
 5. Establish relationships and potentially contract with external organizations, such as cyber security firms, legal experts, and law enforcement agencies. Their expertise and support can prove invaluable in addressing and mitigating the negative impacts of a cyber incident.

Where to Find Assistance to Create a Cyber Incident Response Plan

There are numerous resources available to assist grantees in creating a CIRP that is specific to their program and needs.

NIST issued guidance on incident response plan basics, including additional resources such as links to a NIST Computer Security Incident Handling Guide and a CISA cybersecurity incident and vulnerability response playbook, which can be assessed at [Incident Response Plan \(IRP\) Basics \(cisa.gov\)](https://www.cisa.gov/incident-response-plan-irp-basics).

In its guidance, NIST advises that each organization should have a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support.

The FTC also released a data breach response guide for businesses, which includes general incident response steps to follow, found at [Data Breach Response: A Guide for Business | Federal Trade Commission \(ftc.gov\)](#).

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.

Questions and Contacts

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.

Sign Up for Alerts and Advisories

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.