

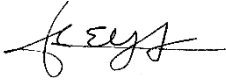


OFFICE OF INSPECTOR GENERAL
LSC | America's Partner
for Equal Justice
LEGAL SERVICES CORPORATION

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 - 00 31 - A - FA

TO: Executive Directors and Board Chairs

FROM: Thomas E. Yatsco
Inspector General 

DATE: January 18, 2024

SUBJECT: OIG Introduces a “Cyber After Incident Report Form” for LSC Grantees

NEW OIG “Cyber After Incident Report Form”

- The OIG is implementing a [“Cyber After Incident Report Form”](#) to gather more information on reported cyberattacks. The information will be used to better assist grantees with their response and recovery in the event of an attack.
 - LSC Grant Terms and Conditions require grantees to report cyber incidents to the Office of Inspector General Hotline. As a follow-up to the hotline report, the OIG will request grantees also complete the attached form when the OIG requires additional information related to the cyber incident.
 - [Cyber Security Resources | OFFICE OF INSPECTOR GENERAL](#) is available to aid grantees in preventing and responding to cyber incidents.
-

The Legal Services Corporation (LSC) Office of Inspector General (OIG) has created the OIG “Cyber After Incident Report Form” to help your organization prepare for, respond to, and recover from a cyber incident. The form is also intended to assist grantees in compiling the information necessary for a thorough report to the OIG, Federal Bureau of Investigation (FBI), and local law enforcement related to cyberattacks or threats that may have occurred at your program.

Effective planning is a critical component of an organization’s preparedness for cyber event recovery. Obtaining accurate, thorough, and timely information will help your cyber incident response team manage the cyber incident by determining the extent of the threat, mitigating the exploited weaknesses, and minimizing loss and damage in the event of an attack.

LSC Requires Grantees to Report Cyber Incidents

LSC’s 2024 Grant Terms and Conditions require grantees to report cyber incidents to the OIG within two (2) business days of discovering their organization has been the likely victim of a cyber incident. You must notify the OIG regardless of recovery of anything lost. After the initial OIG hotline report, we will provide you a link and request that you fill out the OIG “Cyber After Incident Report Form.”

The OIG remains committed to partnering with your organization in preventing cyber related incidences and threats. A timely report with thorough information may help avert further damage to your program or assist other grantees in combatting similar cyber threats.

Create Post-Incident Reports Using the “Cyber After Incident Report Form”

The attached “Cyber After Incident Report Form” seeks to assist grantees in collecting the information necessary to document the incident with the OIG and for potential reporting to the FBI and local law enforcement. Additionally, the form will assist grantees in collecting information to follow the critical lessons learned process recommended by the National Institute of Standards and Technology (NIST).¹

An important post-incident activity is to create a follow-up report for each incident, which can be used to assist in handling similar attempts or incidents. The OIG’s attached questionnaire aims to lay out the foundation for information needed to create the OIG post-incident report and ultimately assist you and other LSC grantees in preventing similar attacks. The questionnaire can be reviewed and is attached for your reference. The OIG will also use the report form to follow-up on a cyber incident hotline report.

Resources to Help Prevent and Respond to Cyber Threats and Attacks

The OIG [Cyber Security Resources webpage](#) provides OIG advisories and resources that are intended to educate grantees on the common schemes targeting LSC funded organizations and ways to detect and prevent their success. The need for awareness and education in implementing cyber

¹ National Institute of Standards and Technology. *Computer Security Incident Handbook*, § 3.4. Accessed December 15, 2023, from <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

security prevention measures is of the utmost importance and the best defense against a cyberattack that may lead to devastating consequences for your program.

The following resources provide additional information and best practices for responding to cyber incidents:

- OIG Fraud Advisory: [Grantees Should Consider Establishing Cyber Incident Response Plans](#)
- NIST Incident Handling Checklist, (See Appendix A).

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 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.

Appendix A

NIST Incident Handling Checklist

The National Institute of Standards and Technology (NIST) checklist provides the major steps to be performed in the handling of an incident. NIST notes that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

	Action	Completed
Detection and Analysis		
1	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc)	
3	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4	Acquire, preserve, secure, and document evidence	
5	Contain the incident	
6	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8	Create a follow-up report	
9	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	



OIG “Cyber After Incident Response Form”

The **OIG** is implementing a “**Cyber After Incident Report Form**” to gather more information on reported cyberattacks. The information will be used to better assist grantees with their response and recovery in the event of an attack.

Directions

Please respond to the following questions related to the recent cyber incident at your program. If a question is not applicable, please answer not applicable (n/a) and if an answer is not known at the time of this report, please answer unknown and provide an explanation if relevant.

General Information

1. Please provide the name of the program, a point of contact, and contact information.
2. What type of cyberattack affected your program?
 - a. Ransomware
 - b. Business Email Compromise Scheme
 - c. Other Type of Cyberattack
 - d. Unknown

Detection of Incident

3. Exactly what happened?
4. How did the program learn that an incident had occurred?
5. Did the cyberattack use email to cause or attempt to cause the diversion of a financial transaction (Business Email Compromise (BEC) scheme)?
6. Briefly describe how email was used in the BEC attack.
7. If funds were diverted, how much?
8. Was email used in the cyberattack for another purpose? Please explain.
9. Provide a timeline of known events that occurred during the cyberattack.

Program Analysis of Incident

10. Briefly explain what the program discovered about the cyberattack, such as what tools were used to gain access.

11. Has the program identified and preserved evidence related to the attack (such as emails or other types of communication and/or evidence of intrusions)?
12. If known, who are the potential suspects?

Containment, Eradication, and Recovery

13. Did the cyberattack compromise the program's network/data?
 - a. Yes
 - b. No
 - c. Unknown
14. If yes:
 - a. What data was exposed or accessed?
 - b. Were any systems infected with malware?
 - c. Have infected systems been remedied?
 - d. Has a ransom payment been requested by the malicious actor?
 - e. Was any Personally Identifiable Information (PII) accessed?
15. If it is unknown whether the cyberattack compromised the program network/data, please explain whether the program plans to take steps to determine whether there was a network intrusion etc.

Post-Incident Activity

16. Did the program implement its cyber incident response plan (CIRP) as a result of the attack? (Please explain why or why not the CIRP was implemented).
17. Did the program contact its cyber insurance provider as a part of the attack?
18. What services did your cybersecurity insurance carrier provide to aid in the containment, eradication and recovery?
19. Did the program report the incident to the appropriate internal personnel and external organizations (law enforcement, FBI etc.)?
20. Is the program taking any follow-up steps to ensure that the program's network and financial accounts are secure?
21. Is the program taking any follow-up measures to help prevent similar future attacks?
22. Has the program identified weaknesses in their systems or response plan and made any necessary improvements? If so, what actions were taken.
23. What are some lessons learned from the cyber incident?