

Example Reporting Template

<Organization Name> Incident Reporting Template

Source: <https://www.cisa.gov>

Date: _____ Name of the individual: _____

Completing this form: _____ Tracking number: _____

Incident Priority

<input type="checkbox"/> HIGH	<input type="checkbox"/> MEDIUM	<input type="checkbox"/> LOW	<input type="checkbox"/> OTHER
<i>Additional Notes:</i> 			

Incident Type

Check all that apply.

<input type="checkbox"/> Compromised System	<input type="checkbox"/> Lost Equipment/Theft
<input type="checkbox"/> Compromised User Credentials (e.g., lost password)	<input type="checkbox"/> Physical Break-in
<input type="checkbox"/> Network Attack (e.g., DoS)	<input type="checkbox"/> Social Engineering (e.g., Phishing)
<input type="checkbox"/> Malware (e.g., virus, worm, Trojan)	<input type="checkbox"/> Law Enforcement Request
<input type="checkbox"/> Reconnaissance (e.g., scanning, sniffing)	<input type="checkbox"/> Policy Violation (e.g., acceptable use)
	<input type="checkbox"/> Unknown/Other (Please describe below.)
<i>Incident Description Notes:</i> 	

Incident Timeline

Please provide as many details as possible.

A. Date and time when the incident was identified	
B. Date and time when the incident was notified	
C. Date and time when the incident occurred	
<i>Additional timeline details:</i>	

Incident Scope

Please provide as many details as possible.

A. Estimated quantity of systems affected	
B. Estimated quantity of users affected	
C. Third parties involved or affected (e.g., vendors, contractors, partners)	
<i>Additional scoping information:</i>	

Systems Affected by the Incident

Please provide as many details as possible.

A. Attack sources (e.g., IP address, port)	
B. Attack destinations (e.g., IP address, port)	
C. IP address of the affected systems	
D. Primary functions of the affected systems (e.g., web server, domain controller)	
E. Operating systems of the affected systems (e.g., version, service pack, patch level, configuration)	
F. Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)	
G. Physical location of the affected systems (e.g., state, city, building, room, desk)	
<i>Additional details:</i>	

Users Affected by the Incident

Please provide as many details as possible.

A. Names and job titles of the affected users	
B. System access levels or rights of the affected users (e.g., regular user, domain administrator, root)	
<i>Additional user details:</i>	

PII Breach Information

Check all that apply.

A. Was any personal identifiable information affected? If yes, then check the options below.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<input type="checkbox"/> Name <input type="checkbox"/> Financial Account Number <input type="checkbox"/> Social Security Number	<input type="checkbox"/> Driver's License <input type="checkbox"/> Medical Information <input type="checkbox"/> Others, Specify _____
<i>Other PII details:</i> 	

Please provide as many details as possible.

A. Is there any requirement of privacy disclosure notice? If yes, then include a sample notification	
B. Estimated quantity of individuals affected	
C. Dates of the notification(s)	
<i>Additional notification details:</i> 	

Incident Handling Log

Please provide as many details as possible.

A. Actions taken to identify the affected resources	
B. Actions taken to remediate the incident	
C. Actions planned to prevent similar incidents	
<i>Additional remediation details:</i>	

Incident Reporting Information

Complete this section if the incident report was system generated.

A. Software package	
B. Host ID and location	
<i>Additional system information:</i>	

Complete this section if an incident report was submitted by an individual.

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Email address	
<i>Additional contact information:</i>	

Incident Contact Information

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of the affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of the affected systems (e.g., state, city, building, room, desk)	