FL [DIGITAL SERVICE]

Cybersecurity After-Action Report

Per Florida Statutes Section 282.318 and 282.3185; State agencies and local governments must submit to FL[DS], within 1 week after the remediation of a cybersecurity or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained because of the incident.

1. Reporting Party Contact Information			
Entity Name:		**Alternate Contact Name:**	
Primary Contact Name:		**Alternate Contact Phone:**	
Primary Contact Phone:		**Contact Email(s):**	

2. Incident Summary			
Report Date:		**Report Method:**	
Incident Level:			

Incident Type (Check all that Apply)			
☐	Account/Credentials Compromised	☐	Distributed Denial of Service (DDoS)
☐	Social Engineering	☐	Loss of Sensitive Data
☐	Malware/Ransomware	☐	Loss of System Access (Availability)
☐	Loss of Equipment	☐	Network Scanning/Detection
☐	System Misuse	☐	Other (Describe Below)

Threat Actor:	☐	External	☐	Internal	☐	Partner	☐	Unknown/Other

Executive Summary, Impact, Key Findings, and Summary of Response:	

3. Incident Background: Describe the incident, list stakeholders, Law Enforcement involvement, and/or 3rd party vendors. Did the vendor play a role in the incident or its resolution. Include incident date and time, how the incident was detected, the nature of the incident, threat attack vector – do you know how the initial attack was made, and the impact to the organization's systems or data. In the case of a ransomware incident, give specific details of the ransom demanded.

4. Forensic Services: Describe what if any forensic services were utilized – i.e., FL[DS] retainer/MS-ISAC SOC/or IT department and what value the services brought to incident handling, response, analysis, or remediation efforts.

5. Timeline of Significant Events: Highlight the key events in sequence detail, including the date and time of detection, who was contacted and who received the first incident report , the nature of the incident.

6. Incident Impact: Describe in detail the event impact to the organization, such as compromised systems, data breaches (list data types – CJIS, PII, HIPAA, etc., and if exfiltration took place). Was there any reputational, regulatory, legal and/or compliance implications.

7. Root Cause Analysis (RCA): Describe any analytical findings that might identify the root causes and/or contributing factors. This may include vulnerabilities, misconfigurations, human error, or external threats. Include recommendations for addressing these root causes.

8. Indicators of Compromise: Describe any digital information clues which might help identify, detect, diagnose, halt and/or remediate malicious threat actor activities such as: Malicious IPs, Curl Commands, Web Shells, etc.

9. Containment Eradication & Recovery: Describe in detail the strategies employed for containment, eradication, and recovery efforts. Also include the status of backups, whether the backups were affected and the expected vs. actual organization recovery times.

10. Response Effectiveness: Evaluate the effectiveness of the incident response efforts, including the strengths and weaknesses of the response team, processes, and technologies utilized. Identify any areas that require improvement and propose remediation measures.

11. Financial Impact: Provide the financial impact from your organization's Cyber event/incident. Include the return-on-investment from your current in-place security controls and/or any financial losses incurred. Provide detail on costs associated with response, recovery, legal consultations, reputation management, and other direct or indirect costs.

Financial Impact:	☐	High	☐	Medium	☐	Low	☐	Unknown/Other
Impact Summary:								

12. Lessons Learned / Recommendations: Provide any information that could help other teams faced with a similar situation navigate their incident response - how well did staff and management perform? Could more training affect the outcome? Will training be revised? Was the escalation process executed properly? Were documented procedures followed and were they adequate. What information was needed sooner? Would more detailed system logging, for example, help in scoping RCA? What additional tools or resources are required to better detect, analyze, and mitigate future incidents? Were there any communication gaps and how can they be improved?

13. Conclusion, resolution and/or Additional Information: