Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

Cybersecurity Incident Reporting Requirements for Public Utilities

Table of Contents

Revision History

Version	Date	Description of Changes
0.1	July 14, 2023	Initial Version
0.2	September 13, 2023	Updates from PSC Collaboration
0.3	September 15, 2023	SCISO feedback incorporated
0.4	September 28, 2023	DoIT legal review / Utility feedback incorporated
1.0	November 10, 2023	Release reviews completed and document published

Approval

Katie Savage -DoIT- (Nov 14, 2023 10:14 EST)

Secretary
Maryland Department of Information Technology

Introduction

Pursuant to the requirements of Md. Code, State Public Utilities Article § 5-306(D)(2) the State Chief Information Security Officer (SCISO), in consultation with the Public Service Commission, is required to establish criteria for a public service company to report cybersecurity incidents. The law compels the SCISO to set criteria for:

- The criteria for determining the circumstances under which a cybersecurity incident must be reported;
- The manner in which to report; and
- The time period within which a report must be made to the Maryland Security Operations Center (MD-SOC)

Cybersecurity incidents are generally defined as an event that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[1]

The Office of Security Management uses the MITRE ATT&CK[2] Framework to support consistent description of, and communication regarding, the tactics, techniques, and software that are used by threat actors to achieve their objectives. For clarity, MITRE ATT&CK tactics and techniques will be displayed in **”bold”** and within double quotations throughout this document.

The reporting process described herein satisfies the legal requirements to report to the Maryland Department of Information Technology and the Maryland Public Service Commission. This reporting process does not satisfy any other reporting required by law or statute.

Critical Energy/Electric Infrastructure Information (CEII) specified in 18 C.F.R. § 388.113 should be redacted in the report to the MDSOC. Representatives from the Maryland Public Service Commission will contact the reporting utility for this information if required.

[1] See 44 U.S. Code § 3552(b)(2)

[2] http://attack.mitre.org/

<u>Nothing within this document should be construed as a prohibition against, or discouragement of, reporting potential or suspected cybersecurity incidents, regardless of whether they meet the thresholds described below.</u>

<u>Even when not compulsory, voluntary reporting of cybersecurity incidents is encouraged.</u>

The MD-SOC and the Maryland-Information Sharing and Analysis Center (MD-ISAC) are available 24/7/365 to aid in identifying cybersecurity incidents and ensuring that resources are available to minimize the impact of cybersecurity incidents.

Reporting Criteria

A public service company <u>must</u> report any cybersecurity incident that results in:

- **“Impact”**, such as:
    - The potential of, or confirmed, unauthorized access to, or modification or deletion of data, regardless of whether the organization was able to recover or restore data.
    - The disruption of a business function resulting from a denial-of-service attack.
- “**Exfiltration**”, including:
    - Unauthorized access to, or acquisition of, non-public data, regardless of whether the **“Exfiltration”** can be confirmed or is merely suspected.
    - **“Exfiltration”** includes the identification of non-public data attributable to your organization in a forum (e.g., pastebin, darkweb) inconsistent with the expected handling of that data.

Additionally, a public service company <u>must</u> report the discovery or detection of:

- Techniques and software similar to those described in the MITRE ATT&CK Framework “**Command and Control**” tactic, regardless of whether the source or nature of the “**Command and Control**” activity can be correlated to related ATT&CK phases or other potentially malicious activity.
- Direct or circumstantial evidence indicating a threat actor is engaged in the “**Collection**” tactic, such as:

    - Collections of non-public files stored in a manner inconsistent with normal operations.
- Techniques, software, activity, logs, files, or other artifacts that would indicate unauthorized behavior consistent with the following tactics:
    - "**Persistence**"
    - "**Lateral Movement**"
    - "**Discovery**"
    - "**Credential Access**"
    - "**Defense Evasion**"
    - "**Privilege Escalation**"
- Techniques, software, logs, files, or other artifacts consistent with the "**Execution**" tactic, unless there is evidence that protective controls were successful in preventing the attempted attack from progressing to a subsequent tactic.
- Techniques, software, logs, files, or other artifacts consistent with the "**Initial Access**" tactic, unless there is evidence that protective controls were successful in preventing the attempted attack from progressing to a subsequent tactic.

The SCISO encourages companies to report activity, including Indicators of Attack (IOAs) and Indicators of Compromise (IOCs) to the MD-ISAC that are associated with the **"Reconnaissance," "Resource Development," "Initial Access," and "Execution"** tactics, because this information can help to protect other units, including local governments and other State partners.

Manner of Reporting

Cybersecurity incidents must be reported to the following, in the following ways:

- State Security Operations Center (MD-SOC) by either (in order of preference):
    1. Using the incident reporting form at https://doitmaryland.service-now.com/cybersecurityincident/
    2. Sending an email with the information below to soc@maryland.gov
    3. Calling the Service Desk at 410-697-9700

Reports should include, at a minimum, the following information:

- Organization Name
- Reporter's name, title, email address, mobile phone, and office phone
- Date and time of incident detection

- Detection method (e.g., user reported, system alert/detection, logs)
- Investigation results (description of activity, impact, and results)
- Indicators of Compromise (IP Addresses, Domains, Network Traffic Abnormalities, Database or File Read/Write Activity, DNS Requests, etc.)
- Indicators of Attack
- Vendor Impacted
- Utility impacts of breach
- Operational Controls Impacted
- Number of Records Impacted, if data was exfiltrated, damaged, destroyed, or encrypted
- Privacy Impact (Did the records contain PII, PHI, CJIS, PCI, FTI, CEII or other regulated data types)?
- Network Impacted (On-Premise Network, Partner Network, Cloud-hosted Network owned by organization such as AWS, Azure, Google, SaaS/PaaS Provider, Vendor's Network)
- Evidence that incident is a "true positive"
- Status and phase of incident (continuing investigation, containing, eradicating, recovering, unsure)
- Impacts to critical infrastructure of systems affecting public health and safety, reliability or the environment
- Impact to business operations, internal users, or public users
- Mitigation Activity: What actions has your organization taken to respond to, contain, eradicate, and recover from the incident?
- Current and Planned Notifications: What notifications has your organization provided or does your organization plan to provide to internal or external parties?
- Any additional information material to the incident and the response

Timing of Reporting

Reports to the MD-SOC must be made as soon as practicable, but not later than twenty four (24) hours after confirmation of a detected cybersecurity incident. If an organization is unsure whether an event constitutes a reportable cybersecurity incident and is actively investigating the circumstances, it may make a preliminary report while working to conclusively determine whether a reportable cybersecurity incident occurred. If, during the course of its investigation, the organization confirms that a reportable cybersecurity incident has not occurred, the MD-SOC will review and close the report without additional action. Generally, you should not wait for absolute confirmation that a cybersecurity incident has occurred before reporting because any delay may affect the ability to take preventative and remedial measures to protect information or reduce the risk of harm.

Disclosure of cybersecurity incident reports

Consistent with the requirements described in Md. Code, State Fin. & Proc. § 3.5-2A-04, the Office of Security Management (OSM) must develop a report on the activities of the Office and the state of cybersecurity preparedness in Maryland, including “the activities and accomplishments of the Office during the previous 12 months at the State and local levels.” This report may include high-level details about the incident.” Additionally, aggregate data regarding incidents may be shared.

Consistent with the limitations established in MD Code, Gen Provisions § 4-338, the OSM **must** deny requests to inspect records related to incident reports when they contain information about the security of an information system. Because incident reports would necessarily contain information about system vulnerabilities, the OSM will deny requests to inspect these records.

Consistent with the requirements established in Md. Code, State Gov't § 2-1226, information obtained by the Office of Legislative Audits (OLA) is generally protected from disclosure. Additionally, if the information obtained will be included in a public audit report, per the requirements described in Md. Code, State Gov't § 2-1224, cybersecurity findings must be redacted from the public report in a manner consistent with auditing best practices.

Appendix A - Examples of Incidents

Scenario 1 - Operational Technology Default Credentials

A network administrator is reviewing external access control lists and realizes that a recent change has allowed access to the management interface of an Operational Technology device from the general internet. While access logs for the management interface are not available, the network administrator realizes that this asset uses default credentials published by the vendor and available to the general public.

The organization is ***required*** to report this incident. While “**Initial Access”** activity is not always a required reporting event, in this case it is not possible to know if an adversary exploited this vulnerability because logging does not exist. There is a reasonable suspicion that given the exposure of the interface and the known credentials that an adversary may have gained initial access.

Scenario 2 - Phishing

A user receives an email indicating that their email password is about to expire and clicks on the link to reset their password. After clicking the link they enter their username and password but the website tells them to try again later. They recognize that they were likely the victim of a phishing attack and report the incident to the service desk, who resets their password, but not before the threat actor unsuccessfully attempts to log into the email service.

The organization is ***required*** to report this incident. The user was successfully phished, while the threat actor could not gain initial access, password reuse warrants a log review and analysis to determine no other activity can be attributed to the event. The organization ***should*** provide the following IOAs and IOCs to the MD-SOC:

- From the email:
  - Sender email address
  - Sender subject line
  - Message Contents
  - Full Message Headers
- From the phishing website
  - URL (website name)
  - IP addresses associated with the website

    - Contents of the website, including file hashes
- From the Attempted login
    - IP address used for the attempt to gain unauthorized access

Scenario 3 - Potential Evidence of Compromise

While conducting troubleshooting of the antivirus service, the IT manager notices a file named mimikatz.exe on the server desktop. Neither the IT manager nor the server administrator is aware of how the file was placed on the system. The IT manager immediately disconnects the computer from the network and confirms that the file does not exist on any of the organization's other computers. No logs indicate unusual behavior, nor was any other suspicious activity detected.

The organization is ***required*** to report this incident. The presence of the mimikatz executable is inconsistent with normal IT operations and likely indicates unauthorized activity consistent with **"Credential Access."**

Appendix B - COMAR Definitions

“Cybersecurity breach” means any unauthorized act that has been confirmed to result in access to acquisition, control, destruction, disclosure, or modification of a utility’s information technology systems, operations technology systems, or smart grid systems.

“Information technology system” means hardware and software related to electronic processing, and storage, retrieval, transmittal, and manipulation of data.

“Operations technology system” means a system or network that monitors or controls electric, gas, or water system infrastructure used for utility operations.

“Smart grid system” means a system or network that enables a utility to gather and store personally identifiable customer information from customer devices or allows for the control of customer devices.

“Utility” means any electric company, gas company, or water company regulated by the Public Service Commission.

Cybersecurity Requirements - Cybersecurity Incident Reporting Requirements for Public Utilities

Final Audit Report 2023-11-14

Created:	2023-11-14
By:	maria fisher (maria.fisher2@maryland.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAuExTp7ooMHwC1uZwA5Lag_1yTXVkgspc

"Cybersecurity Requirements - Cybersecurity Incident Reporting Requirements for Public Utilities" History

Document created by maria fisher (maria.fisher2@maryland.gov)
2023-11-14 - 1:03:23 PM GMT

Document emailed to Katie Savage -DoIT- (katie.savage@maryland.gov) for signature
2023-11-14 - 1:03:53 PM GMT

Email viewed by Katie Savage -DoIT- (katie.savage@maryland.gov)
2023-11-14 - 3:14:40 PM GMT

Document e-signed by Katie Savage -DoIT- (katie.savage@maryland.gov)
Signature Date: 2023-11-14 - 3:14:59 PM GMT - Time Source: server

Agreement completed.
2023-11-14 - 3:14:59 PM GMT