Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

Cybersecurity Incident Reporting Requirements for State Government

Table of Contents

Revision History

Version	Date	Description of Changes
1.0	October 1, 2022	Initial Version

Approval

Charles I Stewart IV __ **__10/1/2022__**

Charles “Chip” Stewart Date

State Chief Information Security Officer

Introduction

Pursuant to the requirements of Md. Code, State Finance & Procurement Article § 3.5-406(b)(2) the State Chief Information Security Officer (SCISO) must establish criteria for units of State government to report cybersecurity incidents. The law compels the SCISO to set criteria for:

- When 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)

Unit of State government (units) is defined in Md. Code, State Finance & Procurement Article § 3.5-101(f) as an agency or unit of the Executive Branch of State government.

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.

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.

Even when not compulsory, voluntary reporting of cybersecurity incident is encouraged

The MD-SOC, 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.

This document supersedes “Supplemental Guidance on Incident Reporting Requirements” version 1.0 published on February 24, 2020.

[1] See 44 U.S. Code § 3552(b)(2)
[2] http://attack.mitre.org/

Reporting Criteria

Units must report any cybersecurity incident that results in:

- **“Impact”**, such as:
    - The potential of, or confirmed, unauthorized 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, units must 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 a reasonable assurance 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 a reasonable assurance that protective controls were successful in preventing the attempted attack from progressing to a subsequent tactic.

The SCISO encourages units 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 and title, email address, mobile and office phone numbers
- Date and time of incident detection
- How was it detected; observations of what happened/is happening
- Whether the incident is confirmed or suspected
- If the cybersecurity incident is ongoing
- If any life-safety or critical infrastructure systems are impacted or suspected to be impacted
- A brief description of the business impact of the event.
- Whether the organization is requesting assistance, and the nature of the assistance requested.
- What, if any, action has been taken
- Who has been notified
- Any additional information material to the incident response

Timing of Reporting

Reports to the MD-SOC must be made as soon as practicable, but not later than one (1) hour 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 delay reporting for up to (3) hours from initial detection while working to conclusively determine whether a reportable cybersecurity incident occurred, for a total of four (4) hours between detection and reporting. If, during the course of its investigation, the organization confirms that a reportable cybersecurity incident occurred, it must immediately report the incident to the MD-SOC. 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 guidelines established in the "*Guidelines for the Public Reporting of Cybersecurity Incidents*," the State Chief Information Security Officer may publish a public notice of the cybersecurity incident if the incident meets the criteria and thresholds established in that document.

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, regardless of whether the incident met the thresholds and criteria described in the "*Guidelines for the Public Reporting of Cybersecurity Incidents*." Additionally, aggregate data regarding incidents may be shared.

Consistent with the limitations established in MD Gen Provisions Code § 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 - 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 ***not required*** to report this incident. While the user was successfully phished, the credentials were changed before the threat actor could gain access. The organization ***should*** consider contributing to the collective defense of the State by providing the following IOAs and IOCs to the MD-ISAC:

- 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 2 - 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.”**