Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

Guidelines for the Public Disclosure of Cybersecurity Incidents

Table of Contents

Revision History

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

Approval

Charles I Stewart III

Charles "Chip" Stewart
State Chief Information Security Officer

10/1/2022
Date

Introduction

Pursuant to Section 8 of SB812, Ch. 242 (2022)[1], on or before October 1, 2022, the State Chief Information Security Officer (SCISO) is required to establish guidelines to determine when a cybersecurity incident shall be disclosed to the public.

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.[2]

Manner of Reporting

Reports will be published on the Maryland Department of Information Technology website.

Scope

The term "units" in this document refers to the entities identified in Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(d)(2), including:

- Units within the Executive Branch of State Government[3], including:
    - The principal departments[4] defined in MD Code, State Government, § 8-201
    - The Maryland State Department of Education and its subdivisions
    - The Comptroller of Maryland[5]
    - The Treasurer of Maryland[6]
    - The Attorney General of Maryland[7]
    - The Secretary of State[8]
    - Miscellaneous Executive Agencies[9]

[1] See Maryland SB0812 (2022) at https://mgaleg.maryland.gov/2022RS/bills/sb/sb0812E.pdf
[2] See 44 U.S. Code § 3552(b)(2).
[3] Md. Code, State Fin. & Proc. § 3.5-101(f)
[4] MD. State Government Code Ann. § 8-201
[5] MD. State Government Code Ann. § 4-101
[6] MD. State Government Code Ann. § 5-101
[7] MD. State Government Code Ann. § 6-101
[8] MD. State Government Code Ann. § 7-101
[9] MD. State Government Code Ann. § 9-101

    - The Governor's Office of Community Initiatives[10]
- County Governments, including Baltimore City[11] and their political subdivisions
- Local School Boards
- Local School Systems
- Local Health Departments

The scope excludes:

- Municipal Governments
- The Legislative Branch and its subdivisions
- The Judicial Branch and its subdivisions

General Guidelines

In general, a cybersecurity incident will be reported publicly when it results in any of the following:

- The unauthorized disclosure of a substantial, as determined by the State CISO, amount of:
    - Protected Health Information (PHI)[12]
    - Personally Identifiable Information (PII).[13]
    - Private Financial Information that does not meet the definition of PII.
    - Otherwise uncategorized, but sensitive information.
- A substantive disruption to governmental administrative functions.
- Any mission-impacting disruption to critical government-run services, including:
    - Emergency services (e.g., 911, Public Safety Radio System)
    - Water and Wastewater Systems (e.g., potable water distribution)
    - Energy Generation or Distribution
    - Transportation Infrastructure Systems (e.g., Permanently-installed Variable-message signs)
- The permanent loss of a substantial, as determined by the State CISO, number of records that the State has a statutory or regulatory obligation to retain.

The State CISO, at their discretion, may elect to report incidents that do not meet these criteria if they believe that transparency regarding the incident is in the public interest.

[10] MD. State Government Code Ann. § 9.5-101
[11] MD. State Government Code Ann. § 1-101
[12] See 45 CFR § 160.103
[13] See MD. State Government Code Ann. § 10-1301

Substance of Report

The report, at a minimum, will contain the following information:

- The date the incident occurred or was detected.
- General information about the identity of the victim, unless the victim agrees to be specifically named or at the discretion of the State CISO.
- A general description of the incident.
- A general description of the impact of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.

Timing of Notice

The timing of the disclosure is based on the date of initial detection, known as “day zero” of the incident. If the unit identifies that individually immaterial cybersecurity incidents are material in aggregate, the date of that determination will be considered “day zero.”

Units are required to provide a written incident report to the Office of Security Management no later than 21 days after it identifies an incident that may meet the criteria above. If the unit makes a good-faith effort to complete the investigation but is unable to provide a final report, the unit must provide:

- As much information as is reliably known would contribute to the substance of the report.
- An estimate of when the final report will be delivered.

If a final report is not provided, a preliminary notice will be published no more than 10 calendar days after notification from the unit that the report will be delayed. The Office of Security Management will publish a notice of a cybersecurity incident within 10 days of receiving a final investigative report from a unit. Whenever possible, the publishing of any notice will be coordinated with the impacted unit.

The State CISO may delay publication of the report if such disclosure would:

- impede a criminal investigation
- adversely affect mitigation or recovery efforts
- or provide an advantage to the threat actor
- would conflict with the notification requirements of Maryland State Government Code §10-1305

Additionally, public reporting of cybersecurity incidents may be delayed to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system.