Department of
INFORMATION
TECHNOLOGY

Supplemental Guidance on the Reporting of Security Incidents

February 24, 2020
Version 1.0

Table of Contents

1 Introduction

The Maryland IT Security Manual describes the requirements for incident reporting in section IR-6, including the timelines and external reporting. The purpose of this Supplemental Guidance is to provide additional clarity to units to ensure that incident handling occurs in a manner congruent with the expectations of the Office of Security Management and the State Chief Information Security Officer (SCISO).

This document should also not be construed as an alternative to the Maryland IT Security Manual or any other Maryland Department of IT documentation. It is meant as supplemental guidance only.

The wording conventions in this guidance document follow Request For Comments (RFC) 2119 (more information here: https://www.ietf.org/rfc/rfc2119.txt) and as outlined in the definitions section of this document. The words defined in this RFC are presented in **bold underline** to ensure clarity that the definition is noted.

This document will be updated as needed, to further provide clarity and as risks and mitigations evolve.

2 Applicability

The policy **applies** to all entities that meet any of the following descriptions, as defined in the Maryland Manual.

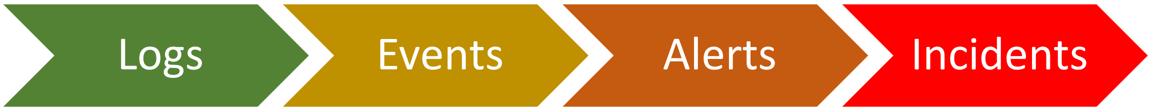
- The Governor's Office and Coordinating Offices
- Each of the Twenty Principal Departments
- Each of the Maryland Independent Agencies
- Each of the Maryland Executive Commissions, Committees, Task Forces, Advisory Boards
- The Military Department
- The Office of the Attorney General
- The Board of Public Works
- The Comptroller of Maryland
- The Secretary of State
- The State Treasurer

3 Key Take-Aways

1. Units **must** report material security incidents and security breaches to the Office of Security Management as soon as they are discovered or reasonably suspected.
2. DoIT **may** provide incident response support and guidance if needed.
3. The handling of all verified security incidents or breaches **must** occur in a manner congruent with legally-accepted mechanisms for the collection and preservation of evidence.

4 Incident Definition Clarification

As security becomes more a part of the design of systems, the generation of logs is occurring at an ever-increasing rate. Additionally, the widespread availability of hacking tools provides even a novice computer user the ability to direct attacks against State government systems. Functionally, the identification of an incident based on the telemetry occurs through the progression illustrated below.



4.1 Logs

In a typical environment, the hundreds or thousands of systems generate millions of log messages in the course of a day, and most of them represent benign activity. The items logged would typically include everything from system activity such as a user unlocking the system, a network port reporting down, to a log message from the firewall noting a potentially dangerous exploit attempt. Generally, no single log message is independently valuable and requires contextual correlation to generate an event.

4.2 Events

In the context of security, an event is typically the point where an analyst would reasonably believe that something has gone wrong, and is the next step in the progression of the declaration of an incident. While many events are notifications of an expected outcome, such as a server backup job completing successfully, some of these occurrences do represent the potential failure of the security apparatus. Adverse events might include anything from user contact regarding an issue about their system, to specific log messages that have been filtered based on context to indicate a need for additional investigation, or an external contact about abnormal traffic. Events may graduate to an incident, or cause the automatic generation of an alert.

4.3 Alerts

Alerts are events that have graduated to the point of triggering a preconfigured notification or alarm, either due to a threshold or because of the nature of a single occurrence. Alerts will fall into one of four categories, based on the outcome of an investigation.

- False Negative
  - No alert is generated where an actual issue occurred.
- True Positive
  - The occurrence of an alert correlated to an event represents an actual issue.
- False Positive
  - An occurrence of an alert that does not represent an actual issue, generally caused by overly sensitive or poorly tuned sensors, or inaccurate user reports.
- True Negative
  - While not generally relevant to the context of alerts, no condition occurred and no alert was generated.

4.4 Incidents

In the context of security, the definition of the term incident is different from that of an ITIL incident. The National Institute of Standards and Technology defines an incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices". Graduated from either an alert or event, an incident is an occurrence that impacts, or has the potential to impact:

- The availability or integrity of a system
- The confidentiality, integrity, and/or availability of the data on a system
- The secrecy of login credentials
- The security of systems connected to the unit's network

Once identified, incidents always require some level of incident response, even if there is no requirement for escalating or reporting the incident to DoIT. Examples of security incidents that do not require reporting are occurrences such as a single user receiving an untargeted phishing email, or a user accessing a folder that they did not have permissions for, where no PII or other protected information was accessed.

5 Incident Reporting Requirements

Because each environment and situation has nuance and unique attributes, DoIT considers the threshold for reporting to require that reasonable judgment be utilized. The primary factors in the decision-making process should consider the following, where if the answer to any of these is "yes" an incident should be reported (the Office of Security Management encourages over-reporting):

- Is/Was the incident visible to members of the general public? (e.g., An informational website experiences a defacement)
- Did/Does the incident impact citizens' ability to access State systems or receive State services? (e.g., Unable to renew a professional license)
- Does the incident create, or have the potential to create, a requirement for external reporting? (e.g., Theft of PII data)
- Does the incident have the potential to spread to other organizations? (e.g., email worm)
- Does the incident involve a third-party that may interconnect with other units or policial subdivisions? (e.g., Ransomware spread by a managed service provider to State systems)
- Could sharing the information about the incident help to prevent another unit or policial subdivision from experiencing the same issue? (e.g., IOCs from a phishing message)
- Is there potential that the incident may be reported by media outlets or generate phone calls from external groups to another group inside of the government? (e.g., A high-profile website is unavailable due to a denial-of-service attack)
- Are there any extenuating circumstances that would cause a reasonable person to report the incident? (e.g., A large number of users are reporting new shortcuts on their desktops that are unexplained by a planned and scheduled change)

5.1 Reporting Process

If an incident is discovered that meets the indicia for reporting described above, or there is a reasonable expectation based on logs, events, and alerts that an incident has occurred, units must report the occurrence to DoIT as soon as it is practical. Incidents may be reported by emailing the attached form to SOC.DoIT@maryland.gov or by calling the service desk directly. The completeness of the form is less important than providing timely notification to DoIT.

5.2 Exceptions for Incident Reporting Requirements

Units may forbear from reporting to DoIT if there is a reasonable expectation that the reporting of the incident would jeopardize an active law-enforcement investigation because an individual at DoIT is a suspect in the incident. In those cases, notification should be made using similar expectations for timeliness using the following escalation path:

- State Chief Information Security Officer
- State Chief Information Officer
- Director of the Governor's Office of Homeland Security

Any incident where an exception to the reporting requirements is utilized must be reported to DoIT using the prescribed mechanism within 24 hours of the resolution of the incident.

Nothing within this section requires reporting where prohibited by federal law or where the individuals receiving the report would not have adequate security clearance to view the information contained within.

6 Definitions

6.1 Acronyms and Definitions

Breach - The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

IOC – Indicator of Compromise - is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion

Unit – Any organization, sub-organization, or entity described in Section, including any departments or divisions not explicitly defined in the Maryland manual.

6.2 RFC 2119 Definitions

MUST - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.

MAY - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Appendix A - Incident Reporting Form

1. Government Contact Information for this Incident	
Name:	
Title:	
Program Office:	
Work Phone:	
Email address:	
2. Contractor Contact Information for this Incident	
Name:	
Title:	
Program Office:	
Work Phone:	
Email Address:	
3. Incident Description.	
Provide a brief description:	
4. Impact / Potential Impact Check all of the following that apply to this incident.	
☐ Loss / Compromise of Data ☐ Damage to Systems ☐ System Downtime ☐ Financial Loss ☐ Other Organizations' Systems Affected ☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information ☐ Violation of legislation / regulation ☐ Unknown at this time	

Provide a brief description:

5. Determine the Sensitivity of Data

Category	**Example**
Public	This information has been specifically approved for public release by Public Relations department or Marketing department managers. Unauthorized disclosure of this information will not cause problems for the Department of Maryland, its customers, or its business partners. Examples are marketing brochures and material posted to Department of Maryland web pages. Disclosure of agency information to the public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.
Internal Use Only	This information is intended for use within DoIT and Maryland Information Systems (MIS) or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the Department of Maryland, its customers, or its business partners. This type of information is already widely distributed within the Department of Maryland, or it could be so distributed within the organization without advance permission from the information owner. Examples are an agency telephone book and most internal electronic mail messages.
Restricted/Confidential **(Privacy Violation)**	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations or may cause significant problems for the Department of Maryland, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are customer transaction account information and worker performance evaluation records. Other examples include citizen data and legal information protected by attorney-client privilege.

Information Involved. Check all of the following that apply to this incident.

Unknown/Other	Describe in the space provided
☐ Public ☐ Internal Use Only	☐ Restricted / Confidential (Privacy violation) ☐ Unknown / Other – please describe:
Provide a brief description of data that was compromised:	
6. Who Else Has Been Notified?	
Provide Person and Title:	