Enterprise Cybersecurity Incident Reporting Guidelines

ITS

Mississippi Department of Information Technology Services

TABLE OF CONTENTS

PURPOSE & SCOPE

This document provides guidance to state agencies for reporting cybersecurity incidents to the Mississippi Department of Information Technology Services (ITS).

The scope of this document and requirements apply to all Mississippi state agencies.[1] "Agency" means and includes all the various state agencies, officers, departments, boards, commissions, offices, and institutions of the state.[2] Additionally, any entity that participates in the Enterprise State Network managed by ITS is considered within scope of this document and is required to adhere to the requirements within. Mississippi governing authorities, who wish to voluntarily comply with the reporting process, are invited to do so.[3]

[1] Miss. Code Ann. § 25-53-201.
[2] Miss. Code Ann. § 25-53-3(2)(e)
[3] Miss. Code Ann. § 25-53-3(2)(f).

INCIDENT REPORTING

Per the requirements of the State of Mississippi Enterprise Security Program and state law[4], state agencies must report all cybersecurity incidents involving their information and information systems, whether managed by the state agency, contractor, or other source.

Reporting incidents to a central group promotes collaboration and information sharing with other entities that may be experiencing the same or similar problems. Reporting to a central group provides the ability to:

- Coordinate activities among agencies experiencing similar incidents to help identify and resolve the problem more quickly than if done separately
- Share threat intelligence to help agencies protect themselves from similar attacks
- Share information between public and private stakeholders, and other appropriate entities
- Collaborate with key entities that can provide the necessary cybersecurity expertise to assist when necessary
- Collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack

Reportable Incidents

A cybersecurity incident is an event that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or a violation or imminent threat of violation of cybersecurity policies, acceptable use policies, or standard cybersecurity practices. This also includes cyberattacks where there is an attempt to gain illegal access, including any data breach, to a computer, computer system or computer network for purposes of causing damage, disruption or harm as well as ransomware.[5] Examples of incidents include, but are not limited to:

- Email/Phishing: An attack executed via an email message or attachment
    - Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
- Impersonation/Spoofing: An attack involving replacement of legitimate content/services with a malicious substitute

[4] Miss. Code Ann. § 25-53-201.
[5] Miss. Code Ann. § 25-53-201(5).

- Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.

- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services
  - Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
- Web: An attack executed from a website or web-based application
  - Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
- Malware: An attack using software, firmware, or hardware to gain unauthorized access to and/or adversely impact the confidentiality, integrity, or availability of a system
  - A virus, worm, and/or Trojan used to steal data, disrupt system services, damage networks, and/or access to system(s) for harmful purpose(s).
- External/Removable Media: An attack executed from removable media or a peripheral device
  - Malicious code spreading onto a system from an infected flash drive.
- Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories
  - User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- Ransom: Any incident resulting in a demand for a designated sum of money or other consideration
  - Malicious code spreading onto a system that obtains and/or encrypts or restricts access to sensitive information, information systems, or information networks.
- Unknown: Cause of attack is unidentified
  - This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
- Other: An attack method does not fit into any other vector
  - This option could include theft of physical devices, physical break-in, *etc*.
- User Error: An incident resulting from user mistakes or violation of policies and security best practices
  - This option could include misconfiguration, sensitive data shared inappropriately, compromised user credentials, *etc*.

Incident Classification

Cybersecurity incident severity classifications are provided below.

- **None (Green)**: Malicious activity has been identified with little to no impact on agency operations, agency assets, or individuals
  - Result in no impact to confidentiality, integrity or availability to information or information systems
  - Result in no financial loss
  - Result in no harm to individuals

- **Low (Yellow):** Malicious activity has been identified with minor impact on agency operations, agency assets, or individuals. Minor impact could
  - Cause a degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is noticeably reduced
  - Result in minor damage to agency assets
  - Result in minor financial loss
  - Result in minor harm to individuals

- **Medium (Orange):** Malicious activity has been identified with a moderate level damage or disruption on agency operations, agency assets, or individuals. Moderate impact could
  - Cause a significant degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is significantly reduced
  - Result in significant damage to agency assets
  - Result in significant financial loss
  - Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries

- **High (Red):** Malicious activity has been identified with a severe level of damage or disruption on agency operations, agency assets, or individuals. Severe impact could
  - Cause severe degradation in or loss of mission capability to an extent and duration that the agency cannot perform one or more of its primary functions

- Result in major damage to agency assets
- Result in major financial loss
- Result in severe harm to individuals that may involve loss of life or serious life-threatening injuries

Reporting Requirements Incidents

Each agency must report cybersecurity incidents classified as low, medium, or high to ITS no later than the close of the next business day following the discovery of the incident.

- Events that are classified as None (Green) do not have to be reported as these are, typically, ordinary events that occur daily for most organizations. Basic security/network tools (firewall, anti-malware, IDS/IPS, *etc.*) that most organizations use easily detect and prevent these types of events from causing any negative impact; however, if the agency recognizes any abnormal pattern that may indicate a potential persistent attack, the agency should report to ITS for situational awareness.

In some cases, it may not be feasible to have complete and validated information for the incident prior to reporting. Agencies should provide their best estimate at the time of notification and report updated information as it becomes available.

Depending on the nature of the incident, agencies may also be required to report and/or provide notification(s) pursuant to applicable state and/or federal statutes and/or regulations. And each agency should consider contacting the appropriate law enforcement agency (e.g., city, county, state, or federal) as applicable. Begin with contacting your local law enforcement agency for assistance if the activity appears criminal in nature.

Reporting Incidents

Cybersecurity incidents must be reported to ITS using the following process:

- The agency IT Director, ISO, or designated official is responsible for reporting incidents using the online web form. The form is accessible at the following location:
  - https://ms.accessgov.com/its/Forms/Page/its/its-cybersecurity-incident-report/
- Complete the incident reporting form with as much detailed information as possible
- If the online form is inaccessible, use a landline as an alternate form of communication to report the incident to ITS and request, complete, and return a physical copy of the cybersecurity incident reporting form to ITS.
  - ITS Service Center (601-432-8080)
  - ITS Main Line (601-432-8000)

- Status updates are expected as new information pertaining to the cybersecurity incident becomes available

Agencies are encouraged to maintain a copy of the incident reporting form submitted online or a hard copy of the submitted incident form, if the online form is inaccessible, to capture details of the incident and for audit, state, and/or, federal statutory or regulatory compliance purposes. The form can be downloaded from the same website location provided above.

ITS CONTACT INFORMATION

Executive Director	Dr. Craig P. Orgeron Craig.Orgeron@its.ms.gov
Chief Administrative Officer	Stephanie Hedgepeth Stephanie.Hedgepeth@its.ms.gov
Chief Information Security Officer	Jay White Jay.White@its.ms.gov
Chief Operations Officer	Brian Norwood Brian.Norwood@its.ms.gov
Data Services	Steve Patterson Steve.Patterson@its.ms.gov
Internal Services	Holly Savorgnan Holly.Savorgnan@its.ms.gov
Procurement Services	Rebecca Henley Rebecca.Henley@its.ms.gov
Telecom Services	Lisa Kuyrkendall Lisa.Kuyrkendall@its.ms.gov
Mississippi Department of Information Technology Services	3771 Eastwood Drive Jackson, MS 39211 (601) 432-8000

Dr. Craig P. Orgeron, Executive Director

3771 Eastwood Drive
Jackson, Mississippi 39211
Telephone (601) 432-8000
Fax (601) 713-6380
Web site: www.its.ms.gov
State Portal: www.mississippi.gov