New York State Cyber Incident Reporting Procedures

As outlined in the New York State (NYS) Incident Response Standard, once an incident is identified and classified, an effective incident response process requires escalation to the proper stakeholders to communicate essential information. Notification is to be made as soon as possible but should not delay a State Entity (SE) from taking appropriate actions to isolate and contain damage.

As per the New York State Information Security Policy, SEs must notify the NYS ITS Cyber Command Center of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to ensure proper incident response procedures, coordination and oversight.

Notification to the Cyber Command Center may be accomplished through one of the following methods:

- TELEPHONE Cyber Command Center Hotline: 518-242-5045. Please identify the urgency of the call. After hours (5PM- 9AM, weekends and holidays), please call NYS Watch Center at 518-292-2200 and ask to report a cyber incident to the Cyber Command Center; OR

- Email CYCOM@ITS.NY.GOV If including sensitive data and you are outside of the NYS Office 365 (O365) tenancy, consider encrypting using the Chief Information Security Office (CISO)'s PGP public key. The key may be found on the CISO web site at Incident Reporting | New York State Office of Information Technology Services (ny.gov).

Notification shall include as much of the information contained on the NYS CISO INCIDENT NOTIFICATION REPORT form (see Incident Reporting | New York State Office of Information Technology Services (ny.gov)) as possible.

It is not always feasible to gather all the information prior to notification. Notification should not be delayed in order to gain additional information. SEs should continue to report information as it is collected.

Information regarding specific cyber security related incidents will not be publicly disclosed by the CISO. CISO may share information about incidents with law enforcement officials and, unless the SE specifically directs otherwise, other appropriate organizations that are subject to non-disclosure requirements, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) or the United States Computer Emergency Readiness Team (US-CERT). In addition, aggregated information concerning cyber security related incidents that does not identify individual SEs may be disclosed by CISO in furtherance of its statutory duties.

Revision History

Date	Description of Change
11/05/2013	Original Procedure Release; *replaces CSCIC/OCS P03-001 Cyber Incident Reporting Policy*
02/10/2015	Updated to fix URLs
03/29/2016	Updated to replace CIRT with Cyber Command Center and provide new email address
04/24/2017	Updated to fix links, remove bullet that refers to ITSM tickets, remove name references in the header, and remove reference to Appendix A
03/08/2022	Updated to fix links, minor change to the title of the office