New York State Cyber Incident Reporting Procedures

This procedure only applies to cybersecurity incidents that are impacting NYS Government entities and employees.

Private entities and individuals who are experiencing a cybersecurity-related incident should contact their local law enforcement agency for assistance.

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 that 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**: NYS Security Operations Center (NYSOC) Hotline at 1-866-44-NYSOC (69762), staffed 24/7 by cyber analysts.
- **Email**: support@soc.ny.gov. If you are including sensitive data and you are outside the NYS Office 365 (O365) tenancy, consider encrypting the data using the Chief Information Security Office (CISO)'s PGP public key. The key can be downloaded from the ITS website.

Notification should include as much of the information contained on the NYS CISO incident Notification Report form as possible. If all information cannot be gathered immediately, SEs should continue to report additional information as it is collected.

Incident Information Sharing

- Information regarding specific cybersecurity-related incidents will not be publicly disclosed by the CISO.
- CISO may share incident details with law enforcement and other appropriate organizations subject to non-disclosure agreements, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) or the United States Computer Emergency Readiness Team (US-CERT).
- Aggregated information about cybersecurity-related incidents, which does not identify individual SEs, may be disclosed by the CISO in furtherance of its statutory duties.