



ANDREW M. CUOMO
Governor

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

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 Cyber Incident Response Team (CIRT) 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 CIRT may be accomplished through one of the following methods:

- TELEPHONE CIRT 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 CIRT;
- Email CIRT@ITS.NY.GOV. If including sensitive data, consider using the NY-ISAC Secure Portal or encrypting using the Enterprise Information Security Office (EISO)'s PGP public key. The key may be found on the EISO web site at <http://www.dhSES.ny.gov/ocs/incident-reporting/>;
- Email "NY IRT" in the NY-ISAC (Information Sharing and Analysis Center) Secure Portal (Note: address will display as "IRT, NY" in the address book); OR
- Submit a ticket using the Office of Information Technology Services (OITS) information technology service management (ITSM) system.

Notification shall include as much of the information contained on the NYS EISO INCIDENT NOTIFICATION REPORT form (see [Appendix A](#) or <http://www.dhSES.ny.gov/ocs/incident-reporting/>) 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 EISO. EISO 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 EISO in furtherance of its statutory duties.

Revision History

Date	Description of Change
11/05/2013	Original Procedure Release; replaces <i>CSCIC/OCS P03-001 Cyber Incident Reporting Policy</i>

Appendix A: EISO Incident Notification Report Form

Incident Notification Report			
Contact Information			
Name:		Title:	
Agency/Department:		Email:	
Office Phone:		Mobile	
Incident Location			
Local Contact Name		Title/Role:	
Office Phone:		Mobile	
Email:			
Location / Address:			
Incident Detection			
<input type="checkbox"/> Device Alert	<input type="checkbox"/> Log Analysis	<input type="checkbox"/> Help Desk	
<input type="checkbox"/> End User Alert	<input type="checkbox"/> Endpoint Security Software Alert	<input type="checkbox"/> Law Enforcement	
<input type="checkbox"/> Other			
Incident Type			
<input type="checkbox"/> Exercise / Network Defense	<input type="checkbox"/> Denial of Service	<input type="checkbox"/> Improper Usage	<input type="checkbox"/> Investigation
<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> Malicious Code	<input type="checkbox"/> Scans / Probes / Attempted Access	
<input type="checkbox"/> Other			
Incident Characteristics			
Source IP/Port:		Destination IP/Port:	
Scope of Impact:		Additional	
Incident Timeline			
Duration of Attack (From):		Duration of Attack (To):	

Incident Impact			
<input type="checkbox"/> Number of Affected Users:			
<input type="checkbox"/> System Down Time:			
<input type="checkbox"/> System Damage:			
<input type="checkbox"/> Service / Information Integrity Damage:			
<input type="checkbox"/> Financial Loss:			
<input type="checkbox"/> Data Loss / Compromise:			
<input type="checkbox"/> Other			
Incident Severity			
<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	<input type="checkbox"/> Unknown
Affected Data Sensitivity			
<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	<input type="checkbox"/> Unknown
Confidentiality			
<input type="checkbox"/> Do Not Share – Information may not be shared beyond EISO and may be shared with law enforcement if necessary.			
<input type="checkbox"/> Share Restricted - Information cleansed of identifying characteristics may be shared with other SEs, states and other appropriate organizations			
<input type="checkbox"/> Share Unrestricted – Information including identifying characteristics may be shared with other SEs, states and other appropriate organizations			
What immediate assistance can the CIRT offer?			
Additional Notes			