NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

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

New York State Information Technology Standard	**No:** NYS-S13-005
IT Standard:	**Updated:** 11/03/2023
Cyber Incident Response	**Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This standard outlines the general steps for responding to information security incidents. In addition to providing a standardized process flow, it (1) identifies the New York State (NYS) incident response (IR) stakeholders and establishes their roles; (2) describes the process and activities through the IR process flow; (3) describes coordination with all relevant IR stakeholders and partners, and (4) provides examples of IR metrics for use in gauging IR effectiveness.

The goals of IR, as outlined in this standard, are to:

- Confirm whether an incident occurred;
- Provide a defined incident notification process;
- Promote the accumulation and documentation of accurate information;
- Contain the incident and halt any unwanted activity quickly and efficiently;
- Minimize disruption to operations;
- Provide accurate reports and useful recommendations to management and other stakeholders; and
- Prevent and/or mitigate future incidents from occurring.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies,

including technology and security standards. *Executive Order No. 117*[1], established in January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, NYS-P08-002 Authority to Establish Enterprise Information Technology Policies, Standards, and Guidelines.

3.0 Scope

This policy applies to all "State Entities" (SE), defined as "State Government" in Executive Order 117, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different policy/standard, it must include the requirements set forth in this one. Where a conflict exists between this policy/standard and a SE's policy/standard, the more restrictive policy will take precedence.

4.0 Information Statement

4.1 IR Stakeholders

To respond effectively to an incident, it is critical that all IR stakeholders understand not only their roles in the IR process, but also the role of other stakeholders. This is necessary to (1) avoid duplication of effort; (2) minimize procedural gaps that may occur; and (3) ensure rapid response to incidents. Appendix E provides a description for the State Agency Division of Authority.

NYS IR stakeholders include:

1. NYS Chief Cyber Officer (CCO) – The NYS CCO leads cross-agency efforts to protect New York State from increasingly prevalent and sophisticated cyber threats. NYS CCO works to ensure the security, integrity, and cyber resilience of the State's information assets and critical infrastructure.
2. NYS Office of Information Technology Services (ITS) NYS Chief Information Security Officer (NYS CISO) – The NYS CISO, or their designee, provides for overall coordination of IR including the escalation of an incident. The NYS CISO leads the Chief Information Security Office (CISO) within ITS which provides IR services for ITS-supported agencies (Client Agencies).
3. NYS ITS Cyber Command Center (CyCom) – CyCom serves as a central group for detection, analysis, tracking, response to, and reporting of cyber threats and incidents for Client Agencies. CyCom responds to incidents by providing hands-on technical IR and will recommend remediation and/or mitigation steps for Client Agency staff to reduce the likelihood of future incidents.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot L. Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011, and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

4. New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) – NYSIC CAU facilitates collaboration and information sharing with other authorized entities that may be experiencing the same or similar incidents, to help resolve the problem more quickly than if done separately. NYSIC CAU collects statewide information on the types of vulnerabilities being exploited and the frequency of attacks, then shares preventative information to help other SEs protect themselves from similar attacks.
5. Division of Homeland Security and Emergency Services (DHSES) Office of Emergency Management (OEM) – At Executive Chamber direction, OEM coordinates state agencies' response to natural and human-caused disasters and emergencies, including those caused by cyber events and major cyber incidents.
6. DHSES Cyber Incident Response Team (CIRT) – CIRT offers remote or on-site support to eligible organizations, local governments, non-Executive state agencies, and public authorities. CIRT provides incident-specific recommendations on containment, eradication, and recovery to reduce the impact of the disruption. CIRT will also provide post-incident security recommendations, which can help organizations build a more proactive cyber program going forward.

7. SE Leadership – SE leadership provides essential IR oversight and is responsible for determining who should be a part of SE IR teams and providing guidance as needed.

8. Information Security Officer (ISO)/designated security representative – The ISO/designated security representative, or their designee, facilitates SE response to potential and actual information security incidents.

9. Cyber First Responders – SE IT staff, such as network managers, system administrators, and other technical personnel, will be called upon, as needed, to provide support and tactical response.
10. SE Incident Response Teams – SEs must prepare predefined teams which must include, at minimum, executive management, counsel, and applicable communications staff. In some cases, human resources and labor relations may become involved.
11. Additional Participating Entities – In consultation with IR Teams, additional participating entities may conduct hands-on IR activities, such as investigative response activities, or may provide guidance. For example, a security solutions vendor may provide assistance on security appliance settings. Additional participating entities include vendors, service providers, or law enforcement including:
    - Multi-State Information Sharing and Analysis Center (MS-ISAC)
    - Federal Bureau of Investigation (FBI)
    - Cyber Security and Infrastructure Security Agency (CISA)
    - New York State Police (NYSP)
    - Internet Service Providers
    - Security Solutions Vendors
    - Data Holder Vendors

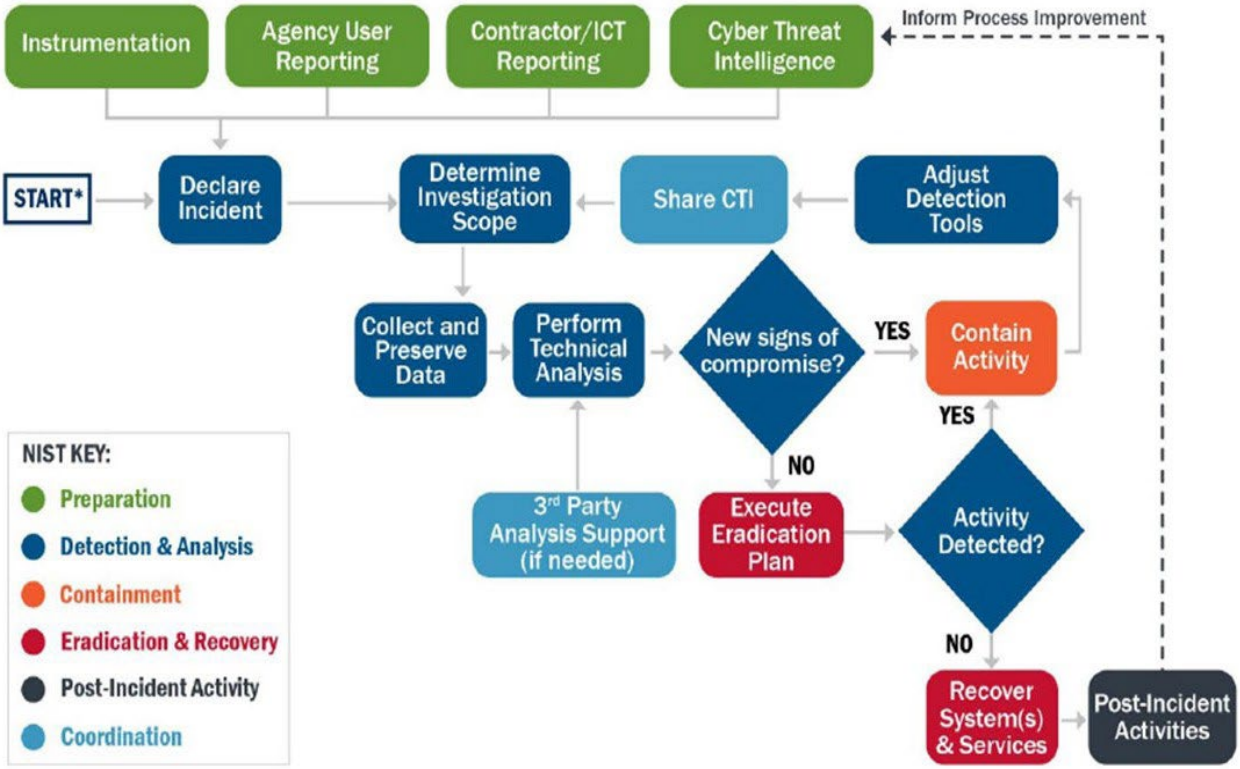
- Other state, local, tribal governments

4.2 IR Process Flow

This IR process flow covers how to respond to specific situations for IR stakeholders to ensure an effective and efficient response. The focus of the NYS IR process is to eradicate the problem as quickly as possible, while gathering actionable intelligence, to restore business functions, improve detection, and prevent reoccurrence.

The information provided in the following section includes activities that are involved in a robust IR Process Flow. All SEs must strive to meet the outlined activities to most efficiently and completely remediate a security incident. Not all activities will be required for every incident. Significant cyber incidents that involve physical or government service impacts may be designated as major incidents. Consequence management for the non-cyber impacts of the response could require an expanded State response, which may involve Multi-Agency Coordination Calls or activation of the State Emergency Operations Center (EOC), coordinated by DHSES OEM.

The CISA Cybersecurity Incident & Vulnerability Response Playbooks provide a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2, including coordination, preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. NYS has adopted a phased approach consisting of activities as depicted below:



CISA Cybersecurity Incident & Vulnerability Response Playbooks[2]

Figure 1 – Incident Response Process Flow

4.2.1 Preparation

Proper planning and preparation for an incident before it occurs ensures a more effective and efficient IR process. As per the NYS-P03-002 Information Security Policy, SEs must have a documented IR plan, consistent with NYS information technology standards, to effectively respond to security incidents.

Activities

1. Train Response Personnel
    - Ensure personnel are trained, exercised, and ready to respond to security incidents. Train all staffing resources that may draw from in-house capabilities, available capabilities at a parent agency/department, third-party organization, or any combination.
2. Policies and Procedures
    - Prepare documented IR plans and procedures that include an up-to-date IR contact list and address notification, interaction, and evidence collection, sharing, and chain of custody procedures.
    - In consultation with their ISO/designated security representative, or their designee, the SE must develop IR standard operating procedures (SOPs) that reflect industry standards and best practices. SEs must also ensure that the SOPs are followed during IR. The SE must routinely vet and validate the tools and techniques used for IR. To operate efficiently and effectively, the IR process must be regularly tested. This testing must occur at least annually . This testing can be accomplished with mock incident training or tabletop exercises using realistic scenarios to provide a high-level outline and systematic walkthrough of the IR process and, to the extent possible, must include all IR stakeholders. These training scenarios must include specific "discussion points" that represent key learning opportunities, and incorporate lessons-learned, which can then be integrated into the IR process as part of its review.
3. Instrumentation
    - Develop and maintain an accurate picture of infrastructure through technology such as anti-virus, end point detection monitoring, data loss prevention, intrusion detection, and log management.
4. Communications and Logistics
    - SEs must assign responsibility to a central point of contact who will coordinate identification and reporting out to the appropriate stakeholders. Typically, this is performed by the SE's ISO/designated security representative, or their designee. All employees are required to report suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative, or their designee.

[2] Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov)

4.2.2 Detection & Analysis

Detection & Analysis is often the most challenging aspect of the IR process. It involves monitoring networks, systems, and data to identify a potential cybersecurity incident and examining the detected incident to determine its scope, impact, and root cause so that an effective response can be undertaken.

Activities

1. Declare Incident
   - This involves the review of anomalies to determine whether an incident has occurred, and, if one has occurred, determining the nature of the incident.
2. Determine Investigation Scope
   - This involves the review of anomalies to determine whether an incident has occurred, and, if one has occurred, determining the nature of the incident. Detection begins with an event, an anomaly that has been reported or noticed in a system or network. Detection can be accomplished through technical sources (e.g., operations staff, anti-virus software), non-technical sources (e.g., user security awareness and reporting), or both. It is important to recognize that not every network or system event will be a security incident. In fact, most events will not lead to security incidents. For that reason, a Cyber First Responder must be assigned to determine if there is an incident, categorize the incident, and escalate as necessary.
3. Collect and Preserve Data
   - Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution.
   - Incidents must be classified and escalated as soon as possible to the proper IR stakeholders to promote collaboration and information sharing.
4. Perform Technical Analysis
   - The goal of this analysis is to examine the breadth of data sources throughout the environment to discover at least some part of an attack chain, if not all of it. As information evolves and the investigation progresses, update the scope to incorporate new information.
5. Correlate Events and Document Timeline
   - Acquire, store, and analyze logs to correlate adversarial activity.
6. Identify Anomalous Activity
   - Assess and profile affected systems and networks for subtle activity that might be adversary behavior.
7. Identify Root Cause and Enabling Conditions
   - Identifying the root cause will help inform triage and post-incident activities.
8. Gather Incident Indicators
   - Will allow for correlative analysis that can provide insight into the capabilities of the adversary.
9. Analyze for Common Adversary Tactics, Techniques, and Procedures (TTPs)
   - TTPs describe “why,” “what,” and “how.” Tactics describe the technical

objective an adversary is trying to achieve ("why"), techniques are different mechanisms they use to achieve it ("what"), and procedures are exactly how the adversary achieves a specific result ("how").

10. Validate and Refine Investigation Scope
    - Using all the data collected and the current response activities, this allows for the iterative element of this phase, and will help find any new issues that might have been missed the first time through.
11. Third-Party Analysis Support (if needed)
12. Adjust Tools

Per NYS-P03-002 Information Security Policy, CyCom must be notified of any cyber incident which may have a significant or severe impact on operations or security.

NYS has adopted the taxonomy used by US-CERT to promote a common set of terminology used in the IR process. For more information see the following:

Incident Severity

NYS has adopted the CISA National Cyber Incident Scoring System (NCISS). For the Cyber Incident Severity Schema see Appendix A.

Attack Vectors

Security incidents can occur from a wide variety of different attacks/events. The table in Appendix B shows a high-level set of attack vectors taken from NIST SP 800-61r2 and included in US-CERT Federal Incident Notification Guidelines.

Impact Categories

Security incidents can have different impact categories. These may be Functional Impact, Information Impact, or Recoverability Impact. For further explanation see US-CERT Federal Incident Notification Guidelines and Appendix C.

Incident Attributes

The following incident attribute definitions are taken from the NCISS and published in US-CERT Federal Incident Notification Guidelines and in Appendix D.

Escalation Procedures

During an incident, clear and effective communication to all IR stakeholders is critical so that everyone has the necessary information to act and carry out their responsibilities promptly. As such, an escalation procedure must address all lines of communication in the event an incident occurs. This includes both internal and external communications. Notification must be made as soon as possible but should not delay an SE from taking appropriate actions to isolate and contain the damage.

Each SE must have a documented IR escalation procedure that consists of:

- an escalation matrix;
- an up-to-date contact list with alternate contacts; and

- multiple communications channels that ensure appropriate and accurate information is disseminated quickly to the appropriate IR stakeholders.

Incident Tracking & Reporting

A secure centralized tracking system that can accommodate "need to know" access leads to a more efficient and systematic IR effort, as well as providing an audit trail, should the efforts lead to legal prosecution of the threat.

At a minimum, documentation of the incident must contain the following information:

- Date / time the incident was reported
- Type of Incident
- Reporting source of incident
- Summary of the incident
- Current status of the incident
- All actions taken concerning the incident
- Contact information for all involved parties
- Evidence and its chain of custody gathered during incident investigation
- Relevant comments from IR team members
- Proposed next steps to be taken

4.2.3 Containment

This step focuses on containing the threat to minimize and further reduce damage. It is during this step that information is collected to determine how the attack occurred. All affected systems within the enterprise should be identified by Cyber First Responders, so that containment, eradication, and recovery is effective and complete.

Activities

1. Isolating impacted systems
   - Taking systems off the network or isolating the infected systems to keep the infrastructure safe.
2. Capturing forensic images
   - Preserves the evidence for further action and any legal action.
3. Other techniques that are involved in containment
   - Updating firewall filtering, blocking access, blocking malware sources, closing ports and services that are not needed, changing passwords.

The SE leadership makes decisions regarding containment measures based on recommendations from the appropriate entity.

4.2.4 Eradication& Recovery

Eradication involves removing elements of the compromise from the environment. Specific eradication measures depend on the type of incident, number of systems involved, and the types of operating systems and applications involved. Typical eradication measures include reimaging infected systems and enhanced monitoring of system activity. This allows for the return to normal operations.

Analysis of information collected is an iterative process and occurs/reoccurs during both the containment and eradication phases.

Activities

1. Remediating all infected IT environments
2. Reimaging affected systems
3. Rebuilding hardware
4. Replacing compromised files
5. Patching
6. Resetting passwords
7. Monitoring
8. Developing response scenarios
9. Allow time for clearing of all possible threats

4.2.5 Recovery

Recovery involves restoring systems to normal operations and confirming that they are functioning normally. The main challenges of this phase are confirming that remediation has been successful, rebuilding systems, reconnecting networks, and recreating or correcting information.

Activities

1. Reconnecting to networks
2. Tightening perimeter security
3. Testing
4. Monitoring

4.2.6 Post-Incident

The goal of this phase is to document the incident, inform SE leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.

Activities

1. Adjust Sensors, Alerts, and Log Collection
    - This will allow the identification of any “blind spots” that were discovered within the organization during the incident. This process will allow for future strengthening of the systems that were compromised along with the identification of any other systems that may be at risk.
2. Finalize Reports

- Provide post-incident updates and documentation as required by law and policy.
- Incident documentation must be retained by the SE based on any regulatory, records retention, or compliance requirements.

3. Perform Lesson Learned Activities

   - These activities can be the results of actual IR activities or IR capability testing and they should happen relatively soon after the incident is closed. They should include, at a minimum, a recap of the steps involved in response to the incident, results of the root cause analysis, along with any potential improvement to the process and procedures. Both incident reports and the results of these lesson-learned discussions must be documented for future use and shared with all IR stakeholders for situational awareness and professional development.

4.3 Coordination

Coordination is foundational to effective IR. It is critical that the SE experiencing the incident coordinate early and often throughout the response process with all relevant IR stakeholders and partners. SEs may need to interact with several types of external organizations while conducting IR activities. Examples of these organizations include other IR teams, DHSES OEM, law enforcement agencies, Internet service providers, constituents, and customers. An SE's IR team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective lines of communication are established.

Key aspects of coordination include:

- Plan incident coordination with external parties before incidents occur.
- Consult with counsel before initiating any coordination efforts.
- Perform incident information sharing throughout the incident response life cycle.
- Attempt to automate as much of the information sharing process as possible.
- Balance the benefits of information sharing with the drawbacks of sharing sensitive information.
- Share as much of the appropriate incident information as possible with other organizations.
- Any required mandated notifications should be followed. (e.g., NYS Information Security Breach Notification Act ["ISBNA"])

4.4 Incident Response (IR) Metrics

SEs should compile IR metrics for each incident for overall situational awareness when possible and practical. In addition, these metrics can be used for periodic reporting purposes.

These metrics allow IR stakeholders (1) to measure IR effectiveness (and reveal potential gaps) over time; (2) to identify trends in terms of threat activities; and (3) to provide justification for additional resources (personnel, training, and tools). Example metrics are below:

IR Metrics		
Category	**Measurement**	**Description**
Incidents	# Total Incidents / Year	Total amount of incidents responded to per year
	# Incidents by Type / Year	Total number of incidents by category responded to per year (Appendix B – Attack Vectors)
Time	# Personnel Hours / Incident	Total amount of labor spent resolving incident
	# Days / Incident	Total amount of days spent resolving incident
	# System Down-Time Hours / Incident	Total hours of system down-time until incident resolved
Cost	Estimated Monetary Cost / Incident	Total estimated monetary cost per incident, to include containment, eradication, and recovery, as well as collection & analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident
	# Records Compromised / Incident	Total number of records compromised per incident
Forensics	# Total Forensics Leveraged Incidents / Year	Total number of incidents requiring forensics (collection & analysis) per year
	# System Images Analyzed / Incident	Total number of system images analyzed per incident
	# System Memory Dumps Examined / Incident	Total number of system physical memory dumps examined per incident

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S13-005
NYS Office of Information Technology
Services 1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: Policies | Office of Information Technology Services (ny.gov)

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
11/15/2013	Original Standard Release; *replaces Office of Cyber Security Policy P03-001, Cyber Incident Reporting*	Thomas Smith, Chief Information Security Officer
11/21/2014	Standard Review – no changes	Deborah A. Snyder, Acting Chief Information Security Officer

Date	Description of Change	Reviewer
03/20/2015	Clarified stakeholder roles/responsibilities, minor process changes	Deborah A. Snyder, Acting Chief Information Security Officer
05/04/2016	Changed Cyber Incident Response Team (CIRT) to Cyber Command Center	Deborah A. Snyder, Acting Chief Information Security Officer
02/10/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/10/2018	Scheduled review – minor change to Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer
11/03/2023	Changes to align the standard with NIST and the CISA Cybersecurity Incident & Vulnerability Response Playbooks. Added new appendices including not limited to tables related to US- CERT Federal Incident Notification Guidelines, and State Agency Divisions of Authority; added NIMS/ICS coordination for major cyber events	Chris DeSain, Chief Information Security Office

9.0 Related Documents

NIST SP 800-61r2, Computer Security Incident Handling Guide

NIST SP 800-83, Guide to Malware Incident Prevention and Handling

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
New York State Cyber Incident Reporting Procedures

US-CERT Federal Incident Notification Guidelines | CISA

Cyber Incident Response | CISA

CISA National Cyber Incident Scoring System (NCISS)

Appendix A - Incident Severity
Cyber Incident Severity Schema

The United States Federal Cybersecurity Centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all departments and agencies have a common view of the:

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The seniority level necessary for coordinating response efforts; and
- The level of investment required of response efforts.

The table below depicts several key elements of how NCISS aligns with the Cyber Incident Severity Schema (CISS) so that severity levels in the NCISS map directly to CISS levels. The general definitions have been altered to reflect New York State scope.

	General Definition[3]	Observed Actions	Intended Consequence[4]
Level 5 *Emergency* (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, state gov't stability, or to the lives of U.S. persons.	Effect	Cause physical consequence
Level 4 *Severe* (Red)	Likely to result in a significant impact to public health or safety, state security, economic security, or civil liberties.	Presence	Damage computer and networking hardware
Level 3 *High* (Orange)	Likely to result in a demonstrable impact to public health or safety, state security, economic security, civil liberties, or public confidence.		Corrupt or destroy data
Level 2 *Medium* (Yellow)	May impact public health or safety, state security, economic security, civil liberties, or public confidence.	Engagement	Deny availability to a key system or service
Level 1 *Low* (Green)	Unlikely to impact public health or safety, state security, economic security, civil liberties, or public confidence.		Steal sensitiv e information
Level 0 *Baseline - Minor* (Blue)	Highly unlikely to affect public health or safety, state security, economic security, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.	Preparation	Commit a financial crime
Level 0 *Baseline - Negligible* (White)	Unsubstantiated or inconsequential event.		Nuisance DoS or defacement

[3] Definitions have been altered to reflect New York State Scope.

[4] In addition to characterizing the observed activity, one must consider the scope and scale of the incident when applying the general definitions to arrive at a severity level.

Appendix B – Attack Vectors

To clearly communicate incidents across organizations, it is necessary for incident response teams to adopt a common set of terms and relationships between those terms. Below is a high-level set of attack vectors and descriptions. This table is taken from US-CERT Federal Incident Notification Guidelines.

Attack Vector	Description	Example
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.
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.
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.
External/ Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected flash drive.
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.
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.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.

Other	An attack method does not fit into any other vector	

Appendix C - Impact Categories

The table below defines each impact category description and its associated severity levels. Use the tables below to identify impact levels and incident details. Note: Incidents may affect multiple types of data; therefore, SEs may select multiple options when identifying the information impact. This table is taken from US-CERT Federal Incident Notification Guidelines.

Impact Category	Category Severity Levels
Functional Impact – A measure of the impact to business functionality or ability to provide services	NO IMPACT – Event has no impact.
	NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
	MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to non-critical systems and services.
	MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
	SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.
	DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
	SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
	DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.
Information Impact – Describes the type of information lost, compromised, or corrupted.	NO IMPACT – No known data impact.
	SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
	PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
	PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
	CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated.

	CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
	DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.
Recoverability – Identifies the scope of resources needed to recover from the incident	REGULAR – Time to recovery is predictable with existing resources.
	SUPPLEMENTED – Time to recovery is predictable with additional resources.
	EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

Appendix D – Incident Attributes

The following incident attribute definitions are taken from the US-CERT Federal Incident Notification Guidelines.

Attribute Category	Attribute Definitions[5]
Location of Observed Activity: Where the observed activity was detected in the network.	LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
	LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.
	LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores.
	LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
	LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
	LEVEL 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments.
	LEVEL 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.
	UNKNOWN – Activity was observed, but the network segment could not be identified.

[5] Definitions have been altered to reflect New York State Scope.

Appendix E – State Agency Divisions of Authority

One agency, either ITS or DHSES, serves as the lead agency for State responses to a cyber incident based on the type of governmental entity affected.

- For incidents that impact Executive state agencies hosted by ITS, ITS is the lead agency.
- For most other incidents, including those that impact local governments, non-Executive agencies, public authorities, and critical infrastructure sites, DHSES is the lead agency.
- However, there are limited exceptions to these general rules, for example:
    - If a local government reports an incident to DHSES but declines State assistance, DHSES will refer the case to ITS for appropriate remediation of potential threats to State agencies.
    - If an incident affects multiple entities, a lead agency may be designated.

Other organizations that may be involved are:

- NYSIC, which will support the response through the production and dissemination of threat intelligence to inform the State's response and help potential victims protect themselves.
- NYS Division of Military and Naval Affairs (DMNA), which provides assistance to the State response as deemed necessary and directed.
- DHSES OEM, which may be designated the lead agency should the cyber incident involve physical or government service impacts designated as major incidents. Consequence management for the non-cyber impacts of the response could require an expanded State response, which may involve Multi-Agency Coordination Calls or activation of the State Emergency Operations Center (EOC), coordinated by DHSES OEM.
- Sector-Specific Agencies (SSAs) will assist with coordinating information exchange between their constituents and the State. This does not preclude involvement from any other State agency in responding to a cyber incident but, rather, serves to establish clear lines of authority and direction during time-sensitive incidents.
    - In particular, ITS will prioritize their efforts to ensure its tenants (i.e., Client Agencies) are not impacted.

Responsibility of Agencies:

- The lead agency is responsible for coordinating all aspects of the State response, notifying and updating the Executive Chamber and coordinating with the Executive Chamber on communications and other issues as necessary
- The lead agency will coordinate with the affected governmental entity or entities and with external response entities such as federal agencies and federally designated Information Sharing and Analysis Centers.
- The lead agency is responsible for notifying the Division of Budget (DOB) and Office of General Services (OGS) when fiscal impacts are expected, or additional resources are needed to respond to or remediate the incident.
- All State agencies, including SSAs, that may manage their own connections with the victim, will work with and through the lead agency to carry out their responsibilities.

Please note that the lead agency does not necessarily perform all response functions. More

often than not, this will include a multi-agency response, and the lead agency can call on other agencies to perform certain activities as needed.

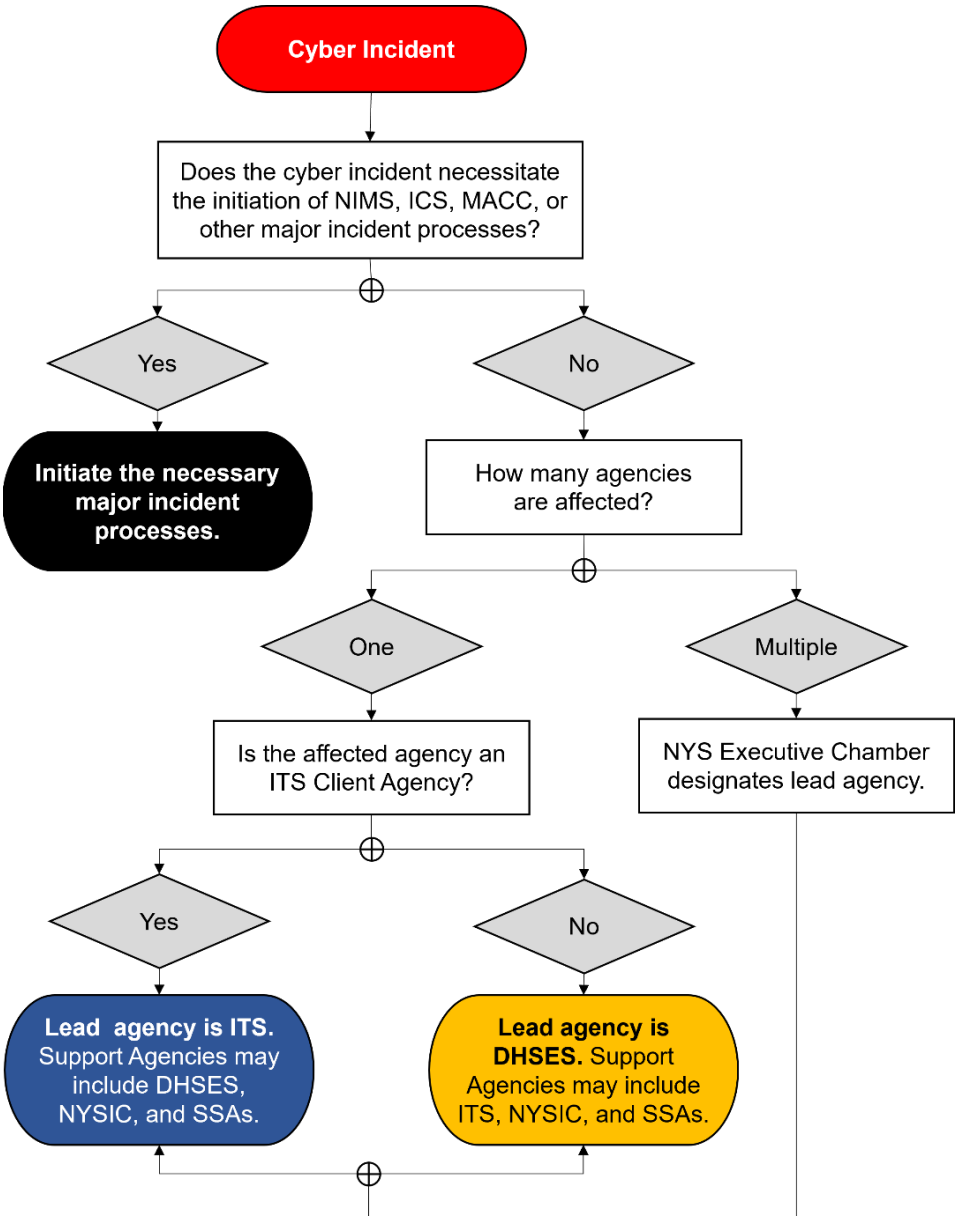


Figure 2 – Lead Agency Designation for Cyber Incident Response