



Cyber Security Policy P03-001
V3.1

Cyber Incident Reporting Policy

Original Publication Date: June 16, 2003

Revision Date: May 3, 2011

Thomas D. Smith
Director
Office of Cyber Security
New York State Division of
Homeland Security and Emergency Services
State Office Campus, Building 7A
1220 Washington Avenue
Albany, New York 12242



CYBER SECURITY POLICY

Reference:	P03-001, V3.1
Policy Title:	Cyber Incident Reporting Policy
Replaces & Supersedes:	Cyber Security Policy P03-001 V3.0, September 24, 2010
Authority:	Section 715 of the Executive Law
Issued By:	Thomas D. Smith, Director, NYS Office of Cyber Security
Original Publication Date:	June 16, 2003
Issue Date:	May 3, 2011

TABLE OF CONTENTS

TABLE OF CONTENTS	3
PURPOSE	4
SCOPE	4
ROLE OF THE NYS ENTITY IN CYBER INCIDENT RESPONSE	4
ROLE OF THE NYS OCS IN CYBER INCIDENT RESPONSE	4
POLICY	5
PART 1. WHAT IS A CYBER SECURITY INCIDENT?	5
PART 2. WHAT TYPES OF CYBER INCIDENTS SHOULD BE REPORTED?	5
PART 3. WHO SHOULD REPORT CYBER INCIDENTS?	6
PART 4. HOW SHOULD CYBER INCIDENTS BE REPORTED?	6
PART 5. WHAT INFORMATION SHOULD BE REPORTED?.....	7
PART 6. CONFIDENTIALITY OF INFORMATION	7
DOCUMENT CHANGE MANAGEMENT	7
DEFINITIONS & ACRONYMS	8
CONTACT INFORMATION	8
APPENDIX A – INCIDENT NOTIFICATION REPORT	9
APPENDIX B – INCIDENT NOTIFICATION XML SCHEMA	11

PURPOSE

The purpose of this policy is to define a process and *procedure* for *State Entities (SEs)* to report cyber security *incidents* to the New York State Office of Cyber Security (OCS). Reporting *incidents* to a central group promotes collaboration and *information* sharing with other entities that may be experiencing the same or similar problems. Some of the benefits this provides include the following:

- The ability to coordinate activities among *SEs* experiencing similar *incidents* to help identify and resolve the problem more quickly than if done separately.
- The ability to coordinate *SEs* that may be pursuing legal actions against the intruder.
- The ability to warn and share preventative *information* to help other *SEs* protect themselves from similar attacks.
- The ability to collect Statewide *information* on the types of *vulnerabilities* that are being exploited, frequency of attacks and cost of recovering from an attack.

The goals of this policy are to ensure that a *SE* recovers from an *incident* in a timely and secure manner and to minimize the impact on other *SEs*.

SCOPE

This policy applies to all *SEs*. This Policy is not intended to unilaterally change the terms and conditions of employment. All *SEs*, when coming into compliance with this Policy, must consider all terms and conditions of employment including collective bargaining agreements.

Those State governmental entities not covered by this policy, who wish to voluntarily comply with the reporting process, are invited to do so.

ROLE OF THE NYS ENTITY IN CYBER INCIDENT RESPONSE

All *SEs* must report to OCS those cyber *incidents*, as specified in Part 2, in conjunction with taking appropriate actions to isolate and contain damage.

ROLE OF THE NYS OCS IN CYBER INCIDENT RESPONSE

Upon report of a cyber *incident*, OCS will work with the impacted *SE* to assess the nature and extent of the event and to approve and/or establish an *incident response* strategy for investigation, containment, mitigation and follow-up.

The OCS Cyber Incident Response Team (IRT) will assess the situation, analyze the entity's ability to respond, and provide a recommendation to the OCS Director as to whether or not OCS IRT should be deployed.

OCS IRT is capable of performing forensics, log and malware analysis as well as reverse engineering. OCS IRT will also recommend steps to remediate the problem and mitigate future attacks.

In those situations where OCS IRT is deployed, the Director of OCS, in close consultation with the impacted *SE*, will make the final decision as to who will be the primary response coordinator. A meeting will be held immediately with senior staff of the respective *SE* to clarify roles and steps in responding to the event.

To further situational awareness, OCS posts a Cyber Alert Level Indicator on its website. The Alert Level Indicator shows the current level of malicious cyber activity and reflects the potential for, or actual damage. The Cyber Alert Level Indicator is updated when there is a significant change in the potential for malicious activity and is reviewed minimally on a weekly basis.

POLICY

Part 1. What is a Cyber Security Incident?

A cyber security *incident* is considered to be any adverse event that threatens the *confidentiality, integrity* or *availability* of *SE information* resources. These events include, but are not limited to, the following malicious activities:

- Suspected criminal use of systems or services, including:
 - Identity theft
 - Disclosure, destruction, or alteration of *SE* managed systems or *data*
- Compromise of a government web page
- Compromised password(s)
- Attempts (either failed or successful) to gain unauthorized access to a system or its *data*
- Unwanted disruption or *denial of service (DoS)*
- Unauthorized use of a system for the transmission, processing or storage of *data*
- Changes to system hardware, firmware or software characteristics without the *SE's* knowledge, instruction or consent
 - Execution of *malicious code*, often referred to as malware, such as *viruses, Trojans, worms* or *botnets*
- Attempts (either failed or successful) to cause failures in critical infrastructure services, loss of critical supervisory control and data acquisition (SCADA) systems
- Attempts (either failed or successful) to cause failures that may cause loss of life or significant impact on the health or economic security of the State

Part 2. What Types of Cyber Incidents Should be Reported?

The following types of *incidents* should be reported to OCS:

Unauthorized Access

- Report successful, unauthorized access to *SE* systems (e.g., web site defacements, unauthorized root or administrator access).
- Report unsuccessful attempts only if they are considered to be persistent (e.g., someone from the same source keeps locking out accounts trying to brute force passwords, an automated script keeps probing a *SE's* web server causing response problems).
- Report suspected unauthorized access, even if unproven, if you believe the *incident* may impact other *SEs*.

Malicious Code

- Report instances of *viruses, Trojans, worms, botnets* or other *malicious code* that have had widespread impact or adversely affected one or more mission critical servers at your site.
- Report *malicious code* blocked by email proxies or other anti-virus software only if it seems to be persistent and beyond current Internet norms.

Denial of Service (DoS)

- Report all *denial of service* attacks that adversely affect or degrade access to critical services.
- Report all other attempted *denial of service* attacks only if they are persistent or significant (e.g., attempted *DoS* attacks aimed specifically at your *DNS* servers or routers would be significant.)

Reconnaissance Scans and Probes

- Scans and probes that precede or are related to the *incidents* listed above should be reported as part of that *incident*.
- Any other scans and probes should be reported only if they are persistent or significant.

Part 3. Who Should Report Cyber Incidents?

The *SE* Information Security Officer (*ISO*) or his/her designee is responsible for submitting *incident* reports to OCS. Reports from any other sources will be validated by OCS with the affected *SE's ISO* before action is taken.

Part 4. How Should Cyber Incidents be Reported?

All cyber *incidents* should be reported to OCS IRT using one of the following methods:

- **Email “NY IRT” in the NY-ISAC Secure Portal** (Note: address will display as “IRT, NY” in the address book).
- **Email IRT@DHSES.NY.GOV**. Please use a subject line of “NYS Cyber Incident”. If including sensitive *data*, consider using the NY-ISAC Secure Portal

or encrypting using OCS's PGP public key. The key may be found on the OCS web site at <http://www.dhSES.ny.gov/ocs/incident-reporting/>.

- **TELEPHONE 518-242-5045.** Please identify the urgency of the call. *After hours (5PM-9AM, weekends and holidays), please call NYS Warning Point at 518-292-2200 and ask to report a cyber incident to OCS.*
- **FAX (518) 322-4976.** Please call and notify OCS IRT prior to the fax being transmitted.

Reports of cyber *incidents* are to be made as soon as possible but should not delay a *SE* from taking appropriate actions to isolate and contain damage.

Part 5. What Information Should be Reported?

Reports shall include as much of the *information* contained on the NYS OCS INCIDENT NOTIFICATION REPORT form (see sample in Appendix A) as possible.

An electronic version of the NYS OCS INCIDENT NOTIFICATION REPORT is available on the OCS web site at <http://www.dhSES.ny.gov/ocs/incident-reporting/>. Alternatively, *information* can be submitted using the XML schema contained in Appendix B.

Depending on the criticality, it is not always feasible to gather all the *information* prior to reporting. Reporting should not be delayed in order to gain additional *information*. *SEs* should continue to report *information* as it is collected.

Part 6. Confidentiality of Information

Information regarding specific cyber security related *incidents* will not be publicly disclosed by OCS. OCS 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 OCS in furtherance of its statutory duties.

DOCUMENT CHANGE MANAGEMENT

Requests for changes to this Policy must be presented by the *SE ISO* to OCS. If the *State ISO* for OCS agrees to the change, he or she will formally draft the change and have it reviewed and approved through the normal OCS policy approval process. Each *SE ISO* will be responsible for communicating the approved changes to their organization.

This Policy and supporting policies and *standards* will be reviewed at a minimum on an annual basis.

DEFINITIONS & ACRONYMS

Definitions and acronyms for New York State Cyber Security policies, *standards* and *guidelines* can be found in the Definitions and Acronyms document, available at www.dhSES.ny.gov/ocs/resources/

CONTACT INFORMATION

Questions concerning this Policy may be directed to OCS at (518) 242-5045.

Appendix A

NYS OFFICE OF CYBER SECURITY INCIDENT NOTIFICATION REPORT

State Entity Name:	XYZ										
Point of Contact:											
Name	John Smith										
Office Phone	(555)555-1234										
Office Phone Extension	555										
Cell Phone	(555)555-1235										
E-mail	John.Smith@xyz.state.ny.us										
Street Address, City											
Date and Time Incident Occurred:	9/23/2010 @ 14:00										
Date and Time Incident Was Detected:	9/23/2010 @ 14:00										
Nature of Incident:	<table><tr><td><input type="checkbox"/></td><td>1 - Unauthorized Access</td></tr><tr><td><input type="checkbox"/></td><td>2 - Denial of Service</td></tr><tr><td><input checked="" type="checkbox"/></td><td>3 - Malicious Code</td></tr><tr><td><input type="checkbox"/></td><td>4 - Recon and Scans</td></tr><tr><td><input type="checkbox"/></td><td>5 - Other (describe below)</td></tr></table>	<input type="checkbox"/>	1 - Unauthorized Access	<input type="checkbox"/>	2 - Denial of Service	<input checked="" type="checkbox"/>	3 - Malicious Code	<input type="checkbox"/>	4 - Recon and Scans	<input type="checkbox"/>	5 - Other (describe below)
<input type="checkbox"/>	1 - Unauthorized Access										
<input type="checkbox"/>	2 - Denial of Service										
<input checked="" type="checkbox"/>	3 - Malicious Code										
<input type="checkbox"/>	4 - Recon and Scans										
<input type="checkbox"/>	5 - Other (describe below)										
Characteristics of Incident:											
Destination IP, Port, Protocol	N/A										
Source IP, Port, Protocol	N/A										
Placement	DMZ										
O/S version, patch release, etc.	Windows XP SP2 with September 2010 security patches										

System Function (DNS/Web Server, workstation, etc.)	Workstations	
A/V software version, latest update	Symantec Antivirus Corporate Edition V10.1 with 9/23/10 virus definitions.	
How was the incident identified? (i.e., IDS, log analysis, sys admin)	IDS system alerted on possible virus infection	
Is Personal, Private or Sensitive Information (PPSI) Present? (Yes, No or Uncertain)	Uncertain	
Scope of Impact:	2,500 workstations across multiple offices statewide have been infected so far. In some cases, processing of human service applications has been slowed.	
Additional Information:	Current anti-virus signatures did not detect this virus	
What immediate assistance can the OCS IRT offer?	Need assistance analyzing malware and getting signatures developed to cleanse infected systems.	
Confidentiality – Specify how this report may be shared:	Do Not Share: <input type="checkbox"/>	Information may not be shared beyond OCS IRT and, if necessary, law enforcement.
	Share Restricted: <input checked="" type="checkbox"/>	Information cleansed of identifying characteristics may be shared with other SEs, states and other appropriate organizations.
	Share Unrestricted: <input type="checkbox"/>	Information including identifying characteristics may be shared with other SEs, states and other appropriate organizations.
Resolution:		

CONFIDENTIAL

Appendix B

NYS OFFICE OF CYBER SECURITY INCIDENT NOTIFICATION XML SCHEMA

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="incident_report">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="external_ticket" type="xs:string"/>
        <xs:element name="submission_date" type="xs:date"/>
        <xs:element name="state" type="xs:string"/>
        <xs:element name="reporter_contact_info">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="name" type="xs:string"/>
              <xs:element name="phone">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="cell" type="xs:string"/>
                    <xs:element name="office" type="xs:string"/>
                    <xs:element name="extension" type="xs:string"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
              <xs:element name="email" type="xs:string"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="incident_characteristics">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="occurred_date" type="xs:date"/>
              <xs:element name="occurred_time" type="xs:time"/>
              <xs:element name="detected_date" type="xs:date"/>
              <xs:element name="detected_time" type="xs:time"/>
              <xs:element name="entity_name" type="xs:string"/>
              <xs:element name="location">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="street_number" type="xs:string"/>
                    <xs:element name="street" type="xs:string"/>
                    <xs:element name="city" type="xs:string"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
              <xs:element name="incident_type">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="unauthorized_access"/>
                    <xs:enumeration value="denial_of_service"/>
                    <xs:enumeration value="malicious_code"/>
                    <xs:enumeration value="recon_and_scans"/>
                    <xs:enumeration value="other"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

```

        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="how_identified" type="xs:string"/>
<xs:element name="scope" type="xs:string"/>
<xs:element name="other_details" type="xs:string"/>
<xs:element name="assistance_required" type="xs:string"/>
<xs:element name="resolution" type="xs:string"/>
<xs:element name="confidentiality">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="do_not_share"/>
            <xs:enumeration value="share_restricted"/>
            <xs:enumeration value="share_unrestricted"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="affected_hosts">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="ip_address" type="xs:string" />
            <xs:element name="placement" type="xs:string" />
            <xs:element name="port" type="xs:integer" />
            <xs:element name="protocol" type="xs:string"/>
            <xs:element name="os" type="xs:string"/>
            <xs:element name="installed_software" type="xs:string"/>
            <xs:element name="function" type="xs:string"/>
            <xs:element name="av_version" type="xs:string"/>
            <xs:element name="related_host" type="xs:string"/>
            <xs:element name="ppsi_present">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="yes"/>
                        <xs:enumeration value="no"/>
                        <xs:enumeration value="uncertain"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="attack_source_info">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="ip_address" type="xs:string" />
            <xs:element name="port" type="xs:integer" />
            <xs:element name="protocol" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```