Cyber Security Citizen's Notification Policy

A. 1bis policy is consistent with the State Technology Law, § 208 as added by Chapters 442 and 491 of the Laws of 2005. This policy requires notification to affected New York residents and non-residents. New York State values the protection of private information of individuals. The Town of Union Vale (the "Town") is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

B. The Town, after consulting with the State's Office of Cyber Security and Critical Infrastructure Coordination. (CSCIC) to determine the scope of the breach and restoration measures, must notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of the individual's private information through unauthorized disclosure.

C. A compromise of private information means the unauthorized acquisition of unencrypted computerized data with private information.

D. If encrypted data is compromised along with the corresponding encryption key, the data is considered unencrypted and thus falls under the notification requirements.

E. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

F. The Town will notify the affected individual directly by one of the following methods:

1. Written notice;
2. Electronic notice, provide that the person to whom notice is required has expressly consented to receiving notice in electronic form and a log of each notification is kept by the Town that notifies affected persons in such form;
3. Telephone notification, provided that a log of each notification is kept by the municipality that notifies affected persons; or
4. Substitute notice, if the Town demonstrates to the state Attorney General that the cost of providing notice would exceed $250,000, that the affected class of persons to be notified exceeds 500,000, or that the municipality does not have sufficient contact information. The following constitute sufficient substitute notice:
    a. E-mail notice when the Town has an e-mail address for the subject persons;

b. Conspicuous posting of the notice on the municipality's web site page, if the municipality maintains one; and

c. Notification to major statewide media.

G. The Town must notify CSCIC as to the timing, content and distribution of the notices and approximate number of affected persons.

H. The Town must notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.

I. Regardless of the method by which notice is provided, the notice must include contact information for the municipality making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

J. This Policy also applies to information maintained on behalf of the municipality by a third party.

K. When more than 5,000 New York residents must be notified at one time, then the municipality must notify the consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.

Definitions

Consumer Reporting Agency: Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. The state attorney general is responsible for compiling a list of consumer reporting agencies and furnishing the list upon request to the municipality.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form of media. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hardcopy.

Information: The representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Personal Information: Any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Private Information: Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired.

1. Social security number; or
2. Driver's license number or non-drive identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Third Party: Any non-municipal employee such as a contractor, vendor, consultant, intern, other municipality; etc.

§ 208. Notification; person without valid authorization has acquired private information

1. As used in this section, the following terms shall have the following meanings:

    1. "Private information" shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

        1. social security number;

        2. driver's license number or non-driver identification card number; or

        3. account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

    2. "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
(2) indications that the information has been downloaded or copied; or
(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

    3. "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(1) the judiciary; and
(2) all cities, counties, municipalities, villages, towns, and other local agencies.

4. "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

    1. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures.

    2. Any state entity that maintains computerized data that includes private information which-such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

    3. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

    4. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;
(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or
(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;
(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and
(3) notification to major statewide media.

5. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

6. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. (b) In the event that more tha five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

7. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

ONE STOP REPORTING

Cybersecurity Incident Reporting

Local government agencies should report a cyber incident to the **New York State (NYS) Division of Homeland Security and Emergency Services (DHSES), Cybersecurity Incident Response Team (CIRT).** Call: (844) 628-2478, email: cirt@dhses.ny.gov. CIRT serves as your 24/7 single point of contact (SPOC) in NYS to report a cyber incident. CIRT will notify all other appropriate agencies including:

- **Multi-State Information Sharing and Analysis Center (MS-ISAC), Security Operations Center (SOC)** 24/7 at (866) 787-4722, email: soc@msisac.org
- **NYS Board of Elections (BOE) Secure Elections Center** 24/7 at (833) 292-3769, email: cyberny@elections.ny.gov
- **NYS Cyber Command Center** at (518) 242-5045. After hours (5PM- 9AM EST, weekends and holidays), please call **NYS Watch Center** at (518) 292-2200 and ask to report a cyber incident to the NYS Cyber Command Center or email: cycom@its.ny.gov
- **NYS Department of Health** (DOH) at (866) 881-2809, email: ohim@health.ny.gov

Government Cybersecurity Resource List

This Government Cybersecurity Resource List provides a compilation of cybersecurity resources that are available to state, local, tribal, and territorial (SLTT) entities. The following resources were discussed at the Hudson Valley Cybersecurity Summit held at Marist College, Poughkeepsie, NY, 1Q20.

Cybersecurity Overview

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Types of cybersecurity threats include:

- **Malware** - malicious software designed to gain unauthorized access or to cause damage to a computer
- **Phishing** - sending of fraudulent emails that resemble emails from reputable sources
- **Ransomware** - malicious software designed to extort money by blocking access to files or the computer system until the ransom is paid
- **Social Engineering** - a tactic hackers use to trick the recipient into revealing sensitive information

Cybersecurity Incident Reporting

Local government agencies should report a cyber incident to the **New York State (NYS) Division of Homeland Security and Emergency Services (DHSES), Cybersecurity Incident Response Team (CIRT).** Call: (844) 628-2478, email: cirt@dhses.ny.gov. CIRT serves as your 24/7 single point of contact (SPOC) in NYS to report a cyber incident. CIRT will notify all other appropriate agencies including:

- **Multi-State Information Sharing and Analysis Center (MS-ISAC), Security Operations Center (SOC)** 24/7 at (866) 787-4722, email: soc@msisac.org
- **NYS Board of Elections (BOE) Secure Elections Center** 24/7 at (833) 292-3769, email: cyberny@elections.ny.gov
- **NYS Cyber Command Center** at (518) 242-5045. After hours (5PM- 9AM EST, weekends and holidays), please call **NYS Watch Center** at (518) 292-2200 and ask to report a cyber incident to the NYS Cyber Command Center or email: cycom@its.ny.gov
- **NYS Department of Health** (DOH) at (866) 881-2809, email: ohim@health.ny.gov

Assessments and Audits

- ***Federal level:*** **Department of Homeland Security (DHS), Cyber Resilience Review (CRR)** — CRR assessments are offered free of charge to local governments. One option is a downloadable self-assessment; the other is a facilitated, onsite 6-hour session with trained DHS representatives. https://www.us-cert.gov/resources/assessments
- ***State level:*** **NYS DHSES, Cybersecurity Incident Response Team (CIRT) and Cyber Support Element (CSE)** — http://www.dhses.ny.gov//oct/cirt/index.cfm. Eligible entities interested in any of these services should email cip.oct@dhses.ny.gov
    - **CIRT** — Provides free services for: a) incident response and digital forensics, b) application and infrastructure penetration testing, and c) cyber training and exercises.
    - **CSE** — Provides free cybersecurity risk assessments to local government including: a) external and internal vulnerability scanning, b) offsite foot-printing and network scanning, and c) cybersecurity posture assessments.

Updated: 1/26/21 by gmarchi@dutchessny.gov

Government Cybersecurity Resource List

Cybersecurity Toolkit

- ***CIS Controls Tool Mapping*** — The Center for Internet Security (CIS) Critical Security Controls (CSC) are recognized by Federal cybersecurity standards as a recommended approach for local government developing a comprehensive security program for organizations of all sizes and sophistication. DHSES CIRT has developed a resource, which maps CIS CSC to free and commercially available tools: http://www.dhses.ny.gov//oct/cirt/documents/DHSES_OCT_CIRT_CIS_Controls_Tool_Mapping_v1.1.1.xlsx

Sample Plans

- **Center for Internet Security CIS Controls** — A set of basic, foundational, and organizational controls to protect, detect, and respond to cyber incidents for organizations of varying sizes. https://www.cisecurity.org/controls/
- **Core Functions & Guidance for Cybersecurity Programs** — Provides guidance for the implementation of a strong, resilient, cyber security program. http://www.dhses.ny.gov//oct/cirt/documents/DHSES_OCT_CIRT_Core_Functions_and_Guidance_for_Cybersecurity_Programs.xlsx
- **SysAdmin, Audit, Network, and Security (SANS) Institute, Information Security Policy Templates** — Find the security policy template you need: https://www.sans.org/security-resources/policies

Other Cybersecurity Resources

- **Center for Internet Security (CIS)** — CIS offers free cybersecurity best practices, tools, membership, and services. https://www.cisecurity.org/
- **Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)** — CISA has resources, which includes best practices and a toolkit for recognizing and addressing cybersecurity risks. There are resources to address four aspects of cybersecurity: Identify, Protect, Detect, and Respond. https://www.us-cert.gov/resources/sltt
- **Federal Bureau of Investigation (FBI) –** Investigates national security and criminal cyber matters. When and what to report a cyber incident to federal govt: https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)** — MS-ISAC is a part of Center for Internet Security (CIS) and is a resource for government information sharing, early warnings and alerts, mitigation strategies, training, and exercises. https://www.cisecurity.org/ms-isac/
- **National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)** — The CSRC provides information security tools and practices, acts as a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia. It is also a good portal to find all NIST's cyber-related standards. https://csrc.nist.gov/
- **NYS Chief Information Security Office (CISO)** – Cybersecurity guidelines (e.g., cyber incident response, backing up information, etc.) https://its.ny.gov/ciso/local-government
- **NYS Intelligence Center (NYSIC), Cyber Analysis Unit (CAU) –** Cyber intelligence. Contact the NYSIC CAU at (518) 786-2191 or CAU@nysic.ny.gov

Updated: 1/26/21 by gmarchi@dutchessny.gov