NEW YORK STATE CHIEF INFORMATION OFFICER
CIO/OFT
NEW YORK STATE OFFICE FOR TECHNOLOGY

David A. Paterson
Governor

STATE OF NEW YORK
State Capitol P.O. Box 2062
Albany, NY 12220-0062

Dr. Melodie Mayberry-Stewart
Chief Information Officer and
Director of Office for Technology

New York State Information Technology Policy	**No:** NYS-P10-004
Guidance for the use of SSNs by State Government Entities	**Issued on:** 7/07/2010
	Issued By: Melodie Mayberry-Stewart State Chief Information Officer Director Office for Technology **Published By:** CIO/OFT Enterprise Strategy & Acquisitions Office **Prepared in Consultation With:** The New York State Consumer Protection Board The New York State Office of Cyber Security & Critical Infrastructure Coordination The New York State Department of Labor **Policy Owner: Counsel & Legal Services**

1.0 Purpose and Benefits of the Policy

Social Security numbers (SSNs) are highly sensitive, personal identifying information and are commonly used in identity theft and fraud. Recent changes to the New York State Labor Law and Public Officers Law were intended to implement controls on the collection and transmission of SSNs by the State and its political subdivisions, thereby reducing the potential that SSNs are subjected to unauthorized disclosure.

The New York State Personal Privacy Protection Law (Public Officers Law, Article 6-A; PPPL) has, since 1983, required State agencies to maintain in their records only that personal information relevant and necessary to accomplish a purpose of the agency required to be accomplished by

statute or executive order, or to implement a program specifically authorized by law. Further, the PPPL obligates agencies to ensure the integrity and security of personal information maintained in their records. Chapter 279 of the Laws of 2008 amended the PPPL and the Labor Law to extend to public entities certain prohibitions already applicable to commercial entities and establish specific requirements applicable to the use and transmission of SSNs. More specifically, Chapter 279 added Section 96-a of the Public Officers Law and Section 203-d of the Labor Law.

This policy describes the new requirements applicable to State government entities, providing guidance to ensure the development and deployment of technology in government is coordinated with consistent approaches for compliance. This guidance is issued by CIO/OFT after consultation with the New York State Consumer Protection Board, New York State Office of Cyber Security and Critical Infrastructure Coordination, and the New York State Department of Labor, all of whom have certain responsibilities concerning the privacy and security of personal identifying information, such as SSNs, used by State government entities. Per statutory law, an employer's failure to establish policies or procedures to safeguard against privacy breaches may be presumptive evidence of a violation. State government entities may wish to adopt agency level policies not inconsistent with these guidelines to avoid allegations of breach and imposition of authorized penalties.

2.0 Authority

Chapter 279 of the Laws of 2008 contained changes to the New York State Labor Law which went into effect on January 3, 2009, and changes to the New York State Public Officers Law, Article 6-A (Personal Privacy Protection Law), which went into effect January 1, 2010, governing the use of SSNs by state agencies and political subdivisions. Many of these changes concern the use of SSNs in technology systems, including the Internet, websites, and electronic mail.

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as Director of the NYS Office for Technology, 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 CIO/OFT Policy NYS-P08-002, Authority to Establish State Enterprise Information (IT) Policy, Standards and Guidelines.

3.0 Scope of the Guidelines

These guidelines apply to all "state government" entities, as defined in NYS Executive Order 117. It applies to state government entity "technology" "systems," as those terms are defined in the NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary: http://www.cio.ny.gov/Policy/glossary.htm

4.0 Policy Statement

NYS LABOR LAW SECTION 203-d

A new section 203-d was added to the NYS Labor Law, effective January 3, 2009. The new provisions prohibit all New York State employers, including the State in its capacity as an employer, from:

- Unless required by law:
    - Publicly posting or displaying an employee's SSN;
    - Visibly printing a SSN on any identification badge or card, including a timecard;
    - Placing a SSN in files with unrestricted access; or
    - Communicating an employee's "personal identifying information" to the general public. "Personal identifying information" means any of the following elements alone or in combination with other elements: an employee's home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, drivers' license number, or SSN; or
- Using a SSN as an identification number for purposes of any occupational licensing.[1]

Labor Law Section 203-d: (i) states it shall be presumptive evidence of a knowing legal violation of this section if an employer has not put into place policies or procedures to safeguard against such violations, including provisions to notify employees; and (ii) provides the Commissioner of Labor authority to impose monetary civil penalties for such knowing violations. Accordingly, State government entities should have policies in place to comply with the requirements of section 203-d. These policies should include:

- an outline of the prohibitions of section 203-d; and
- procedures instituted by the State government entity to safeguard against unlawful disclosure, including as applicable notice to and training of its workforce.

[1] A State government entity should consult with its Counsel's Office concerning the requirements of section 203-d of the Labor Law and their applicability to its specific circumstances.

To the extent a State government entity is using technology systems to accomplish any of the purposes described above (e.g. using the entity's employees' SSNs as identification numbers in its technology systems) it should modify its IT systems to comply with these requirements.

NYS PPPL SECTION 96-a

1. **A new section 96-a was added to the PPPL,** effective January 1, 2010 (hereinafter "Section 96-a"). It extends the prohibitions of Section 399-dd of the General Business Law to the context of the State and its political subdivisions (hereinafter "the State"). These restrictions fall into two main groups: (a) prohibitions against what the State can do; and (b) limitations on what the State can require individuals to do.

Section 96-a defines a "*social security account number*" to "*include the nine digit account number issued by the federal social security administration and any number derived therefrom*" but not "*any number that has been encrypted.*" Under Section 96-a:

Unless required by law, the State <u>shall not</u>:

- Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's social security account number.
- Print an individual's social security account number on any card or tag required for the individual to access products, services or benefits provided by the state and its political subdivisions.
- Include an individual's social security account number, except for the last four digits, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless:
    - state or federal law requires the social security account number to be on the document to be mailed; or
    - the State chooses to include the social security account number in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security account number (but social security account numbers permitted to be mailed under this exception may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened).
- Encode or embed a SSN in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the SSN.

Unless required by law, the State shall not require an individual to:

- Transmit the individual's social security account number over the Internet unless the connection is secure or the social security account number is encrypted; or

- Use the individual's social security account number to access an Internet website, unless a password or unique personal identification number (PIN) or other authentication device is also required to access the Internet website. Such passwords and PINS should be unique to the individual and based on information which is private and not generally available to others.[2]

2. Concerning NYS PPPL section 96-a, all State government entities should:

a. Make checklists concerning their use of social security account numbers and SSNs and consult with their attorneys to confirm they are in compliance with the law.

b. Review the guidance below which was developed to assist State government entities to comply with the law.

c. *With regard to printed documents*:

i. **Make a list of all the documents which the State government entity provides to individuals,** such as employees or members of the public, which show or contain an individual's SSN. These can include cards, tags, letters or forms where the SSN appears on the face of the document and cards or documents where the SSN is embedded or encoded in or on the item.

ii. **Divide this list into two types of documents,** i.e., those which are sent by postal mail for the individual's personal review only, and those which are intended for public use (e.g., a badge).

iii. **For documents intended for the individual's personal review only:**

- State government entities may only use the full SSN:
  - if required by state or federal law, or
  - in applications or forms sent by mail that include documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSN

[2] The statute contains limited exceptions for the collection, use or release of SSNs for fraud investigations, internal verification or other administrative purposes. The existence of these exceptions does not obviate the State government entity's obligation to otherwise ensure the security and integrity of SSNs. A State government entity should consult with its Counsel's Office concerning the requirements of section 96-a and their applicability to its specific circumstances.

-- but --

- for either of the above, only if no portion of the SSN is printed on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

- Otherwise, State government entities may only use the last four digits of the SSN, refraining from doing even that when possible.

iv. For documents intended for public use, State government entities should not use any printed SSNs either in part or in full.

State entities should not, unless required by law, require individuals to choose their SSN as an account ID for the purposes of identification on printed communications.

d. *With regard to e-mail:*

i. State government entities may not include full SSNs in any electronic mail that is copied to third parties, unless state or federal law requires it.

ii. Otherwise, State government entities may only use the last four digits of the SSN, refraining from doing even that when possible.

e. *With regard to Internet communications*:

i. Make a list of all Internet-related communications where the State government entity requires an individual to transmit his/her full SSN over the Internet in order to register for or file a claim for benefits or services, or where an individual is required to use his/her SSN to access the State government entity's Internet website.

ii. Divide this list into two types of communications, i.e., SSN form submissions and SSNs used for website access.

iii. For these types of communications:

- For both types of communications, unless required to do so by law, State government entities are not permitted to require the transmission of the SSN unless the transmission is via a secure (i.e., https) connection or the SSN is encrypted.

- Unless required to do so by law, a State government entity is not permitted to require SSNs to be used to access internet websites unless a password, unique personal identifier, or other authentication device is also required. In those cases in which SSNs are currently used for this purpose, a State government entity must:

- implement multi-factor authentication requiring a password, unique personal identifier, or other authentication device (e.g., a token) to establish the unique identity of the user; or

- provide users with a means of changing their user IDs from an SSN to an identifier that will not identify them personally and is not derived from the SSN. This notice could be provided to all current users of the State government entity's services in the next general postal or online mailing. For prospective users of the State government entity's services, any registration screen that asks for the creation of a user ID should contain a prominent disclaimer warning the individual to exercise care in the selection of a user ID with language such as *"Choose an alias to protect your identity. Do not choose any information that identifies you personally (e.g., a Social Security number)."*

f. *With regard to claim form submissions, either printed or electronically*:

- Unless required to do so by law, State government entities are not permitted to require individuals to print their full SSNs on claim forms, unless required by state or federal law or for internal verification, fraud investigation or administrative purposes.

A worksheet is attached to the end of this policy to further assist State government entities complying with these new laws. See Attachment A.

5.0 Best Practice Guidelines

State government entities should use these guidelines as needed to ensure a consistent approach to complying with the law. This policy takes effect upon publication. The CIO/OFT Enterprise Strategy and Acquisition Services Unit shall review the policy at least once every two years to ensure relevancy. CIO/OFT may also, from time to time, communicate with State government entities about this policy and work with them to ensure State IT systems are designed and functioning in compliance with this policy.

6.0 Definitions of Key Terms

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary" http://www.cio.ny.gov/policy/glossary.htm.

State Government Entity shall have the same meaning as defined in Executive Order No. 117, first referenced above, and shall include all state agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power

and the State University of New York and City University of New York; provided, however, that universities shall be included within this definition to the extent of business and administrative functions of such universities common to State government.

7.0 CIO/OFT Contact Information

Submit all inquiries and requests for future enhancements regarding this policy to:

Policy Owner
Attention: Enterprise Strategy Governance and Acquisition Services
New York State Office of the Chief Information Officer and Office for Technology
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Telephone: 518-473-0234
Facsimile: 518-473-0327

Email: oft.sm.policy@cio.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
http://www.cio.ny.gov/policy/technologypolicyindex.htm

8.0 Revision Schedule and History

Date	Description of Change
7/07/2010	Original Policy Release
7/07/2012	Scheduled Policy Review

9.0 Related Documents

None.

ATTACHMENT A: Worksheet

Under provisions of the new section 96-a of the Personal Privacy Protection Law, Public Officers Law, Article 6-A (the "PPPL"), as amended by chapter 279 of the Laws of 2008 and effective January 1, 2010, state agencies and political subdivisions are subject to new restrictions on the collection and use of Social Security numbers (SSNs).

This Worksheet is intended to assist state agencies in complying with the PPPL. Instructions and examples of responses are provided below. The Worksheet is suggestive only and does not constitute legal advice.

Q. 1 HOW AND WHY DOES MY AGENCY COLLECT SSNs?

Identified instance in which SSNs are collected	**In which formats are the SSNs collected?**	**What agency purpose is served by collecting SSNs in this instance?**	**What is the legal authority for collecting SSNs in this instance?**	**How are these SSNs transmitted?[3]**	**Are changes needed to comply with §96-a?**	**Timetable for indicated changes**
Instructions: Using a new row for each entry, identify an instance in which the agency collects SSNs from individuals.	**Instructions:** For each instance identified in the first column, identify the format for the collection, of SSNs e.g., application forms [web and/or paper], claim forms [web and/or paper], website access.	**Instructions:** For each instance identified in the first column, explain what agency purpose is served by collecting SSNs from individuals.	**Instructions:** For each instance identified in first column, identify the legal authority for the collection of SSNs.	**Instructions:** For each instance identified in first column, identify **the manner of transmission** (e.g., by web transmission; or by fax to an agency fax machine).	**Instructions:** For each specific format identified in first column, identify the necessary remediation.	**Instructions:** For each specific format identified in first column, identify target completion date and any milestone dates.
Example #1: On applications for agency benefits or services.	**Example #1:** On applications for agency benefits or services (web and paper).	**Example #1:** For personal identification and for tax calculation and reporting. State	**Example #1:** Federal or NYS tax law; NYS Personal Privacy Protection Law	**Example #1:** Web application form transmitted through non-secure (i.e.,	**Example #1:** Change page to https.	**Example #1:** Change completed by law's effective date of January 1,

[3] The new SSN law addresses *transmission* of SSNs. State government entities should also review and confirm with their legal counsel whether the manner in which they *maintain* SSNs complies with the PPPL.

		government entity needs to collect and maintain SSN in agency file for these purposes.	(especially the "relevant and necessary" provisions).	non-https) connection.		2010, or as reasonably soon as possible thereafter.
Example #2: Used as an identifier for logging in to a website.	**Example #2:** Login credentials on website.	**Example #2:** For personal identification and to authenticate the individual's identity for web access.	**Example #2:** Well-intentioned but ill-advised effort to comply with laws requiring virtual access security.	**Example #2:** Web page transmitted through non-secure (i.e., non-https) connection. Also, authentication by one-factor, public information (i.e., SSN by itself).	**Example #2:** Connection change same as Example #1. Authentication change requires either non-SSN authenticator or SSN with password or other unique personal identifier.	**Example #2:** Connection change same as Example #1. Page re-design for authentication change by (milestone and completion dates).

Q. 2 HOW AND WHY DOES MY AGENCY <u>USE</u> SSNs?

How does my agency use SSNs it collects?	**Why does my agency use SSNs in this manner?**	**What is the legal authority for this use?**	**What are the security risks?**	**Are changes needed to comply with §96-a?**	**Timetable for indicated changes?**
Instructions: In separate boxes in this column, identify the format for each use, e.g., on cards, tags or forms, on printed materials such as envelopes, letters, postcards or flyers mailed to the individual, or on e-mail messages, for	**Instructions:** For each specific use identified in first column, explain why your agency uses SSNs in this manner, and the justification for such use. If the manner of use is on printed or electronic materials mailed to the individual, indicate whether the purpose of the use is as part of an enrollment or application process, or to confirm the	**Instructions:** For each specific use identified in first column, identify the legal authority for the use of SSNs in this manner.	**Instructions:** For each specific use identified in the first column, review **how the SSNS are displayed or transmitted**, e.g., would the SSN as displayed on the communication be visible to persons other than the SSN owner?	**Instructions:** For each specific use identified in first column, identify the necessary remediation.	**Instructions:** For each specific format identified in first column, identify target completion date and any milestone dates.

fraud investigation, internal verification or administrative purposes.	accuracy of the SSN, or to establish, amend or terminate an account, contract or policy.				
Example #1: On tax forms mailed to the individual.	**Example #1:** To enable individual to report taxable benefits. State government entity is required to show SSN on tax form.	**Examples #1:** Federal or NYS tax law; NYS Personal Privacy Protection Law (especially the "relevant and necessary" provisions).	**Example #1:** If the SSN as displayed on the tax form is visible through the window of the mailing envelope.	**Example #1:** Tax form should always be accompanied by a cover letter which does not display the SSN.	**Example #1:** Cover letter should be included with next tax form mailing.
Example #2: As personal ID on cards, tags for customers and employees to use in order to access benefits or services.	**Example #2:** For personal identification.	**Example #2:** Well-intentioned but ill-advised effort to comply with laws requiring physical access security.	**Example #2:** SSN can be seen by anyone viewing the card, tag or form. Includes encoded or embedded SSNs on cards or documents.	**Example #2:** Phase in new personal ID program that does not allow for use of SSN as personal ID.	**Example #2:** For new IDs, immediately prohibit use of SSN. Phase-in conversion of existing IDs by (milestone and completion dates).
Example #3: Posting on publicly accessible websites or otherwise making available for public inspection *newly received documents containing SSNs* filed with the agency	**Example #3:** Newly received court documents; commercial code filings; clerk's office documents.	**Example #3:** Collection and use made pursuant to the relevant laws pertaining to those specific filings with the requisite State government entity. Public release of the documents to adhere to those laws as well as to government transparency laws and principles.	**Example #3:** SSN can be seen by anyone viewing the site or document.	**Example #3:** SSNs should be redacted from lists prior to posting and documents prior to inclusion in open record repository.	**Example #3:** Immediately correct web postings.

pursuant to court rules, commercial code laws, or other legal requirements *after* the new SSN law became effective.					
Example #4: Having posted on publicly accessible websites or otherwise made available for public inspection *previously received documents containing SSNs* filed with the agency pursuant to court rules, commercial code laws, or other legal requirements *before* the new SSN law became effective.	**Example #4:** Previously received and posted court documents; commercial code filings; clerk's office documents	**Example #4:** Collection and use made pursuant to the relevant laws pertaining to those specific filings with the requisite State government entity. Public release of the documents to adhere to those laws as well as to government transparency laws and principles.	**Example #4:** SSN can be seen by anyone viewing the site or document.	**Example #4:** No, unless requested to do so by an individual to whom the SSN pertains. Redacting SSNs from previously posted documents wholesale without individual prompting would be an optimal practice, should resources permit doing so.	**Example #4:** For documents previously made available for public inspection, redact upon request of individual to whom the SSN pertains.