OSA WRITTEN INFORMATION SECURITY PROGRAM

I. Program Statement

The purpose of this program is to implement the provisions of M.G.L. c. 93H and associated regulations, 965 CMR 3.00, et seq., relative to "personal information",[1] as that term is defined in c. 93H, that is collected, maintained, used, and disclosed by the Massachusetts Office of the State Auditor (OSA). As used throughout the statute, the associated regulations, and this written information security program ("WISP"), "personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. The WISP shall be consistent with the safeguards for protection of personal information of a similar character set forth in other state or federal laws and regulations applicable to OSA information and already in place, including but not limited to: the Fair Information Practices Act, M.G.L. c. 66A, § 1 et seq.; the Criminal Offender Record Information Act, M.G.L. c. 6, §172, et seq.; and 965 CMR 2.00, et seq.

The OSA is committed to an environment where personal information in any form is available for use to support the mission, goals, and objectives of the OSA, but that also safeguards personal information in that the OSA: (1) ensures the security and confidentiality of such information in a manner fully consistent with industry standards and other provisions of law; (2) protects against anticipated threats or hazards to the security or integrity of such information; and (3) protects against unauthorized access to or use of such information that creates a substantial risk of identity theft or fraud.

---

[1] Section 1 of M.G.L. c. 93H defines "personal information" as follows:

A resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

(a) Social Security Number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. Written Information Security Program

A. Designation of Employee

The Director of Information Technology is responsible for the design, supervision, implementation, coordination, and maintenance of the WISP.

B. Risk Assessment

The OSA has conducted a risk assessment to determine reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other record containing personal information, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks. In particular, the OSA identified records[2] containing personal information (exclusive of employee-owned computers or storage media, though policy dictates that all storage media used by OSA employees should be OSA-issued); determined which Divisions collect, store, use, and disclose personal information in order to perform their governmental or statutory functions and duties and to accomplish their governmental purposes; and conducted an identification of information that may constitute "personal data," as that term is used in M.G.L. c. 66A, the Fair Information Practices Act, namely, "any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual; provided, however, that such information is not contained in a public record."

The OSA has identified the universe of reasonably foreseeable internal risks, but this paragraph does not necessarily indicate that such risks are likely to eventuate: physical records containing personal information may be accessed by employees, visitors, and cleaning crews; offices may not be locked; physical files may be left unattended in common spaces and storage areas may be unsecured; and electronic records containing personal information may be accessed by employees, inadvertently because workstations are left unattended after employees have logged on, or deliberately by unauthorized users accessing computerized databases.

The OSA has identified the universe of reasonably foreseeable external risks, but this paragraph does not necessarily indicate that such risks are likely to eventuate: physical records containing personal information may be taken out of the office so that an employee may work at home, attend a hearing, audit, meet with a prosecutor, etc., or may be sent away for outside storage. Electronic records containing personal information may be taken out of the office and lost or stolen: unencrypted personal information may be stored on notebooks or storage media (OSA or employee-owned) which may be left unattended in automobiles, libraries, residences, or other places and may be stolen or lost. Departing employees may have had access to physical or electronic records containing personal information.

---

[2] As used here, "record" or "records" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Unencrypted personal information may be forwarded electronically (through e-mails and attachments) and over unsecure networks from an OSA employee to his or her personal e-mail account (for example, to be able to work from home, though OSA policy forbids this), between OSA employees working together, between OSA employees and other agencies, or between the OSA and individuals working with the OSA. The OSA points out that personal information in either physical or electronic form may be disclosed to prosecutors in the course of preparing for prosecution or other state or federal agencies in the course of an investigation or administrative hearing, and the disclosure of such information in court filings would not necessarily violate M.G.L. c. 93H. This is because, by definition, "personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public, and the OSA is subject to and has had experience handling "personal data" under c. 66A.

C. Collection, Storage, Use, and Disclosure of Personal Information

1) Collection and Storage of Personal Information

As discussed herein, in order to perform its governmental or statutory functions and duties and to accomplish its governmental purposes, the OSA must collect and store personal information. By way of example, and not exhaustively, the OSA collects and stores information from auditees, employees, witnesses, agencies, victims, job applicants, and, specifically in criminal or civil investigations, from and about targets, witnesses, and victims. In civil cases, personal information which is not otherwise obtainable from publicly available information, or from federal, state or local government records lawfully made available to the general public, may be contained in administrative or agency records that are collected from agencies such as the Department of Social Services, the Registry of Motor Vehicles, the Department of Revenue, Mass Health, and the Department of Transitional Assistance. In fraud cases, personal information may be contained in police reports, Board of Probation reports, warrants, and reports of witness interviews that are collected by fraud examiners.

The OSA will collect and store personal information in a way that allows it to perform its governmental or statutory functions, duties, or purposes, but safeguards personal information, and to that end:

(a) The OSA will collect and store personal information as required by federal or state law.

(b) With respect to personal information that the OSA is not required by federal or state law to collect and store, but which is necessary to collect and store in order to accomplish its governmental purpose, the OSA will collect and store the minimum amount of personal information necessary to accomplish its governmental purpose.

(c) When requesting personal information either required by law or necessary to accomplish a governmental purpose, the OSA will make every reasonable effort to maintain the privacy of anyone whose personal information is collected. Furthermore the

OSA will keep secure and disclose information only in accordance with the law, a court order, or written policies for the protection of personal information.

(d) To the extent reasonably technically feasible under the circumstances, the OSA will not collect personal information through e-mail unless the personal information is sufficiently encrypted that it cannot be read by unauthorized persons.

(e) The OSA will control access to stored records containing personal information. The OSA will restrict physical access to records containing personal information to those who need to see the personal information in order to accomplish a governmental purpose. OSA employees will handle personal information discreetly and will guard against unauthorized access to records containing personal information.

(f) The OSA will not store electronic records containing personal information on computers, storage, or electronic devices that are not encrypted or otherwise secured against unauthorized access. Any OSA electronic data/documents leaving OSA premises must be on an OSA-owned and encrypted device. OSA employees are prohibited from transferring OSA stored personal information to personally owned computers or storage devices.

(g) Where possible, the OSA will develop unique personal identifiers unrelated to the personal information. For these purposes, the last four digits of a person's Social Security Number can also be used as a unique personal identifier.

(h) Upon separation from employment, an employee's supervisor or an appropriate member of the Human Resources Division will determine that the departing employee does not have access to physical or electronic records containing personal information.

2) Use and Disclosure of Personal Information

As discussed herein, in order to perform its governmental or statutory functions and duties and to accomplish its governmental purposes, the OSA must use and disclose personal information. By way of example and not exhaustively, the OSA discloses personal information to other law enforcement authorities, prosecutors, and others.

The OSA will use and disclose personal information in a way that allows it to perform its governmental or statutory functions, duties, or purposes, but safeguards personal information and to that end:

(a) The OSA will use and disclose personal information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public, or that it is required by law to disclose, e.g., by the

Public Records Law, M.G.L. c. 66, § 10, or the Fair Information Practices Act, M.G.L. c. 66A, § 1.

(b) The OSA may disclose personal information in documents being filed with the court by prosecutors, provided, however, that with respect to the filing of court documents, the OSA will ensure that prosecutors in possession of personal information obtained by the OSA, comply with M.G.L. c. 66A, the Fair Information Practices Act ("FIPA"), and the Supreme Judicial Court's Interim Guidelines for the Protection of Personal Identifying Data in Publicly Accessible Court Documents.

(c) In non-litigation contexts, the OSA will take appropriate measures to ensure that personal information is not disclosed to anyone but the person to whom such disclosure is intended. The OSA will determine whether it must send personal information through the mail and, if so, the OSA will take reasonable steps to ensure that such personal information is received only by the recipient, for example, by marking envelopes "personal and confidential."

(d) To the extent technically feasible (and taking into account the other provisions of this plan, including the appropriate use and disclosure of personal information), the OSA will encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information that will be transmitted wirelessly. If the record containing personal information is not sufficiently encrypted, it should not be transmitted.

3) Handling of Personal Information

The OSA will minimize the risks of inadvertent or unnecessary disclosure of personal information and to that end:

(a) OSA employees should not leave personal information (in physical files or on computers or other electronic equipment having such personal information stored on it) in the open where it may be accessed by unauthorized individuals, and will not transport or store personal information outside the office where it may be accessed by unauthorized individuals unless appropriate measures are taken to ensure the confidentiality, security, or integrity of the information. For example, employees who take electronic files containing personal information off the premises will make reasonable efforts, including but not limited to speaking with OSA's Information Technology Department about technological resources available, to ensure that personal information being taken off the premises is secure.

(b) The OSA will not leave voice mail messages containing personal information on voice mail systems.

(c) The OSA will not fax documents containing personal information without taking measures to ensure their confidentiality, e.g., that the recipient is alerted to expect the fax and asked to retrieve it immediately.

(d) To the extent possible and consistent with the OSA's ability to accomplish its governmental purposes, the OSA will not ask individuals seeking general information contained in OSA records for personal information in order to look up information in OSA records; however, the OSA will ask individuals seeking their own personal information contained in OSA records for a unique personal identifier unrelated to the personal information in order to look up the individual's own information. For these purposes, the last four digits of a person's Social Security Number can also be used as a unique personal identifier.

(e) OSA employees are required to report to the Director of Information Technology inappropriate disclosure or loss of records containing personal information, whether accidental or intentional.

4) Retention of Personal Information

To the extent required by law, the OSA will retain personal information.

5) Destruction of Personal Information

To the extent permitted by law, e.g., M.G.L. c. 30, § 42, and unless needed for a continuing purpose, the OSA will destroy records containing personal information. When discarding or destroying records in any medium containing personal information, the OSA will meet the minimum standards set forth in M.G.L. c. 93I for the proper disposal of records containing personal information, namely:

(a) paper documents containing personal information shall be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed; and

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

6) Notice Requirements for Improperly Disclosed Information

If personal information is improperly disclosed, the OSA will, pursuant to M.G.L. c. 93H, notify the individual whose personal information was disclosed, unless doing so would be contrary to a governmental purpose, and to that end:

(a) The OSA will provide notice as soon as practicable and without unreasonable delay to individual owners of personal information and any entity that might provide personal information to the OSA, when security measures used to protect the personal information stored and maintained by the OSA have been breached, or when personal information stored and maintained by the OSA was acquired or used by an unauthorized person, or used for an unauthorized purpose.

(b) The OSA shall cooperate with the individual owner of such information, and any entity that might have provided the personal information. Such cooperation shall include, but not be limited to, informing the individual owner or entity of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the OSA has taken or plans to take relating to the incident.

(c) The OSA shall provide notice to the Attorney General and the Director of Consumer Affairs and Business Regulation. The notice to be provided to the Attorney General and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the OSA has taken, or plans to take relating to the incident.

(d) The notice to be provided to residents shall include, but not be limited to, notice of the right to obtain a police report, how to requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(e) The OSA shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the Information Technology Division and the Division of Public Records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

(f) Notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in

writing, thereof and informs the OSA of determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the OSA that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The OSA shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident.

D. Third Party Providers

The OSA will take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.03, and will take all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.03.

E. Monitoring

The OSA's ITD may make assessments of software use, conduct announced and unannounced audits of OSA computers, and take any other actions considered necessary to assure compliance with this program. Supervisors may make assessments of employees' access to paper files containing personal information and will work with their respective employees to prevent unauthorized collection, storage, and disclosure of personal information.

F. Review of Program

The Director of Information Technology (or his or her designees) will review and, where necessary, update the WISP at least annually or whenever there is a material change in personnel, governmental, technological, administrative, or other practices that may reasonably undermine the efficacy of the program.

G. Review of Breach, Responsive Action, and Documentation of Responsive Action

Where the OSA learns that unauthorized access to physical or electronic records by an employee or third party has occurred, the OSA will review the incident in a manner commensurate with the nature and scope of the unauthorized access to determine the possible breach of confidentiality, security, or integrity of the records if any, and make any necessary changes in personnel, governmental, technological, or other business practices relating to protection of personal information. The Auditor in her discretion may impose appropriate disciplinary measures for violations of the WISP. The OSA will document any action taken.

H. Employee Training

At least annually but more often as needed, the Director of Information Technology (or his or her designee) and supervisors will ensure that OSA employees are trained in the law and this WISP relating to the proper collection, storage, use, and disclosure of personal information.

III. Computer System Security Requirements

The OSA has implemented the following computer-related security measures to the extent technically feasible:

A. Secure User Authentication Protocols

To control user IDs and other identifiers, the OSA will establish a secure method of assigning and selecting passwords consisting of at least seven letters and numbers; periodic password changes; control of data security passwords to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access; restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access to the particular system.

B. Secure Access Control Measures

The OSA will restrict access to records and files containing personal information to those who need such information to perform their job duties, and will assign a unique identification plus a password, which is not vendor supplied, to each person with computer access. OSA employees are required to close Outlook and log off their user accounts when leaving their computers unattended for a long period of time and, in any event, at the end of the work day.

C. Safeguards Against Access by Former Employees

The OSA will ensure that departing or former employees cannot access records containing personal information by terminating their physical and electronic access to such records, including deactivating their passwords and user names.

D. Encryption of Transmitted Records

Personal information, including those in wireless environments that will travel across public networks will be encrypted. If a smart phone is reported lost, the data on the portable device may be deleted remotely, but there may be a time delay. For these purposes, "encryption" means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

E. Encryption of Personal Information Stored on Notebooks and other Storage Media

Personal information stored on notebooks and other storage media will be encrypted. OSA employees who download personal information to notebooks or other storage media have been instructed to make sure the data is encrypted.

F. Monitoring

The OSA will engage in reasonable monitoring of networks and systems to determine unauthorized access to or use of personal information, and recording the audit trails for users, events, dates, times, and success or failure of login.

G. Firewalls

The OSA will install firewall protection with up-to-date patches, including operating system security patches. The firewall will, at a minimum, protect devices containing personal information from access by or connections from unauthorized users.

H. Antispyware

The OSA will install the most current version of system security agent software which will include antispyware and antivirus software, including up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and which includes security software that is set to receive the most current security updates on a regular basis.

I. Education

The OSA will train employees on the proper use of the computer security system and the importance of personal information security.

J. Restriction of Access

The OSA will restrict access to computerized records containing personal information to those employees who need to access such records in order to accomplish a governmental purpose.

K. Network Security

The OSA will maintain an appropriate level of security by permitting external access to the OSA network only through the use of a Virtual Private Network (VPN) account. The Director of Information Technology must approve all VPN access. Accessing external networks from within the OSA network is prohibited (this includes the use of PC Anywhere, GOToMyPC.com, MS Live, etc.) to connect to a home or otherwise external computer. The OSA prohibits the use of a modem in conjunction with network-connected equipment without prior written permission from the Director of Information Technology.