



The Official Website of the Executive Office for Administration and Finance

Administration and Finance

[Home](#) > [Research & Technology](#) > [Policies, Legal & Technical Guidance](#) > [Enterprise Advisories](#) > [CIO Advisory - EO 504: Security and...](#)

CIO Advisory - EO 504: Security and Confidentiality of Personal Information

From: Anne Margulies, Assistant Secretary and CIO

Date: January 8, 2009

Re: Advisory Memorandum - Executive Order 504: Order regarding the Security and Confidentiality of Personal Information

Many Executive Department agencies have already begun working towards compliance with Executive Order 504 (EO 504). In this era of constrained resources, it is more important than ever that we work together towards our common goals. The purpose of this advisory memo is to:

1. Communicate ongoing EO 504-related activities being undertaken by the Information Technology Division (ITD) and Enterprise Security Board (ESB);
2. Recommend that individual agencies coordinate their compliance efforts with the ongoing efforts of ITD and the ESB; and
3. Solicit agency input and participation in the EO 504 guidance development efforts being led by the ESB.

Information Technology Division Activities

Through the TechLaw Practice Group, ITD has conducted training for CIOs and General Counsels regarding their general obligations under EO 504. If your agency was unable to attend one of these events, ITD will be posting a link to a "Train the Trainer Program on Executive Order No. 504" webcast on ITD's [EO 504](#) website. The [EO 504](#) site currently includes materials that your agency can use to train agency management along with a checklist/timelines for agency compliance. In particular, ITD has created a checklist for agencies to use as a guide for implementing EO 504, a copy of which is attached hereto as Attachment A.

Enterprise Security Board Activities

Consistent with its obligations under EO 504, ESB is currently engaged in establishing policies, standards, forms, and process recommendations for ITD's CIO as follows:

1. Development of the portion of agency Information Security Programs (ISPs) pertaining to electronic personal information and data, as those terms are defined under M.G.L. Ch. 93H and 66A (electronic security plans or "ESP's"), which will govern agencies' collection, use, dissemination, storage, retention and destruction of electronic personal information and data;
2. Agencies' submission of ESP's to ITD for review;
3. Agencies' training of their employees and contract employees regarding agency-specific ESP's;
4. Agencies' self-audit against their ESP's;
5. ITD's conduct of EO 504 compliance and enforcement;
6. Agencies' reports to ITD of breaches of the security of electronic personal information or data ;

Request for Agency Participation in ESB Workgroups

The ESB has established several workgroups to complete the above-described activities. Towards constructing a comprehensive and inclusive secretariat and executive department input opportunity, ITD and ESB are asking secretariats and executive departments to identify their EO 504 required information security officer (ISO) and request their participation within these workgroups.

Please notify Dan Walsh, ESB Co-Chair, dan.walsh@state.ma.us, John Beveridge, ESB Co-Chair, john.beveridge@state.ma.us, and John Glennon, ESB Executive Committee Chair, john.glennon@state.ma.us, of your ISO assignments and nominees for ESB workgroup participation.

[Agency Compliance Checklist](#) 

Did you find the information you were looking for on this page? *

- ☐ Yes
☐ No

Send Feedback

