INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

October 30, 2003

The Honorable Joshua B. Bolten
Director
Office of Management and Budget
725 17th Street, N.W.
Washington, D.C. 20603

Dear Mr. Bolten:

At its September 2003 meeting, the Information Security and Privacy Advisory Board[1] addressed the issue of agencies using Web-based transactions to provide "e-government" services to members of the public. The Board identified some concerns it wished to bring to your attention, specifically, that there needs to be greater attention paid to how agency applications may affect the integrity of users' computers. A key issue was whether (and how) an application might place program code (often referred to as "plug-ins" or "mobile code") into the user's browser.

In any Web-based interaction, the server may seek to place program code onto the client's machine, and specifically into the browser (since browsers are inherently designed to make it easy to add such code). In many instances, downloading program code is useful – it can harmonize the user experience, provide functionality that the browser does not natively possess, and ensure that any action taken by the member of the public has the full context necessary for that member to make a fully informed decision. At the same time, adding such functionality alters the member's computing environment, and may give rise to security vulnerabilities or opportunities for intruding into the member's computer (including private information) and potentially raises other policy issues.

The Board was unable to find any government-wide policy advising agencies what they should or should not do when developing applications which may seek to place program code onto the

[1] The Information Security and Privacy Advisory Board was established by the Computer Security Act of 1987 and reauthorized by Title III of t he Federal Information Security Management Act of 2002. The Board is charged to identify emerging managerial, technical, administration and physical safeguard issues relative to information security and privacy. The Board is also to advise the National Institute of Standards and Technology, the Secretary of Commerce and the Director of the Office of Management and budget on information security and privacy issues pertaining to Federal government information systems.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-3357 *** Fax: 301/975-4007

client's machine. This is unlike the analogous situation involving "cookies," guidance was developed and published by the Office of Management and Budget on June 2, 1999, as part of the privacy policy on Federal web sites.

As agencies work to make applications available over the Internet to members of the public, the Board believes that there needs to be clear policy on when and how an agency may place program code on a user's computer. We recommend that OMB develop such policy, which, at a minimum, should address the following questions:

1. How can an agency provide adequate notice to the user informing them of the implications associated with downloading program code? Following are examples of relevant questions:

(a) How does an agency ensure that the program code won't conflict with or adversely affect any other application running on the user's machine (e.g., Java sandbox)?

(b) How does an agency ensure that the program code will not change the user's environment other than for the specific functionality that the program code is intended to provide?

(c) How does an agency ensure that the program code will not expose any security holes?

2. What are the liability implications if the program code adversely affects the user's environment (and, how does an agency prove that the environment was not adversely affected if the user contends it was)?

3. What are the privacy implications of placing program code on someone's machine - e.g., how does an agency ensure the program code does not expose user information unknowingly or unwittingly?

4. How does an agency obtain the user's informed consent before installing any program code?

5. How does an agency enable the user to opt out after installation and get the program code cleanly removed?

6. How does an agency ensure that the user-requested installation of program code does not place some users at a disadvantage because they may lack browsers for which the program code will work properly? As a corollary, how does the agency determine which different types of computing environments it needs to provide program code for, to ensure that some users are not disadvantaged?

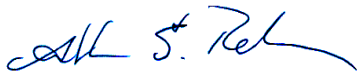
7. How does an agency ensure it knows what program code should be installed (i.e., how to know the user's environment well enough to select the proper program code)?

8. How does an agency establish appropriate controls to ensure that the program code is correct, authentic and uncorrupted? Then, how does the agency convey this information to the user?

9. How does an agency deal with hardware or software changes (or updates) that the user may make after the program code is installed?

We thank you for the opportunity to share our views.

Sincerely,



Franklin S. Reeder
Chairman