Why Internet Explorer 5.0?

- We do not have a choice.
  - Internet Explorer will be installed as a component of our next generation desktop operating system. The extent to which we might be able to disengage it needs to be determined.
  - Operating System integration.
  - Microsoft is unlikely to back away from their commitment to integrating the Web browser into the operating system.
- Office 2000 suite integration.
  - The Office 2000 suite will require of Internet Explorer. (ex. IE will be used to display help content)
- Outlook 98/2000 integration
  - Outlook 98 will require of Internet Explorer. (ex. IE will be used to display HTML mail documents)
- Browser functional equivalence.
  - Both Microsoft and Netscape browsers have similar capabilities. These capabilities are not always implemented using similar techniques.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000412

Risks:

- Two browsers on all Wintel machines.
  - IE comes in the operating system and is available for use as a browser.
  - Netscape would have to be separately installed.
- Not able to fully disengage browser.
  - May be able to remove IE icon from the desktop (to be determined).
  - Windows Explorer can still be used to access internet protocols: (ex. http and ftp).
  - Difficult to enforce Netscape as "The Browser" on the Wintel environment.
- Current Web Development.
  - Transition to IE complicated by applications that are being written to support specific capabilities on specific web systems.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000413

Risks: (continued)

- Minimal ActiveX implications.
  - Security model based on Zones (same as IE 4.0).
  - Abatement is a controlled configuration.
- Browser technology divergence:
  - Incompatible Java implementations and features.
  - Digital object and content signing.
  - Dynamic HTML.
  - Executable content.
- User confusion.
  - Installing both browser will likely cause confusion for end users.
- Infrastructure support will now be required for both browsers.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000414

Abatements:

- Enforcement of web applications guidelines for browser neutral development techniques.
- Continued emphasis on W3C standards.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000415

Internet Explorer 5.0 Evaluation:

- Developers Preview Release available 7/1/98 and shipped with the Office 2000 (version 9) Beta 1.
- Aggressively engage Microsoft on IE Beta code testing (3-4Q98).
- Beta code Testing/Assessment:
  - ActiveX implications.
  - Support for current and emerging W3C standards initiatives.
  - Operating System integration functionality and implications.
  - Impacts of new Microsoft browser initiatives.
  - Ability to disengage internet browser functions.
- 1-2Q99 stable code fully functional integration and on-site testing.
- Anticipate production release IE code tied to availability of NTW 5.0 code March 1999.
- Guideline: Do not install IE 5.0 on workstations that are not dedicated to testing.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000416

Netscape 5.0?

- Beta code available 4Q98.
- Expected to include code developed by the Mozilla public source release project.
- Production release expected 2Q99.
- Beta code Testing/Assessment:
  - Support for current and emerging W3C standards initiatives.
  - Operating System integration functionality and implications.
  - Impacts of new Netscape browser initiatives.
  - Coexistence with IE 5.0.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000417

ActiveX:

- IE 3.0 has several flaws that specifically make it a security risk.
  - ActiveX is control activation is either on or off.
  - If it is on it is on for all web pages that use it.
  - digital signing only identifies who signed a control.
  - A developer could script an existing desktop control to
  - perform malicious actions.
  - An ActiveX control can be written that will execute even though IE 3.0 ActiveX security features are turned on.
- IE 4.0 provides a mitigation strategy that can be used to control ActiveX execution based on Zones.
  - One potential problem with the zones strategy would be an exploit that used IP spoofing to fool the browser into thinking that a page was from a site in a "trusted" zone.
  - Another problem is that the user has access to the configuration options for the browser. Controlled configurations could be developed, assuming that NT logon or Network profiles could be used to enforce the configuration and that the configuration could be agreed upon by Boeing divisions.

US/States v. Microsoft
HIGHLY CONFIDENTIAL
TBC 000418