**FROM**: Academic IT Committee

Bob Buckley, Committee Chair

**TO**: Faculty Senate Executive Committee

**DATE**: February 11, 2011

**SUBJECT**: Issues related to KBox implementation

* **Licensed software**. One of the justifications for the use of the KBox monitoring tool is to monitor the appropriate use of CSUS licensed software. This assumes that the majority of software and software licenses are provided by IRT. In many cases most software and software licenses are in fact purchased by faculty, departments and Colleges. KBox would falsely report these as illegal copies.
* **Privately owned equipment**. In addition, KBox would provide the controls for limiting distribution of CSUS site licensed software to only University owned equipment. Privately owned equipment is often in use by faculty for academic purposes. Unfortunately, there is no data collected on the extent to which privately (i.e. faculty) owned equipment is routinely used for academic purposes.
* **Inappropriate implementation of remotely controlled updates and patches**. Updates and patches could be automatically installed at arbitrary times without an understanding of potential impact on academic related applications as well as the times in which the instructional use of applications would be interrupted by such background activity. IRT cannot be expected to know how, when and for what purposes such applications would be used.
* To minimize the impact on academic users, Colleges typically allow major updating and patching to occur only between semesters. Exceptions occur in critical situations within the Colleges. In such cases, the work is undertaken in such a way as to minimize the programmatic impact.
* **Anonymous System Administrators[[1]](#endnote-1)**. The central administration of KBox grants some system administration rights to unknown parities with no local accountability. For the faculty and staff within the Colleges this presents significant concerns over privacy and security. Given the lack of day-to-day knowledge of the work and needs of faculty and staff within the Colleges and Library, the granting of any system administrative responsibilities to non-local IT staff could significantly negatively impact the provision of IT services and support at the local level.

1. A system administrator is a person employed to maintain and operate a computer system and/or network. The duties of a system administrator are wide-ranging, and vary widely from one organization to another. SysAdmins are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. Other duties may include scripting or light programming, project management for systems-related projects, supervising or training computer operators, and being the consultant for computer problems beyond the knowledge of technical support staff. To perform his or her job well, a system administrator must demonstrate a blend of technical skills and responsibility. [↑](#endnote-ref-1)