**Section 109.40 Department Access to E-mails and Internet Communications**

a) Personal Information on Department Computers – The privacy of materials kept in electronic data storage, internet use, and electronic mail when using Department computers is not a right, nor is it guaranteed. Most materials on Department systems are, by definition, public records. As such, they are subject to laws and policies that may compel the Department to disclose them.

b) Monitoring of Computer Use – The facility director shall ensure e-mail and internet use by individuals on all State-owned computers is monitored to ensure compliance with sanctioned uses. Individuals using State-owned computers for sanctioned uses shall be informed, prior to use, that such use shall be monitored. The Office of Management Information Systems (MIS) administers the Department’s information systems and data processing equipment. MIS may monitor computer use and system accesses by any individual or organizational entity in DHS. This includes the potential to monitor transaction executions, file accesses, communications such as e-mail and accesses of external resources such as the internet.

c) Contents of E-mail – The contents of electronic messages may be seen by a system administrator in the course of routine maintenance or in order to dispose of undeliverable messages. In addition, electronic mail systems store messages in files (e.g., the file containing a user’s inbound mail). These files are copied in the course of system backups and these backup copies may be kept long after original messages are deleted.

d) System Files and Logs – In the course of resolving system performance or security problems, system administrators may examine the contents of files that control the flow of tasks through the system or that grant unauthenticated access to other systems. This includes systems logs that document activities of users.