Security Awareness Message
February 2012
Mobile Computing Tips

Prohibition Against Installing Unauthorized Software

To prevent infection by computer viruses, and to be certain that OCFS complies with software licensing restrictions, you must NOT install any software without prior documented approval. Unauthorized software may contain viruses, worms, Trojan horses, and other software which may damage or compromise OCFS information and systems. You may avoid compromising your security by:

- Avoiding suspicious websites
- Keeping your operating system current
- Keeping Antivirus and Firewalls current
- Refraining from opening suspicious attachments

Laptop Encryption

You are responsible for verifying the encryption status of your state-issued laptop. In order to verify the encryption status, you should look for the encryption ICON in the system tray area (next to where the clock is located) at the bottom right of the screen. The McAfee ICON looks like small picture of a monitor. Details can be retrieved for McAfee Encryption by right clicking the ICON (step 1) and then click status (step 2). The Pointsec ICON is a white "P." If you place the mouse over the ICON it will display Pointsec. Details can be retrieved by right clicking the ICON and then click Information. Should you encounter an issue where a laptop does not appear to be encrypted or you are not sure if the laptop is encrypted, you should immediately bring it to the attention of your LAN Administrator for corrective action.

HSEN network

Reminder: You are responsible to make sure that you connect your laptop to the network for a minimum of 120 minutes each month (preferably overnight) in order for your laptop to receive the latest software updates and operating system patches. If your laptop is not connected to the HSEN monthly, it may be disconnected from the network. If you have any questions, please contact your LAN Administrator.

SSL-VPN

This technology allows OCFS users (with a valid HSEN ID), to access approved OCFS applications, including Webstar, from their **Non-State Owned PCs** via the use of an SSL VPN solution. In order to maintain the confidentiality, integrity and availability of information accessed through this technology, it is critical that the Local District or Agency maintains compliance with all OCFS policies, including installing and maintaining required Antivirus and Firewall software. Failure to maintain required up-to-date Antivirus and firewall software places the district, agency, and network at risk. Viruses and other threats, such as keyloggers (which track or log keystrokes on a keyboard), could potentially threaten the confidentiality, security and integrity of your data.

Outlook Web Access to Exchange 2007- Security

Public or Shared should be selected if you are on a public or shared computer. Selecting Private computer when you are at a library or hotel computer is a security risk. Private computer should only be selected on a computer used only by you. When using Public or Shared, the session will time out after 15 minutes.

If you have questions regarding Information Security you can email your questions the acceptable use mailbox at: ocfs.sm.committee.acceptable-use

OCFS Information Security Unit- 2/12