5003 Mobile Devices and Wireless Networking

I. Applicability

This policy establishes rules for all employees and users granted remote access to DHS information systems through the use of mobile devices (e.g. cell phones, smart phones, tablets, laptops, etc.) approved by the DHS IT Security Office. Mobile devices and outside networks without any connectivity to DHS Information Systems do not fall under the purview of this policy.

II. Mobile Devices

(a) All mobile device users must complete the "Mobile Computing Device Agreement," located on DHS Share to gain access to DHS information systems for each device used. Mobile devices shall be used only by the person authorized to use the device by the DHS Mobile Computing Device Agreement (located here: http://dhsshare/Security/Lists/DHS5008%20Submission/AllItems.aspx)

(b) Users of mobile devices on the DHS network must complete all required DHS Privacy and Security Training. Failure to complete training will result in the device being deactivated. The device can be reactivated once training is complete.

(c) Users have no reasonable expectations of privacy in the use of DHS devices or systems. DHS reserves the right to monitor and log all wireless communication device activity with or without notice, including email and all website communications. Any wireless or mobile device connected to the DHS network is subject to routine or automated scans and can be removed based upon threat. All violations are subject to disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions."

(d) Only devices approved by the DHS IT Security Office can be used to process confidential DHS or client information. This means that employees will not transfer confidential information to a non-DHS device (such as a personal computer, cell phone, tablet, or any mobile device, or a peripheral or external storage device not approved by the Office of Systems Technology (OST)). This also means DHS workforce members or contractors cannot use personal phones or unencrypted devices for business related tasks such as taking pictures for investigations or the use of text messaging DHS or client related data.

(e) Mobile devices must be fully encrypted using DHS enterprise approved encryption software (See DHS APM 126, "Acceptable Encryption").

(f) Laptops, notebooks, and tablets must be connected to the DHS Network at least once monthly for a minimum of 24 hours to allow for updating of system software.

(g) To protect against unauthorized use, loss, or theft, mobile devices should be locked away when not being used.

(h) Handheld computers and smartphones must be configured to automatically lock after five (5) minutes of inactivity at most and require a four or greater digit PIN to unlock the device.

(i) If the mobile device is suspected to be lost or stolen, the user must immediately report the loss as a security incident. All DHS workforce members must report privacy or security incidents, even suspected incidents and may utilize the Security Incident Reporting system on DHS Share to do so. (See DHS Policy 1003, "Privacy and Security Incident Reporting").

(j) Failing to return any state-owned mobile device upon request will result in sanctions (See DHS Policy 4002, "Privacy and Security Sanctions"), and legal action and/or fines. Employees who fail to return any state-owned mobile device when concluding employment must pay to replace the device.

(k) Information on state owned mobile devices covered by this policy, other than laptops, will be wiped upon ten (10) consecutive, unsuccessful device logon attempts.

III. Remote Access

(a) Access to systems containing protected data is prohibited from outside of the state network. System access will be permitted through the use of the DHS Portal or an approved solution by the DHS Chief Information Security Officer (CISO) prior to access. The DHS Chief Information Officer (CIO) reserves the right to approve or terminate a user's remote access privileges at any time.

(b) Requests for remote access or teleworking must be submitted to the Security Gateway Administrator using DHS Form 359 (for DHS employees) or Form 5002 (for contractors), "DHS Systems Security Access Request." Only the employee/user who signs the request form shall be authorized remote access to DHS information systems.

(c) Access is granted on an as-needed basis with approval from the division Authorized DHS Approving Manager (ADAM). The employee requesting access must be aware of all DHS policies and stay up to date with all Privacy and Security Training requirements.

(d) Users may refer to OST's "Remote Access Standards" or contact the IT Security Office for more information.

IV. Wireless Networks

(a) All wireless Access Points connected to the DHS system must be documented and approved by the DHS CIO or CISO. Any wireless device connected to the DHS network is subject to routine or automated scans and removal from the network

based upon threat. Peer-to-peer wireless connections are prohibited. Rogue access point devices located on the network shall be confiscated by the IT Security Office pending outcome of investigations.

(b) Persons utilizing a DHS guest wireless system (internet access for non-DHS users) shall have no expectation of privacy in any data transmitted through such systems. Guest wireless systems and all data transmitted on those systems may be monitored, recorded, and disclosed at the discretion of DHS and other state entities.

(c) Guest wireless systems must not be used to transmit confidential, unencrypted, or sensitive information (e.g., PHI or PII).

(d) Transmitting Federal Tax Information (FTI) data outside of the DHS network is prohibited. FTI data is not allowed on a wireless system and cannot be transferred via email, fax, or multifunction device. An employee who transmits FTI data to a wireless or unsecured device or system will be terminated. Questions or concerns should be directed to the IT Security Office.

(e) Users may refer to OST's "Wireless Access Standards" or contact the IT Security Office for more information.

V. Failure to Comply

Violations of this policy may result in disciplinary action as outlined in DHS policies 4002, "DHS Privacy and Security Sanctions," as well as 1084, "Employee Discipline: Conduct/Performance."