U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Policy Number 4004.1: Use of ICE-Issued Mobile Devices.

Issue Date: 3/3/2014
Effective Date: 3/3/2014
Superseded: None
Federal Enterprise Architecture Number: 306-112-002b

1. **Purpose/Background.** The technological advances embodied in newer-generation mobile devices have introduced significant changes to the way government agencies communicate and conduct business. Mobile devices such as smartphones, tablet devices, cellular telephones, personal communication devices, multifunctional wireless devices, messaging devices, and any other wireless devices capable of storing, processing, or transmitting sensitive information provide additional capabilities beyond voice, email and calendar functionality, which present opportunities for innovation, agility and flexibility in the workplace and a more mobile workforce. However, these additional capabilities present unique challenges to existing policies on limited personal use of government equipment and services and information technology (IT) security. This Directive clarifies the scope of allowable limited personal uses on government-issued mobile devices, while still protecting the integrity and security of the U.S. Immigration and Customs Enforcement (ICE) enterprise and without inhibiting the use of ICE-issued mobile devices for official government business.

   The purpose of this Directive is to provide a policy and procedures to ICE employees on the use of ICE-issued mobile devices for official government business and limited personal use. All ICE personnel must comply with the requirements in this Directive. This Directive applies only to Apple and Android devices. This policy does not specifically apply to ICE's Blackberry assets. ICE's Blackberries are wholly controlled by ICE and individual users do not have the ability to add, customize, or modify the devices' functionality. The controls applied to the Blackberries are similar to those applied to ICE's laptops and desktops, thus limiting the exposure presented to ICE's information. This policy does not apply for devices procured through Certified Undercover Operations.

2. **Policy.** ICE personnel may be issued mobile devices for official government business use. Limited personal use of ICE-issued mobile devices is authorized for ICE personnel only when such use incurs no additional charges to the government and if it does not interfere with official duties, inhibit the security of agency records and information systems, or cause degradation of network services. Supervisors may further restrict personal use based on the needs of the office or due to problems with unauthorized or inappropriate use. Any incident (suspected or actual) that potentially introduces a virus/worm or other malicious software, the release of sensitive information, or potentially compromises the confidentiality, availability, integrity, authentication or non-repudiation of the ICE enterprise must be reported immediately to the ICE Service Desk

and the employee's supervisor regardless if the incident occurred while the mobile device is used for official business or limited personal use.

3. Definitions. The following definitions apply for purposes of this Directive only:

3.1. Agency Records. Records created by, used by, or in the possession of an agency which deal with the work of the agency to include federal records as defined under the Federal Records Act and agency records as defined under the Freedom of Information Act (FOIA).

3.2. Government Equipment or Services. Equipment or services purchased, leased, or owned by the government. This includes, but is not limited to, IT equipment, pagers, Internet services, email, library resources, telephones, mobile devices, facsimile machines, photocopiers, and office supplies.

3.3. IT Equipment. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT equipment includes, but is not limited to: ICE workstations or laptops, mobile devices, related peripheral equipment, and software.

3.4. Non-Work Time. The time when ICE personnel are not performing an activity for the benefit of the Agency and/or under the control or direction of the Agency. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after a workday, weekends, or holidays.

3.5. Mobile Device. A hand-held computing device, typically having a display screen with a touch input and/or miniature keyboard with capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes smartphones, tablet devices, cellular telephones, personal communication devices, multifunctional wireless devices, messaging devices, and any other wireless devices capable of storing, processing, or transmitting sensitive information. This does not include laptops.

3.6. Personal Use. Activity that is conducted for purposes other than accomplishing official government business.

3.7. Secure Container. A mobile device management solution that enables creation of an isolated or contained portion of the mobile device resources for applications to run, and restricts the mobile device's ability to alter or read data outside its specific contained environment. The secure container protects data transmitted over the air and stored on the device as well as prevents mixing with data outside of the secure container, minimizing potential data loss or leakage. This mobile device management solution is commonly referred to as a securely contained "sandbox" environment. In some cases, more than one secure container may exist on the ICE-issued mobile device.

3.8. **Smartphone.** A cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, email, Web browsing, still and video camera capabilities, MP3 player capabilities, video viewing and often video calling. In addition to their built-in functions, smartphones can run applications, turning the device into a mobile computer.

4. **Responsibilities.**

4.1. **The Office of the Chief Information Officer (OCIO)** is responsible for:

1) Establishing the security standards for the ICE-issued mobile devices;

2) Ensuring that employees complete mandatory information assurance awareness training;

3) Providing for the distribution, operation, and administrative support of ICE-issued mobile devices;

4) Maintaining an inventory of licenses for ICE-owned software installed on each ICE-issued mobile device;

5) Ensuring that the secure container technology is installed onto all mobile devices;

6) Maintaining a list of approved applications and digital media for official government business use inside the secure container;

7) Coordinating with Directorates and Program Offices on the development and installation of applications and digital media for official government business use, to determine if applications and digital media are compatible with the mobile device operating system, for the bulk purchase of applications and digital media for official government business use, and for the procurement of services when developing applications and digital media for official government business use;

8) Coordinating with the Office of the Chief Financial Officer (CFO) and the Office of Acquisition Management (OAQ) for the bulk purchase of applications and digital media for official government business use, and for the procurement of services when developing applications and digital media for official government business use;

9) Purchasing (by authorized OCIO employees) individual applications and digital media for purposes of reviewing, testing, and evaluating applications and digital media for future official government business use; and

10) Monitoring the activity on all ICE-issued mobile devices to ensure compliance with this Directive.

4.2. Directorates and Program Offices are responsible for:

1) Maintaining an inventory of ICE-issued mobile devices by serial number, user's office, user's name, and service start/end dates;

2) Coordinating with OCIO on the development and installation of applications and digital media for official government business use, to determine if applications and digital media are compatible with the mobile device operating system, for the bulk purchase of applications and digital media for official government business use, and for the procurement of services when developing applications and digital media for official government business use;

3) Coordinating with CFO and OAQ for the bulk purchase of applications and digital media for official government business use and for the procurement of services when developing applications and digital media for official government business use; and

4) Using Directorate and Program Office funds to purchase additional mobile device accessories (e.g., protective cases, holsters, car chargers, extra power adaptors) beyond the basic accessories issued with the mobile device that are necessary to support their missions.

4.3. Supervisors are responsible for:

1) Ensuring that their employees sign the Mobile Device User Agreement when issued a mobile device;

2) Ensuring that their employees report any lost, stolen, damaged, destroyed, compromised, or non-functional ICE-issued mobile devices to the Property Custodian for their office; and

3) Taking appropriate actions when notified of non-compliance with this Directive, or if problems arise from unauthorized or inappropriate use.

4.4. ICE Employees are responsible for:

1) Completing annual mandatory information assurance awareness training and as appropriate, annual ethics training (new employees are responsible for completing initial ethics training);

2) Signing the Mobile Device User Agreement when issued a mobile device;

3) Complying with this Directive, applicable OCIO guidance or policy, and all applicable federal requirements;

4) Using only ICE-approved and authorized mobile devices for official government business use;

5) Abiding by all federal, state, and local laws for using mobile devices while operating a motor vehicle (in accordance with Executive Order 13513, Federal employees are banned from text messaging while driving federally owned vehicles, and text messaging to conduct official government business while driving non-government vehicles. Agency heads may exempt certain employees, devices, or vehicles that are engaged in or used for protective, law enforcement, or national security responsibilities or on the basis of other emergency conditions.);

6) Purchasing applications and digital media (e.g., music, books, movies) for limited personal use outside the secure container only with the employee's own personal funds and through their own personal user accounts;

7) Reporting lost, stolen, damaged, destroyed, compromised, or non-functional ICE-issued mobile devices to the Property Custodian for their office; and

8) Reporting any unauthorized incident (suspected or actual) to the ICE Service Desk and their supervisor.

5. Procedures/Requirements.

5.1. Privacy Expectations. Employees do not have any right to, nor expectation of, privacy in the use of any government equipment or services, including Internet or email services. Furthermore, use of government equipment or services, whether within the secure container or not and for whatever purpose, is not private or anonymous. By accepting the ICE-issued mobile device, employees consent to having their device usage monitored, including the contents of any files or information maintained or passed through that device. Employees who use ICE-issued mobile devices should be aware that data on the device related to personal use (e.g., personal text messages sent and received, pictures taken, or videos recorded) may be considered a government record subject to official use and disclosure in certain circumstances, such as the use of personal email or text messaging for official business. Official disclosure of personal data from these devices may be ordered or otherwise required in circumstances such as agency litigation, FOIA requests, and the prosecution of ICE criminal investigations, where it is determined that the data or records in question are federal records, agency records, or otherwise subject to disclosure under statute or other legal requirement. Any such disclosures would occur on a case-by-case basis depending on the specific facts of the situation.

5.2. ICE employees issued mobile devices will ensure that official law enforcement sensitive (LES), Sensitive Personally Identifiable Information (Sensitive PII), and any other sensitive information created or captured by the employee for official purposes, or maintained in or derived from agency records, will be maintained within a secure container if possible and that the contents of the devices will be protected and safeguarded from unauthorized disclosure in accordance with applicable laws, regulations, and policies.

5.3. ICE reserves the right to wipe and clean the memory and SIM card of any ICE-issued mobile device at its own discretion, and it need not take into account any consideration other than its own convenience and interests when deciding to exercise this right. ICE will not be liable for any personal data lost when the memory and SIM card of any ICE-issued mobile device is wiped.

5.4. For use within the secure container, ICE employees will create whatever account is required for use of the device (e.g., the Apple ID) using their ICE email address. For personal use outside of the secure container, ICE employees may create such an account with their personal email address.

5.5. ICE employees may not use their government-issued Travel Card or Purchase Card for purchases or account fees on their ICE-issued mobile device, including, but not limited to, downloading and installing applications and digital media. Except as provided for in section 4.1.9, above, ICE employees are not authorized to make individual purchases of applications and digital media for official government business use. Bulk purchases of applications and digital media may only be made in accordance with sections 4.1 and 4.2, above. Applications and digital media for official government business use may only be installed within the secure container by OCIO. Applications and digital media for limited personal use installed outside of the secure container may only be purchased with the employee's own personal funds and through the employee's own personal user account.

5.6. Unauthorized or inappropriate use of ICE-issued mobile devices may result in the loss or limitation of an employee's privilege of personal use. ICE employees may also face administrative action ranging from counseling to removal from the Agency, as well as any criminal or civil penalties or financial liability, depending on the severity of the misuse.

5.7. **Prohibited Uses of ICE-Issued Mobile Devices.** The following are prohibited at all times including during official use, limited personal use and non-work time. Other prohibited uses will be included as new threats emerge:

1) Using an ICE-issued mobile device to view, download, store, display, transmit, or copy any materials that are sexually explicit; are predominately sexually oriented; or are related to gambling, illegal weapons, terrorist activity, or any other activity prohibited by law or agency policy. However, this use is permitted if the activity relates to a law enforcement investigation, operation, or prosecution, or relates to a personnel issue or complaint. Viewing, downloading, storing, displaying, transmitting, or copying child pornography on an ICE-issued mobile device is never permitted.

2) Entering, processing, storing, or transmitting classified information.

3) Disabling or modifying any security configuration of the ICE-issued device set by ICE (e.g., disabling the pin code lock).

4) Deliberately introducing or failing to report accidental introduction of viruses or other malicious software.

5) Using an ICE-issued mobile device as a staging ground or platform to gain unauthorized access to other systems.

6) Acquiring, reproducing, transmitting, distributing, or using proprietary data or material, or computer software and data in violation of law, including copyright, trademark, patent, or privacy laws.

7) Sending or receiving official government business communications via personal email accounts.

8) Using ICE email addresses for subscribing to anything other than official, professional, or job-related websites. The use of the ICE email address is approved for creating the user accounts as described in 5.4 above.

9) Engaging in any fundraising activity, endorsing any enterprise, service or product, or participating in lobbying or partisan political activity as defined by the Hatch Act and related regulations (e.g., activity directed at the success or failure of a political party, candidate for partisan political office, or partisan political group). However, fundraising activity certified by OPM in support of the Combined Federal Campaign or natural disasters is authorized.

10) Using ICE-issued mobile devices for commercial purposes to support a private or personal business, including assisting family members, relatives, friends or other persons in such activities. For example, this prohibition includes employees using government equipment or services to run a business.

11) Creating, copying, or transmitting any material or communications that are illegal or offensive to fellow employees or the public, such as hate speeches, or material that ridicules others based on race, creed, religion, sex, disability, national origin, or sexual orientation. This does not apply when it is being sent for an official agency purpose such as material that is part of an investigation, operation, or prosecution, or it is being sent to appropriate personnel as part of a complaint or personnel action.

12) Creating, copying, or transmitting SPAM, PHISHING, chain letters, or any unofficial mass mailings, regardless of subject matter.

13) Allowing any third party use of the ICE-issued mobile device by non-ICE employees including, but not limited to, friends and family members.

5.8. Authorized Limited Personal Uses of ICE-Issued Mobile Devices. The following limited personal uses are authorized only outside of the secure container environment and when no unofficial charges are applied to the ICE-issued device account:

1) Using personal email sites (e.g., Gmail, Yahoo, AOL, etc.), educational webmail (*.edu), and government contracting companies' webmail. However, since personal email messages sent outside the secure container do not have the same level of protection as official communications sent within the secure container, employees should observe proper Operations Security, Communications Security, and Information Security practices when using personal email sites.

2) Sending and receiving personal text messages. However, since text messaging does not have the same level of protection as official communications sent within the secure container, employees should observe proper Operations Security, Communications Security, and Information Security practices when using text messaging.

3) Downloading applications and digital media. Applications and digital media (e.g., music, movies, books) will only be downloaded using the employee's own personal funds and through the employee's own personal user account.

4) Synchronizing with a personal computer to transfer personal data.

5) Making non-security configuration (e.g., ring tones, background images) changes.

6) Subscribing to, downloading, or streaming media or other automatic Internet services.

7) Using or accessing web-based applications, social media, or social networking sites.

8) Using navigation and/or GPS features.

9) Using personal shopping sites.

10) Making personal calls while on official government travel.

11) Using internet-based phone services (e.g., Skype).

12) Other allowable uses will be considered as technologies evolve.

6. Recordkeeping. Copies of the Mobile Device User Agreement will be stored within the ICE Virtual University in the employee's transcript.

7. Authorities/References.

7.1. Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving," (October 1, 2009).

7.2. 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

7.3. 5 U.S.C. §§ 7321-7326 (The Hatch Act) and implementing regulations at 5 C.F.R. Part 734.

7.4. 5 U.S.C. § 735, Employee Responsibilities and Conduct.

7.5. 5 U.S.C. § 552, Freedom of Information Act.

7.6. Personal Property, DHS Management Directive (MD) 0565.

7.7. Sensitive Systems Handbook, DHS MD 4300A.

7.8. DHS E-mail Usage, DHS MD 4500.1.

7.9 Personal Use of Government Office Equipment, DHS MD 4600.1.

7.10. Personal Communications Device Distribution, DHS MD 4700.1.

7.11. Individual Use and Operation of DHS Information Systems/Computers, DHS MD 4900.

7.12. DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012).

7.13. ICE Policy 1033.1, "ICE Employee Code of Conduct," (August 7, 2012).

7.14. Personal Property Operations Handbook, ICE Office of the Chief Financial Officer, Office of Asset Administration, Property Management Branch (March 2011).

8. **Attachments.** Mobile Device User Agreement.

9. **No Private Right.** These guidelines and priorities are not intended to, do not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.

Daniel Ragsdale
Deputy Director
U.S. Immigration and Customs Enforcement