11-1: Introduction

In this new era of mobile computing, powerful handheld devices, wireless communications, cloud services, and social networks are creating new boundaries that blur the lines between personal computing and corporate resources. Federal agencies must embrace this new world and be ready to mobilize their business, transform their organizations, and modernize their technical infrastructures to meet the significant opportunities as well as challenges that mobility brings to the federal workplace, including compliance with all applicable federal laws and regulations.

Responding to today's mobile opportunities requires that we not only embrace and support the use of these new devices and technologies, but also manage and secure them. Mobile device management (MDM) tools provide the capabilities to secure, monitor, manage, and support mobile devices. MDM functionality typically includes inventory management, monitoring, administration, over-the-air distribution of applications, and data and configuration settings for all types of mobile devices, including mobile phones which are connected to the HUD network, smartphones, tablet computers, laptops, mobile printers, etc., for both government and non-government furnished equipment. This policy does not apply to cellular phones (those with voice only), Wi-Fi devices, satellite phones, or any other device which does not connect to the HUD network. For more information about the policies regarding those telecommunication services and devices, see Chapter 14 of the Administrative Services Policy Handbook (2200.1) and Telecommunications Management (2241.1).

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of mobile devices in our workforce while minimizing cost and downtime. Mobile Information Technology (IT) devices increase the productivity of the Department's employees by providing wireless communications to access HUD information systems when and where such access is needed. These devices can be used for a range of functions, including but not limited to, telephone, electronic mail, address book, calendaring, and Internet access. While these devices provide benefits to HUD employees and the organization, they also pose risks to the Department because they are easy to misplace or have stolen and are vulnerable to malware, spam, electronic eavesdropping, and other security threats that may result in the exposure of sensitive information.

11-2: Purpose

This policy establishes HUD policies and standards for controlling mobile computing and storage devices that contain or access HUD information resources.

This policy should manage the risks of mobile computing by providing guidelines ensuring that:

- HUD mobile computing assets are appropriately procured, managed, and secured, including compliance with all federal laws and regulations;
- The Office of the Chief Information Officer (OCIO) can continue to support and innovate HUD's wireless enterprise and optimize associated resource requirements by implementing standard mobile IT management processes, procedures, and devices;
- The confidentiality, availability, and integrity of HUD information is protected during storage and transmittal; and
- Mobile users are properly trained and made aware of their responsibilities.

This policy applies to mobile smartphones and tablet devices either acquired by HUD (HUD-owned mobile IT devices). Details about the HUD Bring Your Own Device (BYOD) process and policy will be discussed in another chapter of the Information Resource Management policy. Specific roles and responsibilities for the various offices and the participating employee can be found in section 11-5.

This policy ensures that the mobile IT devices (HUD-owned):

- Are used in a manner consistent with HUD's mission and achieve intended results;
- Are protected from waste, fraud, abuse, and mismanagement; and
- Adhere to Federal laws, regulations, and guidelines.

11-3: Effective Implementation Date

This policy is effective upon the issuance date of this policy.

11-4: Policy

It is HUD's policy to develop and maintain security control standards for all HUD-owned mobile IT devices that create, access, process, or store HUD information, and for all information created, collected, and processed on behalf of HUD on these devices. This policy also covers personally-owned mobile IT devices that access HUD information. The Office of the Chief Information Officer (OCIO) directs and

oversees compliance with the security control standards for mobile IT devices. Therefore, this policy is established to adequately safeguard the management of mobile IT devices connected to HUD's network or authorized cloud solutions. Mobile device care is the responsibility of each mobile device user. Failure to adhere to the guidelines listed below may result in personal liability, retraction of device privileges, and/or disciplinary action.

A. This policy applies to all HUD employees and includes all departmental offices and organizations, including headquarters, regional, and field locations.

B. To fully leverage the government's buying power, improve the government's management of its information resources, and drive down costs, HUD will acquire all IT mobile devices through the General Services Administration (GSA) Federal Strategic Sourcing Initiative (FSSI) Wireless solution under commercial practices and Federal Acquisition Regulations (FAR) Part 8 – Required Sources of Supplies and Services.

C. The IT mobile device equipment standards are Apple iOS and Android OS devices at N-1 (new model minus one version). HUD will acquire previous generation devices if functional requirements are met and reduce the total cost of ownership. OMB M-16-20, Memorandum Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services, states that previous generation devices can typically equally meet all the requirements at prices significantly lower than the latest models.

D. Only HUD OCIO-authorized mobile IT devices may be connected to the HUD network or authorized cloud solutions.

E. It is prohibited to distribute HUD-owned mobile IT devices to contract personnel, Fair Labor Standards Act (FLSA) covered employees, interns, or other non-government employees. Requests for a FLSA covered employee waiver to this policy must be approved by the General Deputy Assistant Secretary (GDAS) or designee.

F. Authorized use of mobile IT devices includes any activities that:

    1. Directly support official government business activities and communications; and

2. Comply with:

    - Information Technology Security Policy, HUD Handbook 2400.25, Rev. 4;

    - Information Resource Management Policy, HUD Handbook 2400.1;

    - Limited Personal Use of Government Office Equipment Policy, HUD Handbook 2400.1, Chapter 8 and Appendix 6;

    - Information Technology Security Policy, Handbook 2400.25, Rev. 1 The U.S. Department of Housing and Urban Development Departmental Rules of Behavior **for Use of Information Resources**; and

    - Rules of Behavior for Connecting Mobile IT Personal Device to HUD Resources, as applicable.

F. Use of HUD-owned IT devices for other than authorized government business or limited personal use is prohibited.

G. Defective HUD-issued smartphones should be reported to the HUD National Help Desk (888-297-8689). OCIO will provide the resources required to replace HUD-issued smartphones that are defective and covered under the manufacturer warranty.

H. HUD-issued devices that are lost or stolen must be reported promptly (within 24 hours) to the HUD National Help Desk and will be remotely wiped and have email redirected. This wiping process will erase all information from the device so HUD data cannot be gathered by external parties. Users must also contact their Accountable Officer to initiate a HUD Form 27, Report of Survey. OCIO will report lost and stolen devices to the Office of Administration, Property Management Branch. It is important to note that the Office of General Counsel has determined that employees can be held financially liable if they are found to be willfully or negligently responsible for lost, damaged or stolen government property.

I. International voice and data services are authorized for and limited to:

    - HUD Senior Executive Service (SES) staff. HUD SES staff will contact the HUD National Help Desk at least one week prior to the

international service requirement and identify both the travel date(s) and location(s); and

- HUD employees approved by the Assistant Secretary, General Deputy Assistant Secretary (GDAS) for official international business. HUD employees will submit approved international service requests through their appropriate Office Technology Coordinator (OTC). The OTC will contact the HUD National Help Desk at least one week prior to the international service requirement and identify executive approval, along with the applicable travel date(s) and location(s).

J. Remote access to HUD Mobile and HUD WorkPlace from a mobile IT device is not supported by OCIO. Classified information is not authorized on any mobile IT device. All information downloaded to the device is subject to the Freedom of Information Act (FOIA). Should a device be determined to be subject to a FOIA request, the device will be required to be turned into the Office of Administration's FOIA Branch for an undetermined period.

K. Misuse of departmental resources via a mobile IT device may result in administrative and disciplinary actions. For more details, see the Rules of Behavior for Remote Access.

L. This policy does not imply authorized use of mobile IT devices outside official duty hours.

11-5: Roles and Responsibilities

Management of mobile IT devices is directed by the OCIO. It is the OCIO's responsibility for managing these devices to ensure that the mobile IT devices connected to HUD resources comply with all federal and departmental policy and procedures. As part of this duty, the OCIO has established this policy and associated guidance for the management of all mobile IT devices connecting to HUD resources. This section details the roles and responsibilities for each method of connecting to HUD resources.

Government employees do not have a right, nor should they have an expectation, of privacy while using HUD-owned mobile IT device, including accessing the Internet and using email and voice communications. If employees wish that their private activities remain private, they should avoid using the HUD-owned mobile IT device for limited personal use. By acceptance of the HUD-owned mobile IT device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed-through that device.

The Office of the Chief Information Officer will:

1. Designate a dedicated mobile devices and services category lead. The lead will report to the CIO and will establish and maintain an agency-wide inventory of mobile contracts, identify opportunities for contract consolidation, track savings, and make policy recommendations to the CIO.

2. Centrally negotiate, acquire, support and manage the delivery of HUD-owned mobile IT devices and associated services and licenses to realize cost efficiencies, ensure accountability and control of departmental resources, and ensure compliance with federal technology and security standards.

3. Work with the program and support offices annually to adequately plan for HUD-owned mobile IT device requirements during each budgetary cycle, as required by HUD's established IT Capital Planning process.

4. Identify the baseline number of HUD-owned mobile IT devices to be funded, maintained, and supported by the OCIO and allocated to the Office of the Secretary, SES, and program and support offices. The OCIO will include in this inventory baseline, the phones provided under the Assistive Technology Program and in response to approved reasonable accommodation requests.

5. Additional HUD-owned mobile IT device requirements will be assessed annually by the OCIO, with input from the program or support offices, through the IT Capital and Acquisition planning process. This process will also update the mobile IT device baseline. OCIO will provide information to the program and support offices regarding mobile IT device industry information (i.e., current features, services, and associated costs) and management information (i.e., inventory listing and usage) to ensure effective and prudent use.

6. Distribute and manage the HUD-owned mobile IT devices for the Department, in compliance with established IT Capital Planning and IT acquisition requirements.

7. Provide funding and support resources, as approved by the IT Capital Planning process, for HUD-owned mobile IT devices for the Office of the Secretary, SES, approved personnel, and approved reasonable accommodation requests. OCIO will provide information to the program and support offices regarding HUD-owned mobile IT device

features, services, and associated costs to ensure effective and prudent use.

8. Ensure that HUD-owned mobile IT devices comply with applicable HUD IT security policies and guidance. HUD will use a MDM solution to manage and monitor mobile devices issued to HUD employees. The MDM will enforce mobile security settings that include:

    a. Requiring a password to access each mobile IT device. Failure to enter the password successfully after 10 attempts will reset the device to factory default setting and automatically wipe the device. This wiping process will erase all information from the device so HUD data cannot be gathered by external parties.

    b. Requiring the use of a complex password that includes a minimum of one alphabetic, one numeric, and one special character.

9. Monitor and review HUD-owned mobile IT device voice and data use to ensure:

    a. A sound understanding of HUD-owned mobile IT device needs to support continuous and effective departmental communications;

    b. A proper balance between HUD-owned mobile IT device cost and customer satisfaction requirements;

    c. Compliance with regulatory requirements and standards for HUD-owned mobile IT devices;

    d. Realization of cost savings and/or cost avoidance in the acquisition and management of mobile IT devices; and

    e. The optimal benefits are realized from investments in HUD-owned mobile IT devices and services in supporting program delivery.

10. Advise and assist program and support offices regarding HUD-owned mobile IT devices to ensure effective and prudent use.

11. Periodically conduct market surveys to ensure that HUD-owned mobile IT devices and services are being acquired at the most economical costs available.

12. Provide leadership, guidance, and oversight in the establishment and maintenance of inventories of HUD-owned mobile IT devices, and associated software and licenses, where applicable.

13. Ensure that HUD-owned mobile IT devices and services are upgraded as required to provide reliable voice and data capabilities.

14. Monitor and manage the level of availability, performance, and restoration for HUD-owned mobile IT devices and associated services.

14. Notify the appropriate program or support office of receipt of any damaged or returned HUD-owned mobile IT devices.

15. Develop and disseminate annual HUD-owned mobile IT device reports for each program and support office.

16. Develop and disseminate quarterly usage reports to ensure adequate and appropriate HUD-owned mobile IT device usage. OCIO reserves the right to terminate government-provided services for the HUD-owned mobile IT device for non-use. OCIO will contact the appropriate Program Office OTC or point of contact for any device identified with 30 days non-usage to confirm information is correct before action is taken. The policy for terminating voice and data services for non-use is 60 days. Upon service termination, devices will be collected by OCIO and eligible for redistribution by the applicable Program Office OTC or point of contact.

17. Conduct annual user update requests for HUD-owned mobile IT devices.

18. Ensure that program and support offices comply with the HUD-owned mobile IT device guidance.

19. Establish and maintain security configurations for all HUD-owned mobile IT devices, including patching and upgrading of software/firmware.

20. Develop and maintain mobile device policies, procedures, and guidelines regarding HUD-owned IT mobile device management.

OCIO reserves the right to recall/disconnect government-provided mobile devices due to budget restrictions or changes to deployment priorities.

21. Provide basic device training to users receive a HUD-owned mobile device.

22. 22. OCIO is responsible for replacing HUD-issued devices for SES staff that are damaged and cannot be repaired by HUD's smartphone contractors.

Program and support offices will:

1. Recognize the OTC or designated Point of Contact identified for each program and support office as the authorized individual for approving and submitting requests to the OCIO for HUD-owned mobile IT devices and services.

2. Manage their allotted devices. Each program office is allocated a specific number of smartphone devices based on available inventory and funding. This distribution level ensures devices are provided, at a minimum, to all SES staff and current HUD-owned mobile device users. This allocation information will be provided to each OTC. The program offices can allocate assigned devices to staff and projects based on program office priorities.

3. Address expanding mobile device requirements that exceeds their allotted distribution through the annual budget process.

4. Initiate transfer of mobile IT devices to different personnel within their program office to address program office requirements. The OTC is authorized to contact the HUD National Help Desk to open a ticket requesting the transfer the HUD-owned device from one employee to another.

5. Submit approved requests for HUD-owned mobile IT devices and services to the OCIO, and confirm Working Capital funding availability.

6. Identify business and program requirements and work with the OCIO to develop standardized, cost-effective solutions based on a common telecommunications infrastructure.

7. Review the monthly OCIO HUD-owned mobile IT device usage reports to ensure that the office is using these devices adequately and effectively; and take actions to eliminate redundant, unauthorized, or unused HUD-owned mobile IT devices.

8. Maintain inventories of the office's HUD-owned mobile IT devices and ensure compliance with associated monitoring requirements from the OCIO.

9. Include, as necessary, HUD-owned mobile IT device requirements as part of the IT Capital Planning process.

10. Submit approved waiver requests to the OCIO for distribution of HUD-owned mobile IT devices to FLSA covered employees, interns, or other non-government employees.

11. Notify OCIO of any employee separation, transfer, or termination from the Department of any personnel using HUD-owned mobile IT devices so OCIO can take the appropriate actions.

12. Notify OCIO, no less than one week prior, of any employee approved to use a HUD-owned mobile device during official international travel. International roaming services may be available temporarily for business travel only. Data rate plans for email and broadband cards are an additional cost to HUD for mobile device users traveling outside the continental U.S.

13. Confirm authorized employees with a HUD-owned mobile IT device with the OCIO annually.

14. Ensure that the office and applicable employees comply with the HUD-owned mobile IT device guidance.

15. Recognize delays in obtaining a replacement device for damaged equipment may occur.

HUD Employees will:

1. Complete the HUD annual IT Security Awareness Training within the designated timeframe and understand the security risks associated with mobile IT devices prior to requesting service or equipment.

2. Request HUD-owned mobile IT devices through the authorized OTCs in their program or support office.

3. Comply with HUD Rules of Behavior and departmental Limited Personal Use of Government Office Equipment policy.

4. Use a complex password that includes a minimum of one alphabetic, one numeric, and one special character. Failure to successfully enter the password after 10 attempts will result in the device resetting to factory defaults and automatically wiping the device. This wiping process will erase all information from the device so HUD data cannot be gathered by external parties.

5. Promptly report HUD-issued devices that are lost or stolen (within 24 hours) to the HUD National Help Desk. The device will be remotely wiped and have email redirected. This wiping process will erase all information from the device so HUD data cannot be gathered by external parties. Users must also contact their Accountable Officer to initiate a HUD Form 27, Report of Survey. OCIO will report lost and stolen devices to the Office of Administration, Property Management Branch. It is important to note that the Office of General Counsel has determined that employees can be held financially liable if they are found to be willfully or negligently responsible for lost, damaged or stolen government property.

6. Ensure that all electronic messages received or created on the device outside of the secure MDM solution that are HUD federal records are stored in or transferred to a HUD network or system.

7. Submit requests for mobile applications required for HUD business requirements to the HUD National Help Desk. These requests will be assessed and approved by OCIO for distribution to the HUD-owned mobile IT device.

8. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel, of HUD-owned mobile IT devices.

9. Immediately report any lost or stolen HUD-owned mobile IT devices to the HUD National Help Desk.

10. Return HUD-owned mobile IT devices that are damaged or are no longer required to the OCIO.

11. Due to voice plan minute restrictions, opt to use their work landline phone when at their workstation to make and receive calls.

12. Abide by the applicable laws governing the use of mobile cell phones and/or smartphones (e.g., only hands-free use and no texting while driving).

13. Ensure that the HUD-owned mobile IT device is protected from unauthorized access and is not used by any other user.

14. Comply with the HUD Mobile IT Device guidance, including use of the device for official government use and limited personal use.

15. Comply with the federal records laws and agency record retention policies and schedules for all data/communications (including text messages) downloaded or maintenance on a HUD-owned mobile IT device.

11-6: Acquisition

Acquisition of HUD-owned mobile IT devices and services is centrally administered through OCIO.

A. The OCIO is responsible for the acquisition and distribution of HUD-owned mobile IT devices for the Office of the Secretary, Senior Executive Service (SES), and approved program and support office personnel. The OCIO will ensure that anticipated HUD-owned mobile IT device requirements undergo IT Capital Planning and Acquisition processes, comply with all federal laws and regulations, and adhere to IT Security policies and procedures.

B. Requests for HUD-owned mobile IT devices for departmental personnel other than the Office of the Secretary or SES personnel must be submitted to the OCIO by the authorized program and support office OTC. Program and support offices will be required to provide funding for the purchase and maintenance of mobile IT devices for departmental personnel that exceed their designated number of devices. Therefore, program and support offices must ensure that anticipated HUD-owned mobile IT device requirements are identified each Fiscal Year in adherence to the Department's established IT Capital Planning process.

11-7: Authorities

This policy ensures compliance with the following statutes, directives, and guidance:

- E-Government Act of 2002 (44 U.S.C. Chapter 36);
- Privacy Act of 1974 (5 U.S.C. 552a);
- Federal Information Security Management Act of 2002 (FISMA), [Title III of the E-Government Act of 2002 (44 U.S.C. Chapter 36)];
- Clinger-Cohen Act of 1996 (40 U.S.C 11315);
- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource;
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control;
- National Institute of Standards and Technology (NIST) Special Publication 800-124, Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise;
- NIST Special Publication 800-121, Guide to Bluetooth Security;
- NIST Special Publication 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks;
- NIST Special Publication 800-45, Guidelines on Electronic Mail Security;
- NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations;
- National Telecommunications and Information Administration, Manual of Regulations & Procedures for Federal Radio Frequency Management, 2015;
- 47 Code of Federal Regulations, Telecommunications Parts 0-199;
- National Archives and Records Administration, Encrypt all data on mobile computers/devices, 2009;
- NARA Bulletin 2015-02, “Guidance on Managing Electronic Messages,” 2015;

- Executive Order 13589, Promoting Efficient Spending, 2011;
- Executive Order 13513, Federal Leadership on Reducing Text Messaging While Driving, 2009;
- Freedom of Information Act (5 U.S.C. 552);
- Limited Personal Use of Government Office Equipment Policy (HUD Handbook 2400.1, Chapter 8 and Appendix 6); and
- OMB M-16-20 Memorandum Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services.
- Form HUD –22018 (03/2010) Office of the Chief Information Security Officer Rules of Behavior for Remote Access