UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS and AMERICAN OVERSIGHT Plaintiffs, v. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT Defendant.	D. Mass No. 21-10761-NMG

SUPPLEMENTAL DECLARATION OF RICHARD CLARK

I. INTRODUCTION

I, Richard J. Clark, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am employed as the Chief Technology Officer (CTO) in the Office of the Chief Information Officer (OCIO) for the U.S. Immigration and Customs Enforcement (ICE). I have held this position since January 28, 2019. Prior to this position, I was the Chief Enterprise Architect (CEA) in OCIO for ICE. I have over twenty-five years of experience in Information Technology (IT). I have a degree in Electrical and Computer Engineering from Clarkson University.

2. ICE OCIO is responsible for providing information technology services and products that enable ICE to meet its mission. Services that the OCIO provides include the purchasing and contracting of mobile devices, their supporting services, mobile device management

infrastructure, electronic mail (e-mail) and supporting infrastructure for e-mail operations for all ICE employees.

3. As the CTO and CEA I have specific knowledge of the policies, procedures and capabilities of the ICE infrastructure and contracted services pertaining to email and mobile devices issued by ICE to its employees.

4. Pursuant to the Court's opinion, dated June 3, 2022, I make this supplemental declaration to address the Court's concerns relating to data preservation on mobile phones and the process of deactivation of mobile phones. Specifically (1) the process by which it, as a general matter, deactivates and replaces employee mobile devices; (2) what, if any, steps it takes to preserve data located on mobile devices at the time they are deactivated; and (3) the dates on which each of the seven named custodians have had a mobile device deactivated since the first day of the Request period, and what steps, if any, were taken to preserve data located on each of those devices.

5. The statements contained in this supplemental declaration are based upon my personal knowledge and experience, information provided to me in my official capacity, and upon conclusions and determinations made in accordance therewith.

II. INFORMATION REGARDING DATA PRESERVATION ON MOBILE DEVICES

6. My previous declaration states that ICE OCIO does not have the capability or the supporting technological infrastructure to search mobile devices for messages.[1]

7. In its memorandum of opinion, the Court instructed ICE to provide a supplemental declaration describing the process by which ICE, as a general matter, 1) deactivates and replaces employee devices 2) what steps, if any, are taken to preserve data located on mobile devices at the time they are deactivated and 3) the dates on which each of the seven named custodians have

[1] *See* Defendant's Reply and Opposition to Plaintiffs' Cross-Motion for Summary Judgment, Declaration of Richard Clark, Doc. 37-2, February 14, 2022, ¶ 11-14.

had a mobile device deactivated since the first day of the Request period, and what steps, if any, were taken to preserve data located on each of those devices. ICE OCIO does not have a policy to preserve data on mobile phones nor does ICE OCIO have an infrastructure capability to preserve and/or store data from employees' cell phones.

8. As previously noted in my declaration, DHS Directive 141-03 provides a step-by-step guide of how individuals should preserve and maintain records, should any records be inadvertently created using chat, text, or instant messaging. The directive states that the [individual][should] "write a memo to the file. Be sure to include Date and time of the communication; Type of communication (e.g., text, voicemail, telephone call); Context of the message or conversation (electronic messages); Participants; Subject; Details on any decisions or commitments (verbal communications); Corresponding threads that precede a communication and provide more background."[2]

9. OCIO provides instructions to all ICE custodians of mobile devices on how to administratively reset and or wipe the mobile device before the mobile device is returned to its property custodian. The document with instructions is entitled "Steps to Erase All Data from iPhone_iPad.pdf," and provides a step-by-step guide to demonstrate how to erase data from mobile devices. *See* Exhibit 1.

10. Specifically, the instructions state the following: 'Log into your iOS device with your user passcode then tap on settings; Select the ">" to the right of your name and under your Apple ID account information select "iCloud" and turn off any iCloud services, then tap on "Find my iPhone"; Slide the "Find my iPhone" button to the off position and enter your Apple ID when prompted. Finally you will see the device disconnecting from the cloud; Tap <iCloud <Apple ID

[2] *Id.*at ¶ 14-15.

and scroll to the bottom of the screen and tap Sign Out; Press the home button and Select Settings then General and tap on Reset; Select "Erase All Content and Settings" and enter your passcode then tap on Erase iPhone Tap Sign Out to remove data from this iPhone; Tap on Erase iPhone again and the iOS device will reboot and wipe all the contents and then you will see the factory welcome screen; Turn your iPhone off and return to your property custodian.'[3]

11. Pursuant to OCIO instructions listed above, ICE mobile devices are reset by the employee to whom the ICE mobile device was assigned. This ensures that all content of the device has been securely erased prior to the device being e-cycled. OCIO provides further detailed instructions in its guidance document entitled: "IOS Device Data Wiping: Quick Reference Guide, Department of Homeland Security, Immigration Customs Enforcement OCIO."[4] This guidance is provided to all ICE personnel with mobile devices and identifies the steps ICE employees need to take to wipe and or erase all data from their mobile device prior to returning the device to an ICE Property Custodian or their supervisor. *See* Exhibit 2.

12. Per the instructions listed in IOS Device Data Wiping Quick Reference Guide, it is the ICE employee's responsibility to take appropriate steps to establish and maintain separate records if the employee had conducted official business on his or her cell phone utilizing applications with a messaging component other than e-mail.

13. Therefore, per DHS policy 143-01 and IOS Device Data Wiping Quick Reference Guides, it was the responsibility of the seven (7) custodians to take appropriate steps to maintain and preserve any data that may have inadvertently been stored or created on their individual assigned mobile devices that would be considered official business records.

---

[3] Steps to Erase All Data from iPhone guide, Quick Reference Guide, Department of Homeland Security, Immigration and Customs Enforcement OCIO. *See* Exhibit 1.

[4] IOS Device Data Wiping: Quick Reference Guide, Department of Homeland Security, Immigration Customs Enforcement OCIO," (November 1, 2017).[4] *See* Exhibit 2.

14. Pursuant to the Court's Order dated June 3, 2022, ICE provides the following with respect to the seven (7) custodians' mobile devices: 1) Thomas Homan's line of service was deactivated on February 26, 2019; 2) Matthew Albence's line of service was deactivated on February 19, 2020; 3)Tracey Short's line of service was deactivated on January 19, 2021; 4) Jon Feere's mobile was returned to the property custodian on January 1, 2021; 5) Ronald Vitiello's line of service was deactivated on December 16, 2020; 6) Thomas Blank's line of service was deactivated on May 21, 2020; and 7) Nathalie Asher's mobile was returned to the property custodian in December 2021.

15. All lines were confirmed deactivated[5] with the exception of Nathalie Asher and Jon Feere's mobile devices. However, regarding Jon Feere's mobile device, it was determined that the cellphone that Mr. Feere used during his employment with ICE, was issued outside of normal procedures i.e. carried over from a previous agency. OCIO became aware of this matter after the Court's June 3, 2022, Order. Since this new development, ICE has not yet been able to unlock this device and respectfully requests the court to allow it 30-days to provide an update. This will provide an ample time for ICE to work extensively on unlocking this device if it is possible.

JURAT CLAUSE

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge and belief. Signed this 18th day of August 2022.

[5] Upon completion of employment at ICE, employees with mobile devices are instructed to deactivate their mobile devices. Deactivation of mobile devices signals that the mobile phone data has been wiped clean according to OCIO instructions outlined in the quick reference guide: IOS Device Data Wiping: Quick Reference Guide, Department of Homeland Security, Immigration Customs Enforcement OCIO," (November 1, 2017).[5]

RICHARD J CLARK

Digitally signed by RICHARD J CLARK
Date: 2022.08.18 16:07:52 -04'00'

Richard J. Clark
Chief Technology Officer
Technology Transformation Office
Office of the Chief Information Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Steps to Erase All Data From iPhone/iPad

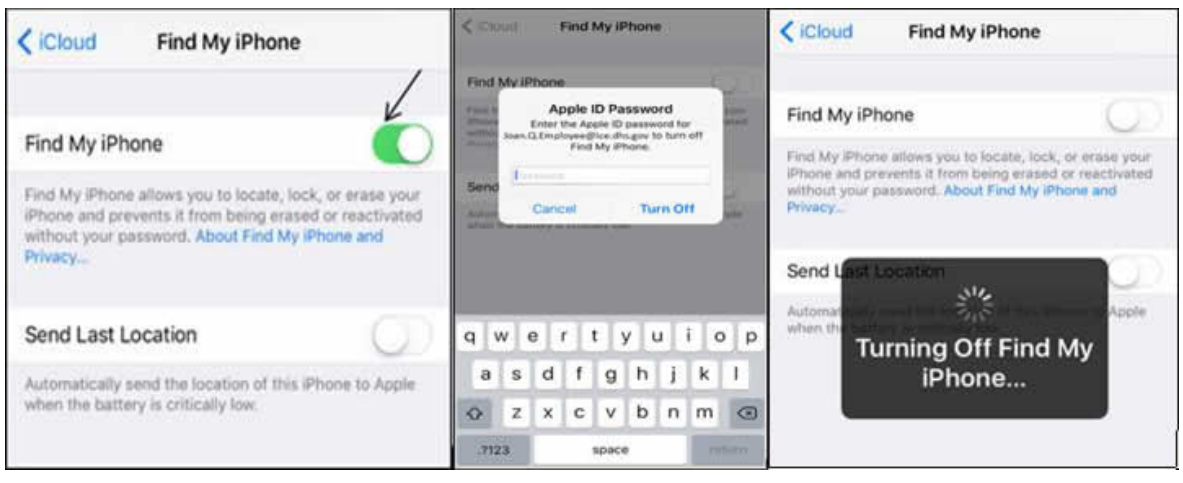
As you upgrade to a new iPhone or iPad it's important that you erase all data on your old device before you turn your device into your program property custodian. The device data erasing steps are simple and are shown below.

Erasing your iOS device (Based on Latest Version of iOS 10.3.2)

1. Log into your iOS device with your user passcode then tap on settings

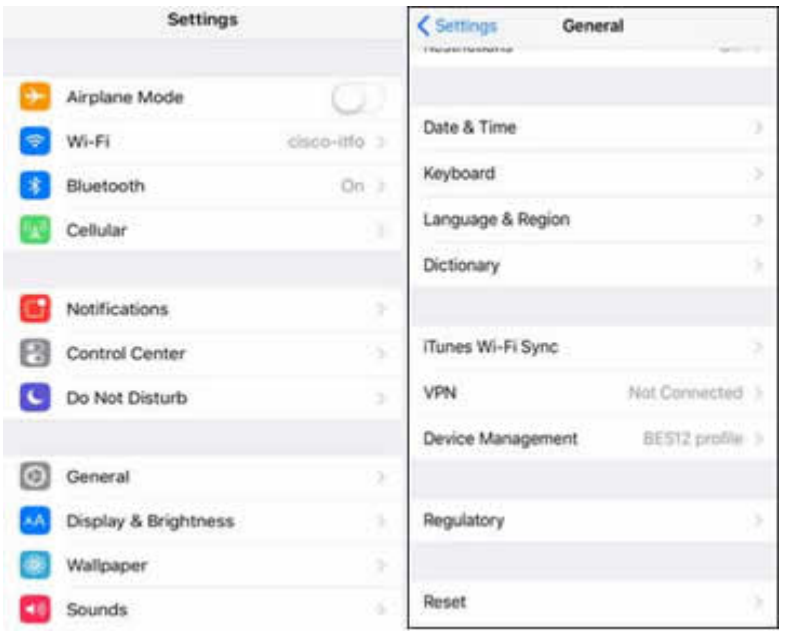
2. Select the ">" to the right of your name and under your Apple ID account information select "ICloud" and turn off any ICloud services, then tap on "Find my iPhone"

3. Slide the "Find my iPhone" button to the off position and enter your Apple ID when prompted. Finally you will see the device disconnecting from the cloud

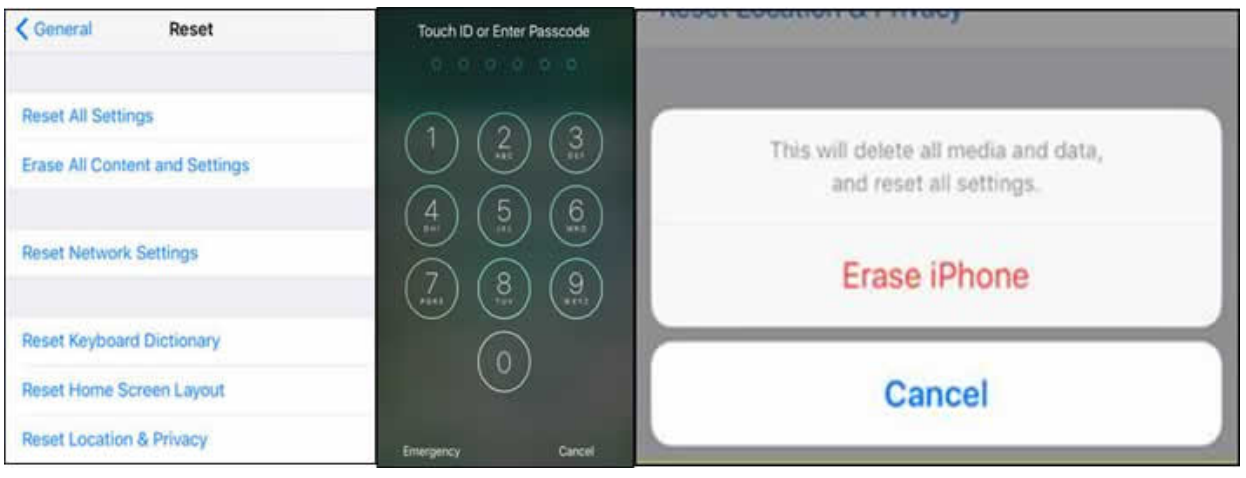


4. Tap <iCloud <Apple ID and scroll to the bottom of the screen and tap Sign Out.

5. Press the home button and Select Settings then General and tap on Reset



6. Select “Erase All Content and Settings” and enter your passcode then tap on Erase iPhone
   - Tap Sign Out to remove data from this iPhone



7. Tap on Erase iPhone again and the iOS device will reboot and wipe all the contents and then you will see the factory welcome screen.

8. Turn your iPhone off and return to your property custodian.

Warning : Sensitive PII NOT authorized on this site!

DHS Connect ICE.gov DHS.gov ICE Apps

U.S. Immigration and Customs Enforcement
Terms of Use | Privacy Statement

Webmaster.ICE@ice.dhs.gov

U.S. Immigration and Customs Enforcement

IOS DEVICE DATA WIPING QUICK REFERENCE GUIDE

Purpose: The purpose of this QREF is to identify the steps ICE users need to take to wipe/erase all data from an IOS device prior to returning the device to an ICE Property Custodian or their supervisor. Additionally, simple wipe verification instructions are included for the property custodian to confirm prior to accepting the iOS device from the user.

Scope: All ICE users are responsible for performing the data wipe steps shown herein prior to returning the device back to an ICE property Custodian or a supervisor. The property custodians or the supervisors are responsible for confirming the IOS device has been wiped by the owner/user of the device per the steps identified herein.

Location of QREF Guide: The QREF Guide can be found on SharePoint HERE. Look in the "Other Documents" section in the link.

NOTE: It is the responsibility of each ICE user of an IOS device to perform the wiping steps defined herein.

List of Steps

A **Steps to wipe your IOS device (ICE User)**

- Log into your iOS device with your user passcode then tap on settings

- Select the ">" to the right of your name and under your Apple ID account information select "iCloud" and turn off any iCloud services, then tap on "Find my iPhone"

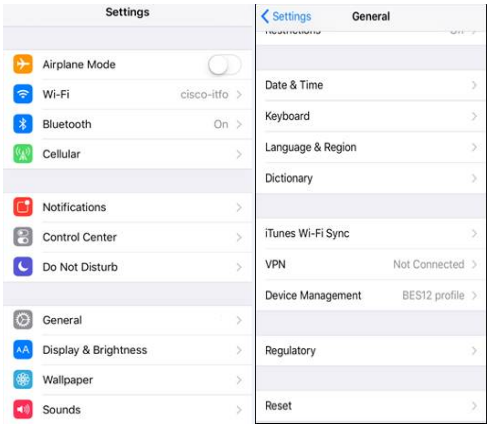
DHS ICE OCIO
Operations Directorate
IT Field Operations Branch
IITFOBRANCHMAILBOX@ice.dhs.gov

- Slide the "Find my iPhone" button to the off position and enter your Apple ID when prompted. Finally you will see the device disconnecting from the cloud

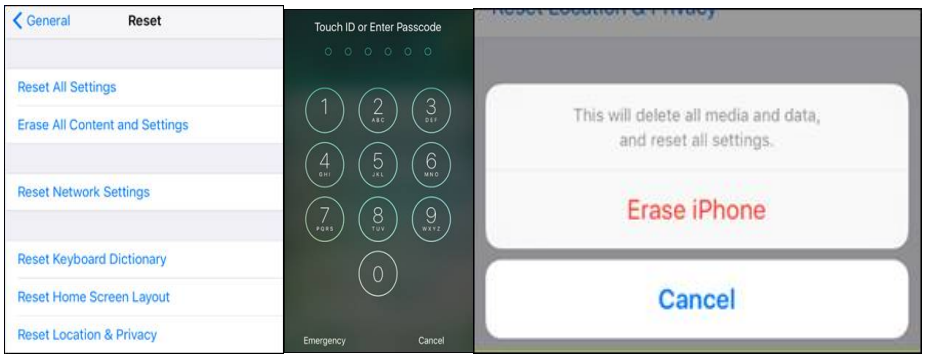
- Tap <iCloud <Apple ID and scroll to the bottom of the screen and tap Sign Out
  a. Tap Sign Out to remove data from this iPhone

DHS ICE OCIO
Operations Directorate
IT Field Operations Branch
IITFOBRANCHMAILBOX@ice.dhs.gov

- Press the home button and Select Settings then General and tap on Reset



- Select "Erase All Content and Settings" and enter your passcode then tap on Erase iPhone



- Tap on Erase iPhone again and the iOS device will reboot and wipe all the contents and then you will see the factory welcome screen.

- Turn your iPhone off and return to your property custodian.

DHS ICE OCIO
Operations Directorate
IT Field Operations Branch
IITFOBRANCHMAILBOX@ice.dhs.gov

B **ICE Property Custodian or Employee Supervisor (Verification of User Wipe/Erase of Data)**

- All iOS devices must be verified that they have been wiped by the ICE user prior to the property custodian or employee supervisor accepting the device
- Property Custodian or Supervisor have the employee turn on the IOS device and verify the welcome screen below comes up. If you see the welcome screen the phone can be accepted. If not return the device to the user to complete the wiping steps referenced herein.
- Once the device is confirmed as wiped complete the Sanitization Form and follow proper Sunflower disposal steps and completion of appropriate paperwork to excess the devices.

C **Addendum (iOS Devices in possession of a property custodian that are locked and cannot be wiped)**

- For locked devices that are not visibly damaged, the property custodian should coordinate with WidePoint and Apple to have the phone unlocked. The unlocked devices should then follow the wiping process. For damaged devices or ones that cannot be unlocked continue below.
- Coordinate with local ITFO to determine if a shredder is on hand. If one is on hand open a ServiceNow ticket for ITFO to destroy the iOS devices. Additionally, complete all necessary paperwork per the PPOH and identify the hardware as scrap in all appropriate paperwork being submitted for approval. Complete a Certificate of Disposal form and include a statement that devices were destroyed on-site and witnessed by 2 ICE personnel. Obtain needed approval for scrap and once approved complete all Sunflower transactions (please note that NUO will not approve any on-site request without assets having already been sanitized or have been disabled.)

DHS ICE OCIO
Operations Directorate
IT Field Operations Branch
IITFOBRANCHMAILBOX@ice.dhs.gov

- If no local shredder is on hand then coordinate a destruction run to a facility that can destroy the iOS devices. Complete all necessary paperwork per the PPOH and identify the hardware as scrap in all appropriate paperwork being submitted for approval. Complete a Certificate of Disposal Form and include a statement that devices will be destroyed off-site with ICE witnesses. Once approval for disposal has been granted the responsible program will arrange needed safeguards, precautions and transport the iPhones to the location where destruction will be witnessed by 2 ICE employees and the Certificate of Disposal will be signed by the ICE witnesses.

Executive Sponsor	
Cesar Cuni ITFO Branch Chief	Signature: Date: Digitally signed by CESAR CUNI DN: c=US, o=U.S. Government, ou=Department of Homeland Security, ou=ICE, ou=People, cn=CESAR CUNI, 0.9.2342.19200300.100.1.1=0567981695.ICE Date: 2017.11.01 09:53:38 -04'00'
Approve: ☒	Disapprove: ☐

DHS ICE OCIO
Operations Directorate
IT Field Operations Branch
IITFOBRANCHMAILBOX@ice.dhs.gov