

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information Act Program
Communications Center
245 Murray Lane, S.W., Building T-5
Mail Stop 8205
Washington, D.C. 20223

Date: March 20, 2023

CREW
1331 F Street, N.W., Suite 900
Washington, DC 20004
Email: foia@citizensforethics.org

File Number: 20220640-L

Dear Requester:

This is the final response to your Freedom of Information Act (FOIA) request, originally received by the United States Secret Service (Secret Service) on August 16, 2022, for information pertaining to:

1. “[A]ll communications and directives from the Secret Service Office of Technical Development and Mission Support (“TEC”) concerning the three-month system migration, which included a reset begun in January 2021 of the Secret Service’s mobile phones, referenced in the July 14, 2022 Statement of Anthony Guglielmi, Chief of Communications for the United States Secret Service on Accusations of Deleted Text Messages From DHS Inspector General (“Guglielmi Statement”). This request includes, but is not limited to, directions on whether and how to preserve text messages and emails.” (Your request was subsequently clarified and all USSS official messages, not just those from TEC, were searched).
2. “[A]ll communications and directives concerning the recordkeeping responsibilities of departing Secret Service employees, including but not limited to whether and how to preserve text messages and emails.”

After a detailed review of all potentially responsive records, 176 page(s) were released, and 0 page(s) were withheld in their entirety. Exemptions under the FOIA Statute, Title 5 U.S.C. § 552 have been applied where deemed appropriate.

Enclosed are the documents responsive to your request, as well as a document that explains the exemptions in more detail. Withheld information is pursuant to the exemptions marked below.

Section 552 (FOIA)

(b) (1) (b) (2) (b) (3) Statute: (b) (4) (b) (5) **(b) (6)** (b) (7) (A)
(b) (7) (B) **(b) (7) (C)** (b) (7) (D) (b) (7) (E) (b) (7) (F) (b) (8)

The following checked item(s) also apply to your request:

As you have already filed suit in the United States District Court for the District of Columbia, 1:22-CV-03248, regarding the above referenced request, there is no further right to administratively appeal this decision outside your pending civil action.

If you need any further assistance or would like to discuss any aspect of your request, please contact Cormac A. Early, Trial Attorney, United States Department of Justice, Civil Division, Federal Programs Branch, 1100 L Street, NW, Washington, DC 20005. Phone: (202) 616-7420, Email: cormac.a.early@usdoj.gov

Sincerely,



Kevin L. Tyrrell
Freedom of Information Act Officer
Office of Intergovernmental and Legislative Affairs

Enclosure:
FOIA and Privacy Act Exemption List

**FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

Provisions of the Freedom of Information Act do not apply to matter that are:

- (b) (1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b) (2) related solely to the internal personnel rules and practices any agency;
- (b) (3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute: (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) is established after the date of enactment of the OPEN FOIA Act of 2009;
- (b) (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b) (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency; provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested;
- (b) (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b) (7) records or information compiled for law enforcement purposes, but only to the extent that the information: (A) could reasonably be expected to interfere with enforcement proceedings; (B) would deprive a person of a right to a fair trial or an impartial adjudication; (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source; (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b) (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for regulation or supervision of financial institutions;
- (b) (9) geological and geophysical information and data, including maps, concerning wells.

**PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a**

The provisions of the Privacy Act do not apply to:

- (d) (5) material compiled in reasonable anticipation of civil action or proceeding;
- (j) (2) material reporting investigative efforts pertaining to enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) material is currently and properly classified pursuant to an Executive Order in the interest of national defense or foreign policy;
- (k) (2) material compiled during investigations for law enforcement purposes;
- (k) (3) material maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;
- (k) (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or for access to classified information, but only to the extent that the disclosure of such material would reveal the identity of the person who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or prior to the September 27, 1975, under an implied promise that the identity of the source would be held in confidence;
- (k) (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;

REMOVAL OF PAPERS AND OTHER DOCUMENTARY MATERIALS

Background

44 U.S.C. 3105 requires that heads of Federal agencies establish safeguards against the removal or loss of records. These safeguards include notifying agency officials and employees that criminal penalties are provided for the unlawful removal or destruction of Federal records (18 U.S.C. 2071) and for the unlawful disclosure of certain information pertaining to national security (18 U.S.C. 793, 794, and 798).

Definitions

- a. Records. These include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved, or appropriate for preservation by that agency or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them (44 U.S.C. 3301).
- b. Documentary Materials. This is a collective term for records and nonrecord materials that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.
- c. Nonrecord Materials. These are Government informational materials that do not meet the statutory definition of records (44 U.S.C. 3301) or that have been excluded from coverage by the definition. Nonrecord materials are unofficial copies of documents kept only for reference, stock of publications and processed documents, and library or museum materials intended solely for reference or exhibit.
- d. Personal Papers. These are documentary materials, or any reasonably segregative portion thereof, of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of the agency business (36 Code of Federal Regulations (CFR) Part 1222).
- e. Documentary Materials Removal/Nonremoval Certification. This Department of Homeland Security form (DHS Form 141-02) formally documents the process of review and concurrence for removal or nonremoval of agency documentary materials. Before completing this form, separating employees must read the National Archives and Records Administration (NARA) publication *Documenting Your Public Service*, available at <http://www.archives.gov/records-mgmt/publications/documenting-your-public-service.html> so that by signing the form, employees also certify that they have read and understand the provisions of the above publication.

Procedures for Removal of Papers and Other Documentary Materials

No documentary material, even though judged to be nonrecord material, shall be withdrawn if this will create such a gap in the files as to impair the completeness of essential documentation. Indexes, or other finding aids, necessary to the use of the official files may not be removed.

Personal diaries, which are really private records of public activities, are private property and may be removed. When the matters dealt with in such work aids as office diaries, logs, memoranda of conferences and telephone calls are covered elsewhere by adequate records, such work aids may be removed.

Extra copies (carbons, photocopies, etc.) of records may be removed under certain circumstances, but only with the permission of the Secret Service.

Prior to removal, the separating employee's supervisor shall consult with the OSP Chief Records Officer and other cognizant Secret Service review officials to decide if a legal or policy reason exists for keeping the information contained therein confidential and that the record copy, and other necessary copies, are available in the Secret Service. If the copy is of a document originating with another agency, the wishes of the originating agency will also be determined and respected.

Material that is marked as national security information and officially limited information may not be removed from the Secret Service under any circumstances. Material so marked may include information pertaining to but not limited to:

- the enforcement of criminal/civil law relating to Secret Service matters;
- all protection related activities;
- Secret Service personnel rules and regulations; and
- sensitive or proprietary information relative to Secret Service policy.

Such information should remain classified, controlled or restricted as long as required for national security and/or Secret Service interest.

Any violation of the statutory and regulatory limitations placed on removal of papers by Secret Service officials who resign or retire will be forwarded to the Office of Professional Responsibility, who shall confer with the Inspector General regarding such violations.

If the private or nonofficial papers of a Secret Service official are kept in the official's office, they shall be filed separately from the official records of the office.

Responsibilities

Reviewing Official

The supervisor of a separating employee will serve as the primary reviewing official (see DHS Form 141-02) for documentary materials being requested for removal by departing employees. (Requests for removal of materials made by Component heads will be coordinated for review as directed by the DHS Chief Records Officer, through the Component Chief Records Officer.)

If documents are being proposed for removal, the reviewing official will:

- a. Obtain a signed Homeland Security Form DHS Form 141-02 from any departing employee desiring to remove documents (paper or electronic media) from the Secret Service.
- b. Review all documents being proposed for removal by an employee to ensure that none of the information being taken contains law enforcement data, trade secrets, national security or privacy material, or other interests protected by law. To do this, the reviewing official may require the requesting employee to provide documentation of concurrence (or seek it directly) in writing, from:
 - the Security Management Division
 - the Office of the Chief Counsel
 - Disclosure officials of the Office of Intergovernmental and Legislative Affairs
 - the Office of Communication and Media Relations
 - Assistant Directors/Executive Chiefs with subject matter responsibility for the content of the material

The Chief Records Officer should also be consulted following the outreach above, as the Chief Records Officer must also sign the DHS Form 141-02 when materials are requested for removal.

- c. Following signature by the Chief Records Officer, forward all signed DHS Form 141-02s to the Office of Human Resources.

Employees

All employees will:

- a. Certify to having read this "Removal of Papers" policy by signing the SSF 3218, "Annual Employee Certification".
- b. Notify the Chief Records Officer, Office of Strategic Planning and Policy, when they are about to remove any documents (paper or electronic media) from the Secret Service.
- c. Sign a DHS Form 141-02, when they resign or retire as part of their Department of Homeland Security - U. S. Secret Service Employee Separation Clearance Procedure.

- d. Be aware of the consequences of violation of the statutory and regulatory limitations on removal of papers.

Office of Human Resources

The Office of Human Resources will:

- a. Obtain a signed DHS Form 141-02, "Documentary Materials Removal/Nonremoval Certification", from all employees when no documents are being removed. This will be accomplished at the time of separation.
- b. Maintain all signed copies of the DHS Form 141-02 for three (3) years after the separation or retirement of an employee from the Secret Service.

United States Secret Service
Directives System

Manual : Human Resources
RO : HUM

Section : HUM-19(04)
Date : 11/02/2022

From: HUM <HUM@OfficialMail.usss.dhs.gov>
To: USA <usa@OfficialMail.usss.dhs.gov>
Cc: HUM <HUM@OfficialMail.usss.dhs.gov>
Subject: DCP#: HUM 2022-47, Separation Procedures for All Employees
Date: Wednesday, November 2, 2022, 10:15 AM

//ROUTINE//

From: Headquarters (Office of Human Resources) DCP# HUM 2022-47
To: All Supervisors and Holders of the Office Human Resources Manual
Subj: Separation Procedures for All Employees

This directive is filed in front of the Human Resources Manual section HUM-19(04), "Separation Procedures for All Employees" and is in effect until superseded.

Reference is made to the Chief Operating Officer Official Message dated November 1, 2022, subject: "Actions to Enhance Retention and Preservation of Electronic Messaging." Reference also is made to the following concurrent directives:

- DCP# CIO 2022 16, CIO 04(06), "Mandatory Preservation of Records on Secret Service Issued Smartphones"
- DCP# RPM 2022-09, RPM-03, "Issuance and Use of eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices"

This directive implements revisions to SSF 3106 (Employee Separation Clearance) and SSF 4467 (Employee Separation Checklist) reflecting required completion of eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices."

Effective November 1, 2022, prior to separating from the agency or erasure/factory reset of their issued mobile device(s) for any reason, each affected employee must access the [USSS eForms Library](#) and complete eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices." By completing this form, employees will document that they have examined their mobile device(s) for federal records and ensured that those records were preserved and retained on the agency's computer network. Supervisors are responsible for ensuring this requirement is fulfilled.

Questions regarding this message may be directed to the Office of Human Resources. Additionally, questions regarding the recordkeeping and preservation requirements in this message may be directed to the Office of Strategic Planning and Policy, Enterprise Records Management Division via e mail to Records@usss.dhs.gov.

Headquarters (Chief - Office of Human Resources) Magnuson/Hall

United States Secret Service
Directives System

Manual : Human Resources Manual
RO : HBS

Section : HUM-07(02), HUM-19(04)
Date : 01/27/2022

From: HUM
To: USA
Cc: HUM
Subject: DCP#: HUM 2022-02 USSS Employee Separation Survey
Date: Thursday, January 27, 2022 5:42:28 PM

//Routine//

FROM: Headquarters (Chief – Office of Human Resources) DCP#: HUM 2022 02

TO: All Supervisors and Holders of the Human Resources Manual

SUBJECT: USSS Employee Separation Survey

This directive should be filed in front of the Human Resources Manual Section HUM-19(04), Separation Procedures for All Employees, and HUM 07(02), Employee Performance Files.

This directive is in effect until superseded.

This directive updates Human Resources Manual section HUM-19(04), Separation Procedures for All Employees to state the employee separation survey ([USSS Separation Survey](#)) has been removed from the Workforce Planning Division (WP.) Intranet page and added to the Human Resources Business Solutions Division (HBS) intranet page. The link may be found on the HBS Homepage under HUM Surveys - Current Survey (titled USSS Separation Survey). Supervisors/managers should continue to ensure separating employees complete this electronic survey before departing the Secret Service. This survey is available for immediate use.

Please click on link below to view the survey:

[USSS Separation Survey](#)

Please contact the Human Resources Business Solutions Division (HBS) at HUMSurveys@ussc.dhs.gov if you have any questions.

Headquarters (Chief – Office of Human Resources)

Ashley/Yarwood

SEPARATION PROCEDURES FOR ALL EMPLOYEES

Issuance and Completion of Required Documents

As soon as the effective date of an employee's separation is known, supervisors or their authorized designees are responsible for forwarding an electronic SF 52, Request for Personnel Action, via HR Connect, to the Office of Human Resources, Benefits and Payroll Division (BPR) as soon as the effective date of an employee's separation is known. Supervisors must clearly enter the appropriate separation action (distinguishing between resignation or transfer to another federal agency) when entering in HR Connect. The BPR, Employee Benefits Branch (EBB) processes all types of retirement and separations. The BPR, Payroll Operations Branch (POB) processes all transfers. It is important to distinguish between resignations and transfers as benefits elections and annual lump sum payments will be affected. Offices must act promptly to ensure that each separating employee receives their final pay in a timely manner and no unearned salary is paid because of a delay in processing the separation.

Prior to the last day of employment, supervisors should ensure separating employees complete an electronic Employee Separation Survey. The Employee Separation Survey can be accessed by going to the Office of Human Resources, Workforce Planning Division's Intranet page. The Employee Separation Survey is located under the section entitled, "Quick Links."

Survey responses are confidential. The survey information will be used to provide the Secret Service management with summary reports regarding separations. Survey responses are confidential. When the survey is completed, the employee will receive an e-mail receipt which may be submitted to the supervisor and verified on Secret Service Form (SSF) 3106, Employee Separation Clearance.

The employee's supervisor is responsible for the initiation of the process detailed on the SSF 3106, Employee Separation Clearance. The separating employee is responsible for obtaining signatures for all record of clearances indicated on the SSF 3106; section II – Record of Clearances. The separating employee should return the SSF 3106 to their supervisor, who will ensure all appropriate sections have been completed. The supervisor will then forward the SSF 3106 to the Security Management Division (SMD) for final retention.

Supervisors must ensure employees complete Department of Homeland Security (DHS) Form 141-02, Documentary Materials Removal/Nonremoval Certification. Guidance for completing this form may be found in MNO-06(08), Removal of Papers in the Secret Service Record Programs Management Manual. Final retention of the DHS Form 141-02 is maintained by the Performance Management and Employee Relations Division (PRF).

Supervisors of separating employees are required to complete the SSF 3229, Re-Employment Recommendation and submit it to the Office of Investigations, Investigative Support Division, no later than two weeks following an employee's separation from the Secret Service.

Supervisors of separating employees are required to provide the employee's personal e-mail address and mailing address when entering a separation action in HR Connect. In an effort to streamline and expedite the notification process, a separation packet will be sent electronically to the separating employee's personal email address. In the event the employee does not have a personal email address, the separation packet will be mailed to the home address on record.

Procedures and Responsibilities

Employee Responsibilities

The employee is responsible for notifying their supervisor of the date and nature of separation from the Secret Service. If an employee is transferring to another agency, the employee should provide their supervisor with the name of the new agency and a Human Resources point of contact and phone number. The separating employee must contact the EBB at 202-406-5670 to discuss benefits matters.

If the separation action is a resignation the employee must complete a resignation action, SF 52, in HR Connect through the employee self-service menu and route it through the appropriate Assistant Director's or Executive Chief's Office for forwarding to BPR. The SF 52 should be submitted to BPR, at least one pay period before the separation date. The employee is also responsible for notifying the supervisor if their records are subject to a litigation hold.

Public Financial Disclosure Report

Employees who are required to file a Public Financial Disclosure Report (OGE Form 278) are required to file a termination 278 report within 30 days of separating from the U.S. Government. Employees with questions regarding this requirement should contact the Office of Chief Counsel.

Manager Responsibilities

If the separation action is a transfer the manager must complete a transfer action, SF 52, in HR Connect through the manager self-service menu and route it through the appropriate Assistant Director or Executive Chief's Office for forwarding to BPR. The SF 52 should be submitted to BPR at least one pay period before the separation date.

Accountable Property

Prior to the last day of employment, an employee must turn in their commission book, identification cards and other credentials, firearms, Secret Service badges, and all other Secret Service property for which the employee is accountable. The separating employee will return all accountable property to the property representative of their office. The employee's name should be removed from the Custodian field in Sunflower (a property tracking component of TOPS) except for lost, stolen, or damaged property. The employee's Personal Identity Verification (PIV) card should be returned to SMD for disposal. The appropriate division to which all property must be returned can be found in the Chief Financial Officer Manual, section AOD-02(01), Control of Individually Issued Property. Lost, stolen, or damaged property must be accounted for in accordance with Chief Financial Officer Manual, section AOD-06(05), Reporting Incidents of Loss of, Theft of, or Damage to Property.

Timekeeper Responsibilities

The separation date on the timecard must be the same as the date reflected on the SF 52 in order for the National Finance Center payroll/personnel system will not process the separation. It is the timekeeper's responsibility to note in the remarks section of the employee's final timecard the nature and effective date of the employee's separation.

The timekeeper is required to notify POB of the effective date of the employee's separation via webTA to ensure the required payroll system entry is made for the employee's separation to be processed automatically. Manual processing will delay the employee's transfer of leave or payment of lump sum and issuance of final paycheck.

Supervisor Responsibilities

The employee's supervisor is responsible for initiating the process detailed on the SSF 3106, Employee Separation Clearance, during last pay period of employment and ensuring that the completed form is sent to SMD for final retention. The supervisor must complete the electronic SF 52 at least one pay period prior to the effective date of the separation. EBB will complete the SF 52 for retiring employees.

Supervisors are required to ensure separating employees have completed the required service agreements related to Government-funded training and other recruitment and retention initiatives. For additional information regarding Employee's Agreement to Continue in Service, please refer to the following directives: Training Manual, section RTC-02(02), Training Requests, Human Resources Manual section HUM-10(08), Student Loan Repayment Program and DCP#: HUM 2016-09 (dated 04/12/2016) – "Tuition Assistance (Educational Reimbursement)" filed in from of section HUM-10(09).

In addition, supervisors are required to send an official message notifying all appropriate parties of the employee's intent to separate. (See sub-section, *Review of Financial Obligations*). The supervisor will forward the Employee Performance File to POB. The employee's time and attendance records should be retained in the employee's departing office for six full years. If there is no active or pending litigation involving the records, then the files can be destroyed in accordance with the records retention schedule.

If the employee notifies the supervisor that their records are subject to a litigation hold, the supervisor is responsible for collecting the records subject to the litigation hold, ensuring that the records are maintained in a secure location, and notifying the Office of Chief Counsel that the supervisor has collected the records.

Review of Financial Obligations

Notification of an employee's intent to separate will result in the determination and liquidation of any outstanding indebtedness prior to the termination of employment.

Upon notification of an employee's **intent to separate for any reason**, supervisors must notify the following: BPR, (both POB and EBB), PRF, Financial Management Division (FMD), Administrative Operations Division (AOD)/Property Management Branch, Office of the Chief Information Officer, Office of Integrity, Inspection Division, SMD, and other pertinent offices via official message and provide the following information:

1. Name of employee;
2. Office Name;
3. Social Security Number (truncate to last four digits);
4. Date of separation or beginning and ending date of nonpay status;
5. Reason for separation or entry into nonpay status (in as much detail as possible); and,
6. Date of assignment to the office (if it has occurred within the last twelve months).

Upon receipt of this information, FMD initiates a review of the employee's records for outstanding claims and AOD will review for any lost, stolen, damaged property pending financial liability. FMD formally notifies the requesting office/division of any outstanding amounts due from the separating employee. If there are no outstanding claims, a negative response is forwarded to the employee's office/division. POB should confirm with PRF whether the employee has satisfied the Service Agreement commitment for the Student Loans Repayment Program and/or Tuition Assistance if applicable.

Issuance of Final Paycheck

The POB will verify that the separating employee does not have an outstanding debt to the Secret Service. Every pay period the POB will provide a list of departing employees to FMD for authorization to release final paychecks and lump sum payments. Upon BPR's receipt of FMD authorization to release funds, the final paycheck for each employee will be routed through POB. If the employee has a debt, the salary check will be held until the debt is cleared, or the salary check will be offset to clear the debt. Once the debt is satisfied, the final salary is released and deposited electronically in the employee's account of record.

Notice Regarding Unemployment Insurance

Each office is responsible for ensuring the SF 8; Notice to Federal Employee about Unemployment Insurance is issued to each separating employee on or before their last day of work. This form must be issued to each employee who is separating, or placed in a nonpay status for seven days or more.

The SF 8 must contain the following address:

TALX
P.O. Box 66945
St. Louis, MO 63166

All Unemployment Compensation for Federal Employees Requests for Wage and Separation Information, Form ES 931, received from State employment security agencies should be transmitted immediately by express mail to the TALX at the following address:

TALX
1845 Borman Court
St. Louis, MO 63146

Failure to forward these forms immediately may result in the Secret Service being billed for unwarranted unemployment compensation payments.

Nondisclosure Notification and Agreement for Separating Employees

Separating employees must acknowledge and sign their consent to be legally bound to the terms contained in the SSF 4322A, Nondisclosure Notification and Agreement for Separating Employees. This agreement reaffirms the consent each employee previously signed as a Secret Service employee via SSF 4322, Employee Nondisclosure Notification and Agreement, consistent with Secret Service nondisclosure policy.

The separating employee's supervisor will forward the completed SSF 4322A to the SMD for inclusion in the employee's Personnel Security File.

Debriefings

All employees granted Top Secret security clearances and/or Sensitive Compartmented Information (SCI) access and who terminate employment with the Secret Service will be debriefed and the Top Secret and/or SCI access will be withdrawn. In short, the individual does not hold or have a security clearance if no longer employed by the Agency.

Employees assigned to Headquarters will be debriefed by SMD. For employees outside of Headquarters, the debriefing will be conducted by the employee's supervisor using the SSF 1776, "Certification Security Debriefing," and the SF 312, "Classified Information Nondisclosure Agreement." For those employees who have been read into SCI, the completion of Form 4414, "SCI Nondisclosure Agreement", is also required. In cases where the supervisor is unavailable to perform this function, SMD will administratively debrief the employee.

After the debriefing has been completed and all forms filled out and signed, the employee's clearance is withdrawn and will no longer be active. The separating employee will relinquish their DHS PIV card at this time. The separating employee's DHS PIV card and the completed SSF 1776, SF 312, and Form 4414 should be submitted to SMD for destruction or final retention.

If a former employee decides to transfer to another agency that requires a security clearance, the former employee can inform the hiring agency of their previous background investigation, and the clearance and/or access level granted. The hiring agency will be responsible for verifying the background information provided by the former employee, as well as any reciprocal recognition of the investigation or re-issuance/re-instatement of the Top Secret Security Clearance.

For additional information, refer to the Human Resources manual, section SCD-02(01), Special Security Clearances Requirements and Reporting.

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service
EMPLOYEE SEPARATION CLEARANCE
(see instructions on page 3)

SECTION I - EMPLOYEE DATA

1. NAME (First, Last, MI):		2. SOCIAL SECURITY NUMBER:	3. DEPARTURE DATE:
4. ORGANIZATIONAL UNIT AND POD:	5. TITLE AND GRADE OF PRESENT POSITION:	6. TELEPHONE NUMBER (include a/c): Office (needed): Home:	
7. ADDRESS (including ZIP code):			
8. E-MAIL ADDRESS (personal):			

SECTION II - RECORD OF CLEARANCES (To be completed by officials indicated).

PART ONE. ADMINISTRATIVE OPERATIONS DIVISION, PROPERTY MANAGEMENT BRANCH

No unresolved reports of damaged, lost and/or stolen property. Reports of damaged, lost and/or stolen property pending; pertinent information is attached.

Did the employee participate in the Public Transportation Incentive Program (PTIP)? Yes No If yes, have benefits been canceled? Yes No

Did the employee participate in the Executive Parking Program? Yes No If yes, has the employee returned his/her parking pass? Yes No

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - PROPERTY MANAGEMENT BRANCH:	

PART TWO. LIAISON DIVISION, PASSPORT AND VISA OFFICE - The above named employee's diplomatic/official passport status has been reviewed and:

All diplomatic/official passports must be returned to the Passport and Visa Office without exception

If employee is retiring, request the diplomatic/official passport as a souvenir.

If employee is transferring to the private sector, the passport(s) will be returned to Department of State for destruction.

If employee anticipates being hired as a rehired annuitant, Liaison Division will retain the passport(s).

If employee is transferring to another agency, passport(s) will be returned to Department of State with a request to transfer to the gaining agency.

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - LIAISON DIVISION, PASSPORT AND VISA OFFICE:	

PART THREE. FINANCIAL MANAGEMENT DIVISION - The above named employee's fiscal records have been reviewed and the employee is:

Not in debt to the Secret Service and is cleared for release. In debt to the Secret Service, pertinent information attached. Other

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - FINANCE AND ACCOUNTING BRANCH:	

PART FOUR. BENEFITS AND PAYROLL DIVISION (Payroll Operations Branch) - The above named employee's Continued Service Agreement record(s) has been reviewed and the employee is:

Not in debt to the Secret Service and is cleared for release. In debt to the Secret Service, pertinent information attached. Other

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - BENEFITS AND PAYROLL DIVISION:	

PART FIVE. Supervisor or Delegate will verify the following:

- A. All separation actions must be entered on or before the effective date or the separation to avoid delay in processing the annual lump sum payment (see HUM-19(04)). Please be sure to enter the separation action accordingly (Resignation from the federal government vs. Transfer to another federal agency) as benefits could be impacted. Please check appropriate line:
- SF 52, Request for Personnel Action, has been forwarded to the Benefits and Payroll Division upon notification of the separation date. (See Human Resources Manual section HUM-19(04).)
 - Employee is separating without giving a two-week notice, therefore, the Benefits and Payroll Division was notified by sending a fax copy of the SF 52. The SF 52 will be forwarded to the Benefits and Payroll Division as soon as possible thereafter. (See Human Resources Manual section HUM-19(04).)
- B. Procedures outlined in Human Resources Manual section HUM-19(04) have been complied with as regards notifying the Financial Management Division of the intended separation.
- NOTE:** Field Offices are to use an Official Message to accomplish this requirement if there are time constraints.

PART FIVE (CONTINUED). Supervisor or Delegate will verify the following:

- C. Accountable items and property issued to the above employee have been collected and will be disposed of according to the procedures of Office of the Director Manual, section AOD-02(05).
Please check appropriate line:
 All issued accountable items and property were returned in good condition.
 Circumstances concerning unreturned or damaged accountable items and property have been reported in accordance with Office of the Director Manual, section AOD-06(05).
- D. SF 8, "Notice to Federal Employee About Unemployment Insurance," has been issued per Human Resources Manual, section HUM-19(04).
- E. Employee has contacted the Office of Human Resources, Benefits and Payroll Division, Employee Benefits Branch at BPR-Benefits@uss.s.dhs.gov, concerning health, life, and retirement benefits. Name of Employee Benefits Branch employee that separating employee contacted: _____ Date contacted: _____
- F. SSF 3229, "Re-Employment Recommendation," has been completed and forwarded to the Office of Investigations, Investigative Support Division.
- G. SSF 4322A, "Nondisclosure Notification and Agreement for Separating Employees," has been completed and forwarded to the Security Management Division for inclusion in the Employee's Personnel Security File.
- H. Employee Separation Survey has been completed via Secret Service MSForms (this survey is anonymous).
- I. Employee has read the National Archives and Records Administration (NARA) publication Documenting Your Public Service; and DHS Form 141-02, "Documentary Materials Removal/ Nonremoval Certification," has been provided, signed as appropriate, and forwarded to the Performance Management and Employee Relations Division (PRF).
- J. Employee has completed the period of service agreed upon for Government-funded training per Training Manual section RTC-02(02).
(Law Enforcement Employees Only) Supervisor has initiated SSF 4073C, "Documentation of "Good Standing" (LEOSA)," and provided to Office of Integrity.
- K. Employee is aware of process for requesting a LEOSA card and has access to the SSF 4073, Retired/Former Employee (Firearm) Identification Card Request and Waiver Form and associated forms in the SSF 4073 series. (See ITG-02)
- L. Employee has properly closed out of any non-USSS accounts or systems (e.g., Cornerstone Services on Demand (CSOD), etc.)
- M. Employee has contacted the Office of the Chief Counsel/Ethics Staff to obtain post-government employee guidance.
- N. (OGE Form 278 Public Financial Disclosure Report Filers Only) Employee has contacted the Office of the Chief Counsel, Secret Service Ethics Program at ethics@uss.s.dhs.gov.

PART SIX. DEBRIEFING CERTIFICATION - See Human Resources Manual section SCD-02(01), for authorized debriefing officials. The above named individual has been properly debriefed and: _____ has executed SSF 1776 _____ has executed other appropriate debriefing forms
 (Top Secret Clearance)

SIGNATURE OF DEBRIEFING OFFICIAL:	DATE:
SIGNATURE OF SUPERVISOR OR DELEGATE:	DATE:

SECTION III - EMPLOYEE CERTIFICATION

I, the undersigned, make the following statement in connection with my separation from U.S. Secret Service subject to exceptions, if any, which I have fully explained below.

- a. I have returned to the responsible official all Government property and identification for which I was accountable or which I had in my possession.
- b. I have no indebtedness to the U.S. Secret Service for travel advances, imprest fund allowances, advanced leave, overpayment of salary, or other.
- c. I have no unsatisfied period of obligated service for travel or transportation to my first post of duty, to a new post of duty, or for training.

- d. I have returned to responsible officials all data in any form such as internal management documents, written information of a confidential nature, reference materials, or other documents containing data of an official nature; furthermore, I have not copied nor retained any such data in my possession.
- e. I agree not to reveal to any person any classified information, information of a confidential nature, information for limited official use, sensitive information, or any other information that is for official use only, of which I have knowledge, unless officially authorized to do so by appropriate officials of the U.S. Secret Service.

EMPLOYEE'S STATEMENT OF EXCEPTIONS:

SIGNATURE OF EMPLOYEE:	DATE:
------------------------	-------

SECTION IV - SUPERVISOR'S STATEMENT OF EXCEPTIONS

SIGNATURE OF SUPERVISOR OR DELEGATE:	DATE:
--------------------------------------	-------

INSTRUCTIONS

This form is to be initiated by the separating employee's supervisor on the last pay period of employment. Separating employees are those who are either resigning, retiring, transferring to another Government agency or otherwise leaving the employ of the Service.

A. Procedures for Separating Field Employees

Field SAICs will:

1. Complete Section I; Section II, Part Five;
2. Explain Employee Certification and have employee sign in Section III;
3. Complete Section IV, if applicable; and
4. Sign form in Section IV where indicated and forward original copy to Administrative Operations Division, Property Management Branch.

B. Procedures for Separating Headquarters Employees

Appropriate Headquarters supervisors will:

1. Complete Section I; Section II, Part Five;
2. Explain Employee Certification and have employee sign in Section III;
3. Complete Section IV, if applicable;
4. Sign form in Section IV where indicated; and
5. Instruct employee to hand carry original copy to the Administrative Operations Division (Property Management Branch), the Liaison Division (Passport and Visa Office) if applicable, the Financial Management Division, and the Benefits and Payroll Division for signature in Section II; and ultimately hand carry original copy to the official responsible for his/her debriefing (Security Management Division).

Headquarters employees who are separating will:

1. Hand carry the completed original form to the Administrative Operations Division, Property Management Branch, for signature;
2. Hand carry the completed original form to the Liaison Division, Passport and Visa Office, if applicable, for passport status review;
3. Hand carry the completed original form to the Financial Management Division, Accounting Branch, for determination of employee indebtedness;
4. Hand carry the completed original form to the Benefits and Payroll Division for signature; and
5. Hand carry the completed original form to the Security Management Division for signature. The Security Management Division will retain the form for inclusion in employee's Personnel Security File.

PRIVACY ACT STATEMENT: Executive Order 9397 authorizes use of the Social Security number to identify and distinguish between individuals with similar or identical names or initials. Furnishing your Social Security number, as well as other personal data, is voluntary. Failure to provide this information may result in delays in issuance of final pay checks and other benefits.

EMPLOYEE PLEASE NOTE

Clearances must be verified by Financial Management Division before release of FINAL SALARY and LUMP SUM LEAVE (if appropriate) checks.

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service
EMPLOYEE SEPARATION CHECKLIST

Name	Last Four of SSN
Personal Phone	Personal Email
Separation Date	Home Address
USSS EOD Date	Supervisor's Name
Type of Separation <input type="checkbox"/> Retirement <input type="checkbox"/> Resignation <input type="checkbox"/> Termination <input type="checkbox"/> Transfer to Another Agency	Agency Transferring To

FORM NO.		DESCRIPTION	DISPOSITION	ATTN.
N/A	<input type="checkbox"/>	Initiate Debriefing – AO Briefing Dashboard	SMD	AO Debriefing Dashboard
N/A	<input type="checkbox"/>	HR Connect personnel action for resignations/transfer to another agency only; transfer to another gov't agency is a "termination" action; EBB will complete for retiring employees	Employee's Office	Ensure you list the employee's personal email and current mailing address withing HR Connect for official purposes
N/A	<input type="checkbox"/>	Separation Official Message	Supervisors must send an OM notifying all parties of the employee's intent to separate (See ATTN.)	BPR (POB, EBB), PRF, FMD, AOD Property Mgmt. Division, CIO, ITG, ISP, SMD
N/A	<input type="checkbox"/>	Check for outstanding Continuing Service Agreement(s)	BPR/POB	
DHS 141-02	<input type="checkbox"/>	Documentary Material Removal Nonremoval Certification	PRF	HUM-19(04); email to (b)(6); (b)(7)(C)
SSF 4322A	<input type="checkbox"/>	Nondisclosure Notification and Agreement for Separating Employees	SMD	AO Debriefing Dashboard
SSF 1776	<input type="checkbox"/>	Certification of Security Debriefing	SMD	AO Briefing Dashboard
SSF 3229	<input type="checkbox"/>	Re-Employment Recommendation	PARIS	
SF 312	<input type="checkbox"/>	Classified Information Nondisclosure Agreement	SMD	AO Debriefing Dashboard
SSF 3106	<input type="checkbox"/>	Employee Separation Clearance	SMD	Email to (b)(6); (b)(7)(C)
SSF 4414	<input type="checkbox"/>	Sensitive Compartmentalized Information Nondisclosure Agreement (found under the Non-Secret Service Form Tab in Forms Library)	SMD	AO Debriefing Dashboard
SSF 1638	<input type="checkbox"/>	Official Property Receipt (signed when returning property)	AOD	AOD-02(02)
SF 8	<input type="checkbox"/>	Unemployment Notice	Employee	
OGE 278	<input type="checkbox"/>	Financial Disclosure Report	LEG	If applicable, email to (b)(6); (b)(7)(C)
SSF 1780	<input type="checkbox"/>	Weapons Receipt	RTC	Baton: forward copy to AOD with the Baton Pistol: send copy with weapon to RTC via registered mail Retain a copy in Admin File 501.022; transfer assets in Sunflower
SSF 4073	<input type="checkbox"/>	Retired (Firearm) Identification Card Request and Waiver Form	FSD	Mail hardcopy to Brendan Westphal (FSD); attach photo/NCIC checks
SSF 4073C	<input type="checkbox"/>	Documentation of "Good Standing" (LEOSA)	FSD	ITG-07(01); mail hardcopy to Brendan Westphal (FSD)

N/A	<input type="checkbox"/>	Have employee complete the USSS Separation Survey		HUM quick links or HBS "current surveys"
N/A	<input type="checkbox"/>	Run Sunflower individual property report		
N/A	<input type="checkbox"/>	Send Official Message to Deactivate PIV after employee departure	SMD	
N/A	<input type="checkbox"/>	Get approval from AOD in Sunflower for PIV disposal; destroy PIV card locally		
N/A	<input type="checkbox"/>	Active Directory Account Disabled		Email request to (b)(6); (b)(7)(C) with effective date
N/A	<input type="checkbox"/>	OSR (Office Security Rep) submits a ticket via the IT Portal requesting the account be disabled. Ticket should be assigned to Cyber Security		IT Portal/Cyber Security
N/A	<input type="checkbox"/>	Turn in Accountable Property		See accountable property checklist below
N/A	<input type="checkbox"/>	Timecard (WebTA) – timekeeper make the appropriate "status change" entry	Employee's timekeeper	TAM-03
SSF 3115VIB	<input type="checkbox"/>	Farewell Logo Mat (employee's preference – yes or no)	FSD/GDB	Email request to (b)(6); (b)(7)(C)
N/A	<input type="checkbox"/>	Retirement Wall (retired employee only)	BPR	BPR/Benefits (Retirement Wall) Dashboard
N/A	<input type="checkbox"/>	Close USA Performance Profile		USA Performance

PROPERTY CHECKLIST

ITEM	SEND TO	DESTROY LOCALLY	MEMO/EMAIL
<input type="checkbox"/> Badges (LG/SM)	AOD - transfer asset in Sunflower; retiring agents – can be encased in Lucite (obtain order form from BPR/EBB prior to official retirement date)		Memo and email to AOD Liaison
<input type="checkbox"/> Ballistic Vest	AOD – mail vest to AOD warehouse; transfer asset in Sunflower; attach date and tracking info; RTC-05(02)		Memo and email to AOD Liaison
<input type="checkbox"/> Baton	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Handcuffs	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Lapel Pins	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Radio – Handheld	Return radio and accessories to CIO Radio, transfer radio in Sunflower; attach date and tracking to: (b)(6); (b)(7)(C) for more info; Portables Systems Group (b)(6)		
<input type="checkbox"/> Gas Card	Request permission for destruction; AOD-12(04)	X	Memo and email to (b)(6)
<input type="checkbox"/> Commission Book	Transfer to SMD in Sunflower (Resignation/Transfer to Other Agency) or BPR-EBB (Retirement); convert to award in Sunflower if employee wants it stamped "retired" (BPR- (b)(6); (b)(7)(C))		Memo and email
<input type="checkbox"/> DHS Card/Employee ID Card	Transfer to SMD in Sunflower (Resignation/Transfer to Other Agency) or BPR-EBB (Retirement – APT Only)		Memo and email
<input type="checkbox"/> Laptop	CIO or Regional CIO Rep; Reassign in Sunflower		
<input type="checkbox"/> PIV Card	After OM is sent, put up for disposal in Sunflower; then Final Event and destroy locally	X	SMD Deactivation Official Email
<input type="checkbox"/> GETS Calling Card	Email for deactivation; Final Event in Sunflower once deactivated	X	
<input type="checkbox"/> Thumb Drive	Put up for disposal in Sunflower; then Final Event and destroy locally	X	
<input type="checkbox"/> Gun	Send to RTC; attach date and tracking info		
<input type="checkbox"/> Radio	Send to CIO-16/RCB (b)(6); drop code before shipping)		Memo
<input type="checkbox"/> Cell Phone	Wipe and keep as space; CIO-04(06); Wireless Communication Section (b)(6); (b)(6)		Disposal Procedures

<input type="checkbox"/>	Purchase Card	Approving official send email for cancellation after all outstanding transactions are verified in TOPS; FMD-18(02)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	Fleet Card and/or WEX Card	Send email for cancellation after all outstanding transactions are verified; AOD-12(04)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	CBA Travel Card	Send email for cancellation after all outstanding transactions are verified; FMD-14(02)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	IBA Travel Card	Send email for cancellation after all outstanding transactions are verified; AOD-12(04)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	Official Passport	All diplomatic/official passports must be returned to Liaison Division, Passport and Visa Office (LIA/PPT); LIA-04		Coordinate with LIA/PPS at (b)(6); (b)(7)(C)
<input type="checkbox"/>	Gas mask	ATTN: TSD-CBSM (Equipment Return), 843 Brightseat Road (Rear Entrance), Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6); (b)(7)(C)		Memo
<input type="checkbox"/>	Gas Mask Carrier	ATTN: TSD-CBSM (Equipment Return), 843 Brightseat Road (Rear Entrance), Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6); (b)(7)(C)		Memo
<input type="checkbox"/>	Chemical Biological Protective Ensemble (CBPE Kit)	ATTN: TSD-CBSM (Equipment Return), 843 Brightseat Road (Rear Entrance), Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6); (b)(7)(C)		Memo
<input type="checkbox"/>	Issued TSD-CBPE Carrying Bag	ATTN: TSD-CBSM (Equipment Return), 843 Brightseat Road (Rear Entrance), Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6); (b)(7)(C)		Memo
<input type="checkbox"/>	Raid Jacket	Keep in office		
<input type="checkbox"/>	Office Keys	Keep in office		
<input type="checkbox"/>	Garage Pass	Keep in office if GOV; return to AOD if POV – AOD-10(02)		
<input type="checkbox"/>	Government Vehicle	Keep in office (car key, placard, gas card)		
<input type="checkbox"/>	Classified Courier Card	Send to SMD; attach date and tracking information		
<input type="checkbox"/>	Shout Nanos	Return to IPD		
<input type="checkbox"/>	Hotspot	Return to IPD or CIO, which it was assigned from		
<input type="checkbox"/>	Local Airport Access Pass	Keep in office		

[Find your AOD property representative here](#)

[Find your BPR liaison here](#)

Form Processed by (Name/Date):

Supervisor:

Supervisor Signature:

Note: For updates to this form, contact the Benefits and Payroll Division (BPR) at

(b)(6); (b)(7)(C)

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service

DOCUMENTATION OF RECORDS RETENTION ACTIVITIES FOR MOBILE DEVICES

As required by the DHS Secretary's Decision Memorandum signed September 14, 2022, and effective November 1, 2022:

Prior to offboarding or erasure of their mobile device(s) for any reason, each employee must document that they have examined their mobile device(s) for any records sent or received that were created through electronic messaging.

Please review the instructions in the following, step-by-step guides:

[DHS Records Management 101 Job Aid](#)

[USSS Preserve Content Guide for iPhone and iPad](#)

then select the applicable statement below, before submitting this form.

- I HAVE** created or received electronic messages that would be considered a Federal record, and:
- I have retained those records.
 - My retention of these records follows DHS policy and guidance.
 - These records are filed in a standard accessible location (screenshots have been saved to my Pictures folder in my OneDrive account, and e-mailed to my Secret Service e-mail address).
 - I have forwarded any records created on personal devices or accounts due to exigent circumstances while conducting official government business to a government account and have stored them in compliance with DHS policy and guidance.
 - I have complied with any preservation request, including legal holds, and have preserved all records responsive to the preservation request(s) in a manner accessible by Department or Secret Service counsel.
- I HAVE NOT** created or received any electronic messages that would be considered a Federal record, and that would require action on my part in order to be retained.

SUBMIT

DEPARTMENT OF HOMELAND SECURITY
CERTIFICATION OF DEPARTURE DOCUMENTARY MATERIALS REQUEST

4b. SIGNATURE OF EMPLOYEE	4c. DATE
5a. I have reviewed the above request and approved the removal of the documentary material(s).	
5b. NAME OF SUPERVISOR OR REVIEWING OFFICIAL	
5c. SIGNATURE OF SUPERVISOR OR REVIEWING OFFICIAL	5d. DATE
6a. I certify the documentary material(s) are <input style="width: 150px; height: 20px;" type="text"/> for release.	
6b. NAME OF RECORDS OFFICER OR REVIEWING OFFICIAL	
6c. SIGNATURE OF RECORDS OFFICER OR DESIGNATED OFFICIAL	6d. DATE

PRIVACY ACT STATEMENT

AUTHORITY: This information collection is authorized by 18 U.S.C. § 2071; 18 U.S.C. §§ 641, 93, 794, 798, and 952; and 36 CFR 1222.36.

PRINCIPAL PURPOSE(S): This information collected certifies Department of Homeland Security employees departing the agency do so without retaining federal records including any documents relating to any pending or contemplated civil, criminal, or administrative proceeding or other program information that would impair or prejudice the outcome of the proceeding or government policy determinations, decisions, or other actions. The requested documents for removal do not include those prohibited by the Department of Homeland Security or federal statute and regulations from removal.

ROUTINE USE(S): The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in OPM/GOV'T – 001 General Personnel Records (71 FR 35356, June 19, 2006).

DISCLOSURE: The disclosure of this information is voluntary; however, failure to provide the information requested may prevent the Department of Homeland Security from successfully separating you from the agency.

POLICY FOR REMOVAL OF DOCUMENTARY MATERIALS

The following types of documentary materials may NEVER be taken:

- (1) Any Federal record regardless of format, including any copy that is unique (i.e., because it contains the signature or initials of the writer, reviewers, and/or concurring parties, etc.).
 - a. Material labeled "personal," or "private," or similarly designated, and used in the transaction of public business, are Federal records. The use of a label such as "personal" does not affect the status of documentary materials in a Federal agency.

The following types of documentary materials MAY BE taken (see 36 C.F.R. 1222.18 and 1222.20):

- (1) Non-record materials, including extra copies of unclassified or formally declassified agency records kept only for convenience of reference, may be removed by departing employees from Government agency custody ONLY with the approval of a Component Records Officer or Designated Official.
- (2) Copies of records that are publicly available, for example on the public DHS web site and/or available without a FOIA request.
- (3) Personal files, notes, or memos not related to Government agency business or transactions.
- (4) Personal files may contain references to or comments on agency business, but they are considered personal if they are not used to conduct business.
- (5) Documents labeled as "personal" or "private" and separate from the office's official records.
- (6) If information about official matters and agency business appears on the received document, the document is a Federal record. Agencies may make a copy of the document with the personal information deleted or redacted and provide copy for removal.

DEPARTMENT OF HOMELAND SECURITY
CERTIFICATION OF DEPARTURE DOCUMENTARY MATERIALS REQUEST

4b. SIGNATURE OF EMPLOYEE	4c. DATE
5a. I have reviewed the above request and approved the removal of the documentary material(s).	
5b. NAME OF SUPERVISOR OR REVIEWING OFFICIAL	
5c. SIGNATURE OF SUPERVISOR OR REVIEWING OFFICIAL	5d. DATE
6a. I certify the documentary material(s) are <input style="width: 150px; height: 20px;" type="text"/> for release.	
6b. NAME OF RECORDS OFFICER OR REVIEWING OFFICIAL	
6c. SIGNATURE OF RECORDS OFFICER OR DESIGNATED OFFICIAL	6d. DATE

PRIVACY ACT STATEMENT

AUTHORITY: This information collection is authorized by 18 U.S.C. § 2071; 18 U.S.C. §§ 641, 93, 794, 798, and 952; and 36 CFR 1222.36.

PRINCIPAL PURPOSE(S): This information collected certifies Department of Homeland Security employees departing the agency do so without retaining federal records including any documents relating to any pending or contemplated civil, criminal, or administrative proceeding or other program information that would impair or prejudice the outcome of the proceeding or government policy determinations, decisions, or other actions. The requested documents for removal do not include those prohibited by the Department of Homeland Security or federal statute and regulations from removal.

ROUTINE USE(S): The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in OPM/GOV'T – 001 General Personnel Records (71 FR 35356, June 19, 2006).

DISCLOSURE: The disclosure of this information is voluntary; however, failure to provide the information requested may prevent the Department of Homeland Security from successfully separating you from the agency.

POLICY FOR REMOVAL OF DOCUMENTARY MATERIALS

The following types of documentary materials may NEVER be taken:

- (1) Any Federal record regardless of format, including any copy that is unique (i.e., because it contains the signature or initials of the writer, reviewers, and/or concurring parties, etc.).
 - a. Material labeled "personal," or "private," or similarly designated, and used in the transaction of public business, are Federal records. The use of a label such as "personal" does not affect the status of documentary materials in a Federal agency.

The following types of documentary materials MAY BE taken (see 36 C.F.R. 1222.18 and 1222.20):

- (1) Non-record materials, including extra copies of unclassified or formally declassified agency records kept only for convenience of reference, may be removed by departing employees from Government agency custody ONLY with the approval of a Component Records Officer or Designated Official.
- (2) Copies of records that are publicly available, for example on the public DHS web site and/or available without a FOIA request.
- (3) Personal files, notes, or memos not related to Government agency business or transactions.
- (4) Personal files may contain references to or comments on agency business, but they are considered personal if they are not used to conduct business.
- (5) Documents labeled as "personal" or "private" and separate from the office's official records.
- (6) If information about official matters and agency business appears on the received document, the document is a Federal record. Agencies may make a copy of the document with the personal information deleted or redacted and provide copy for removal.

United States Secret Service
Directives System

Manual : Human Resources
RO : HUM

Section : HUM-19(04)
Date : 11/02/2022

From: HUM <HUM@OfficialMail.usss.dhs.gov>
To: USA <usa@OfficialMail.usss.dhs.gov>
Cc: HUM <HUM@OfficialMail.usss.dhs.gov>
Subject: DCP#: HUM 2022-47, Separation Procedures for All Employees
Date: Wednesday, November 2, 2022, 10:15 AM

//ROUTINE//

From: Headquarters (Office of Human Resources) DCP# HUM 2022-47
To: All Supervisors and Holders of the Office Human Resources Manual
Subj: Separation Procedures for All Employees

This directive is filed in front of the Human Resources Manual section HUM-19(04), "Separation Procedures for All Employees" and is in effect until superseded.

Reference is made to the Chief Operating Officer Official Message dated November 1, 2022, subject: "Actions to Enhance Retention and Preservation of Electronic Messaging." Reference also is made to the following concurrent directives:

- DCP# CIO 2022 16, CIO 04(06), "Mandatory Preservation of Records on Secret Service Issued Smartphones"
- DCP# RPM 2022-09, RPM-03, "Issuance and Use of eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices"

This directive implements revisions to SSF 3106 (Employee Separation Clearance) and SSF 4467 (Employee Separation Checklist) reflecting required completion of eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices."

Effective November 1, 2022, prior to separating from the agency or erasure/factory reset of their issued mobile device(s) for any reason, each affected employee must access the [USSS eForms Library](#) and complete eForm SSF 4468, "Documentation of Records Retention Activities for Mobile Devices." By completing this form, employees will document that they have examined their mobile device(s) for federal records and ensured that those records were preserved and retained on the agency's computer network. Supervisors are responsible for ensuring this requirement is fulfilled.

Questions regarding this message may be directed to the Office of Human Resources. Additionally, questions regarding the recordkeeping and preservation requirements in this message may be directed to the Office of Strategic Planning and Policy, Enterprise Records Management Division via e mail to Records@usss.dhs.gov.

Headquarters (Chief - Office of Human Resources) Magnuson/Hall

United States Secret Service
Directives System

Manual : Human Resources Manual
RO : HBS

Section : HUM-07(02), HUM-19(04)
Date : 01/27/2022

From: HUM
To: USA
Cc: HUM
Subject: DCP#: HUM 2022-02 USSS Employee Separation Survey
Date: Thursday, January 27, 2022 5:42:28 PM

//Routine//

FROM: Headquarters (Chief – Office of Human Resources) DCP#: HUM 2022 02

TO: All Supervisors and Holders of the Human Resources Manual

SUBJECT: USSS Employee Separation Survey

This directive should be filed in front of the Human Resources Manual Section HUM-19(04), Separation Procedures for All Employees, and HUM 07(02), Employee Performance Files.

This directive is in effect until superseded.

This directive updates Human Resources Manual section HUM-19(04), Separation Procedures for All Employees to state the employee separation survey ([USSS Separation Survey](#)) has been removed from the Workforce Planning Division (WP.) Intranet page and added to the Human Resources Business Solutions Division (HBS) intranet page. The link may be found on the HBS Homepage under HUM Surveys - Current Survey (titled USSS Separation Survey). Supervisors/managers should continue to ensure separating employees complete this electronic survey before departing the Secret Service. This survey is available for immediate use.

Please click on link below to view the survey:

[USSS Separation Survey](#)

Please contact the Human Resources Business Solutions Division (HBS) at HUMSurveys@ussc.dhs.gov if you have any questions.

Headquarters (Chief – Office of Human Resources)

Ashley/Yarwood

SEPARATION PROCEDURES FOR ALL EMPLOYEES

Issuance and Completion of Required Documents

As soon as the effective date of an employee's separation is known, supervisors or their authorized designees are responsible for forwarding an electronic SF 52, Request for Personnel Action, via HR Connect, to the Office of Human Resources, Benefits and Payroll Division (BPR) as soon as the effective date of an employee's separation is known. Supervisors must clearly enter the appropriate separation action (distinguishing between resignation or transfer to another federal agency) when entering in HR Connect. The BPR, Employee Benefits Branch (EBB) processes all types of retirement and separations. The BPR, Payroll Operations Branch (POB) processes all transfers. It is important to distinguish between resignations and transfers as benefits elections and annual lump sum payments will be affected. Offices must act promptly to ensure that each separating employee receives their final pay in a timely manner and no unearned salary is paid because of a delay in processing the separation.

Prior to the last day of employment, supervisors should ensure separating employees complete an electronic Employee Separation Survey. The Employee Separation Survey can be accessed by going to the Office of Human Resources, Workforce Planning Division's Intranet page. The Employee Separation Survey is located under the section entitled, "Quick Links."

Survey responses are confidential. The survey information will be used to provide the Secret Service management with summary reports regarding separations. Survey responses are confidential. When the survey is completed, the employee will receive an e-mail receipt which may be submitted to the supervisor and verified on Secret Service Form (SSF) 3106, Employee Separation Clearance.

The employee's supervisor is responsible for the initiation of the process detailed on the SSF 3106, Employee Separation Clearance. The separating employee is responsible for obtaining signatures for all record of clearances indicated on the SSF 3106; section II – Record of Clearances. The separating employee should return the SSF 3106 to their supervisor, who will ensure all appropriate sections have been completed. The supervisor will then forward the SSF 3106 to the Security Management Division (SMD) for final retention.

Supervisors must ensure employees complete Department of Homeland Security (DHS) Form 141-02, Documentary Materials Removal/Nonremoval Certification. Guidance for completing this form may be found in MNO-06(08), Removal of Papers in the Secret Service Record Programs Management Manual. Final retention of the DHS Form 141-02 is maintained by the Performance Management and Employee Relations Division (PRF).

Supervisors of separating employees are required to complete the SSF 3229, Re-Employment Recommendation and submit it to the Office of Investigations, Investigative Support Division, no later than two weeks following an employee's separation from the Secret Service.

Supervisors of separating employees are required to provide the employee's personal e-mail address and mailing address when entering a separation action in HR Connect. In an effort to streamline and expedite the notification process, a separation packet will be sent electronically to the separating employee's personal email address. In the event the employee does not have a personal email address, the separation packet will be mailed to the home address on record.

Procedures and Responsibilities

Employee Responsibilities

The employee is responsible for notifying their supervisor of the date and nature of separation from the Secret Service. If an employee is transferring to another agency, the employee should provide their supervisor with the name of the new agency and a Human Resources point of contact and phone number. The separating employee must contact the EBB at 202-406-5670 to discuss benefits matters.

If the separation action is a resignation the employee must complete a resignation action, SF 52, in HR Connect through the employee self-service menu and route it through the appropriate Assistant Director's or Executive Chief's Office for forwarding to BPR. The SF 52 should be submitted to BPR, at least one pay period before the separation date. The employee is also responsible for notifying the supervisor if their records are subject to a litigation hold.

Public Financial Disclosure Report

Employees who are required to file a Public Financial Disclosure Report (OGE Form 278) are required to file a termination 278 report within 30 days of separating from the U.S. Government. Employees with questions regarding this requirement should contact the Office of Chief Counsel.

Manager Responsibilities

If the separation action is a transfer the manager must complete a transfer action, SF 52, in HR Connect through the manager self-service menu and route it through the appropriate Assistant Director or Executive Chief's Office for forwarding to BPR. The SF 52 should be submitted to BPR at least one pay period before the separation date.

Accountable Property

Prior to the last day of employment, an employee must turn in their commission book, identification cards and other credentials, firearms, Secret Service badges, and all other Secret Service property for which the employee is accountable. The separating employee will return all accountable property to the property representative of their office. The employee's name should be removed from the Custodian field in Sunflower (a property tracking component of TOPS) except for lost, stolen, or damaged property. The employee's Personal Identity Verification (PIV) card should be returned to SMD for disposal. The appropriate division to which all property must be returned can be found in the Chief Financial Officer Manual, section AOD-02(01), Control of Individually Issued Property. Lost, stolen, or damaged property must be accounted for in accordance with Chief Financial Officer Manual, section AOD-06(05), Reporting Incidents of Loss of, Theft of, or Damage to Property.

Timekeeper Responsibilities

The separation date on the timecard must be the same as the date reflected on the SF 52 in order for the National Finance Center payroll/personnel system will not process the separation. It is the timekeeper's responsibility to note in the remarks section of the employee's final timecard the nature and effective date of the employee's separation.

The timekeeper is required to notify POB of the effective date of the employee's separation via webTA to ensure the required payroll system entry is made for the employee's separation to be processed automatically. Manual processing will delay the employee's transfer of leave or payment of lump sum and issuance of final paycheck.

Supervisor Responsibilities

The employee's supervisor is responsible for initiating the process detailed on the SSF 3106, Employee Separation Clearance, during last pay period of employment and ensuring that the completed form is sent to SMD for final retention. The supervisor must complete the electronic SF 52 at least one pay period prior to the effective date of the separation. EBB will complete the SF 52 for retiring employees.

Supervisors are required to ensure separating employees have completed the required service agreements related to Government-funded training and other recruitment and retention initiatives. For additional information regarding Employee's Agreement to Continue in Service, please refer to the following directives: Training Manual, section RTC-02(02), Training Requests, Human Resources Manual section HUM-10(08), Student Loan Repayment Program and DCP#: HUM 2016-09 (dated 04/12/2016) – "Tuition Assistance (Educational Reimbursement)" filed in from of section HUM-10(09).

In addition, supervisors are required to send an official message notifying all appropriate parties of the employee's intent to separate. (See sub-section, *Review of Financial Obligations*). The supervisor will forward the Employee Performance File to POB. The employee's time and attendance records should be retained in the employee's departing office for six full years. If there is no active or pending litigation involving the records, then the files can be destroyed in accordance with the records retention schedule.

If the employee notifies the supervisor that their records are subject to a litigation hold, the supervisor is responsible for collecting the records subject to the litigation hold, ensuring that the records are maintained in a secure location, and notifying the Office of Chief Counsel that the supervisor has collected the records.

Review of Financial Obligations

Notification of an employee's intent to separate will result in the determination and liquidation of any outstanding indebtedness prior to the termination of employment.

Upon notification of an employee's **intent to separate for any reason**, supervisors must notify the following: BPR, (both POB and EBB), PRF, Financial Management Division (FMD), Administrative Operations Division (AOD)/Property Management Branch, Office of the Chief Information Officer, Office of Integrity, Inspection Division, SMD, and other pertinent offices via official message and provide the following information:

1. Name of employee;
2. Office Name;
3. Social Security Number (truncate to last four digits);
4. Date of separation or beginning and ending date of nonpay status;
5. Reason for separation or entry into nonpay status (in as much detail as possible); and,
6. Date of assignment to the office (if it has occurred within the last twelve months).

Upon receipt of this information, FMD initiates a review of the employee's records for outstanding claims and AOD will review for any lost, stolen, damaged property pending financial liability. FMD formally notifies the requesting office/division of any outstanding amounts due from the separating employee. If there are no outstanding claims, a negative response is forwarded to the employee's office/division. POB should confirm with PRF whether the employee has satisfied the Service Agreement commitment for the Student Loans Repayment Program and/or Tuition Assistance if applicable.

Issuance of Final Paycheck

The POB will verify that the separating employee does not have an outstanding debt to the Secret Service. Every pay period the POB will provide a list of departing employees to FMD for authorization to release final paychecks and lump sum payments. Upon BPR's receipt of FMD authorization to release funds, the final paycheck for each employee will be routed through POB. If the employee has a debt, the salary check will be held until the debt is cleared, or the salary check will be offset to clear the debt. Once the debt is satisfied, the final salary is released and deposited electronically in the employee's account of record.

Notice Regarding Unemployment Insurance

Each office is responsible for ensuring the SF 8; Notice to Federal Employee about Unemployment Insurance is issued to each separating employee on or before their last day of work. This form must be issued to each employee who is separating, or placed in a nonpay status for seven days or more.

The SF 8 must contain the following address:

TALX
P.O. Box 66945
St. Louis, MO 63166

All Unemployment Compensation for Federal Employees Requests for Wage and Separation Information, Form ES 931, received from State employment security agencies should be transmitted immediately by express mail to the TALX at the following address:

TALX
1845 Borman Court
St. Louis, MO 63146

Failure to forward these forms immediately may result in the Secret Service being billed for unwarranted unemployment compensation payments.

Nondisclosure Notification and Agreement for Separating Employees

Separating employees must acknowledge and sign their consent to be legally bound to the terms contained in the SSF 4322A, Nondisclosure Notification and Agreement for Separating Employees. This agreement reaffirms the consent each employee previously signed as a Secret Service employee via SSF 4322, Employee Nondisclosure Notification and Agreement, consistent with Secret Service nondisclosure policy.

The separating employee's supervisor will forward the completed SSF 4322A to the SMD for inclusion in the employee's Personnel Security File.

Debriefings

All employees granted Top Secret security clearances and/or Sensitive Compartmented Information (SCI) access and who terminate employment with the Secret Service will be debriefed and the Top Secret and/or SCI access will be withdrawn. In short, the individual does not hold or have a security clearance if no longer employed by the Agency.

Employees assigned to Headquarters will be debriefed by SMD. For employees outside of Headquarters, the debriefing will be conducted by the employee's supervisor using the SSF 1776, "Certification Security Debriefing," and the SF 312, "Classified Information Nondisclosure Agreement." For those employees who have been read into SCI, the completion of Form 4414, "SCI Nondisclosure Agreement", is also required. In cases where the supervisor is unavailable to perform this function, SMD will administratively debrief the employee.

After the debriefing has been completed and all forms filled out and signed, the employee's clearance is withdrawn and will no longer be active. The separating employee will relinquish their DHS PIV card at this time. The separating employee's DHS PIV card and the completed SSF 1776, SF 312, and Form 4414 should be submitted to SMD for destruction or final retention.

If a former employee decides to transfer to another agency that requires a security clearance, the former employee can inform the hiring agency of their previous background investigation, and the clearance and/or access level granted. The hiring agency will be responsible for verifying the background information provided by the former employee, as well as any reciprocal recognition of the investigation or re-issuance/re-instatement of the Top Secret Security Clearance.

For additional information, refer to the Human Resources manual, section SCD-02(01), Special Security Clearances Requirements and Reporting.

REMOVAL OF PAPERS AND OTHER DOCUMENTARY MATERIALS

Background

44 U.S.C. 3105 requires that heads of Federal agencies establish safeguards against the removal or loss of records. These safeguards include notifying agency officials and employees that criminal penalties are provided for the unlawful removal or destruction of Federal records (18 U.S.C. 2071) and for the unlawful disclosure of certain information pertaining to national security (18 U.S.C. 793, 794, and 798).

Definitions

- a. Records. These include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved, or appropriate for preservation by that agency or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them (44 U.S.C. 3301).
- b. Documentary Materials. This is a collective term for records and nonrecord materials that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.
- c. Nonrecord Materials. These are Government informational materials that do not meet the statutory definition of records (44 U.S.C. 3301) or that have been excluded from coverage by the definition. Nonrecord materials are unofficial copies of documents kept only for reference, stock of publications and processed documents, and library or museum materials intended solely for reference or exhibit.
- d. Personal Papers. These are documentary materials, or any reasonably segregative portion thereof, of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of the agency business (36 Code of Federal Regulations (CFR) Part 1222).
- e. Documentary Materials Removal/Nonremoval Certification. This Department of Homeland Security form (DHS Form 141-02) formally documents the process of review and concurrence for removal or nonremoval of agency documentary materials. Before completing this form, separating employees must read the National Archives and Records Administration (NARA) publication *Documenting Your Public Service*, available at <http://www.archives.gov/records-mgmt/publications/documenting-your-public-service.html> so that by signing the form, employees also certify that they have read and understand the provisions of the above publication.

Procedures for Removal of Papers and Other Documentary Materials

No documentary material, even though judged to be nonrecord material, shall be withdrawn if this will create such a gap in the files as to impair the completeness of essential documentation. Indexes, or other finding aids, necessary to the use of the official files may not be removed.

Personal diaries, which are really private records of public activities, are private property and may be removed. When the matters dealt with in such work aids as office diaries, logs, memoranda of conferences and telephone calls are covered elsewhere by adequate records, such work aids may be removed.

Extra copies (carbons, photocopies, etc.) of records may be removed under certain circumstances, but only with the permission of the Secret Service.

Prior to removal, the separating employee's supervisor shall consult with the OSP Chief Records Officer and other cognizant Secret Service review officials to decide if a legal or policy reason exists for keeping the information contained therein confidential and that the record copy, and other necessary copies, are available in the Secret Service. If the copy is of a document originating with another agency, the wishes of the originating agency will also be determined and respected.

Material that is marked as national security information and officially limited information may not be removed from the Secret Service under any circumstances. Material so marked may include information pertaining to but not limited to:

- the enforcement of criminal/civil law relating to Secret Service matters;
- all protection related activities;
- Secret Service personnel rules and regulations; and
- sensitive or proprietary information relative to Secret Service policy.

Such information should remain classified, controlled or restricted as long as required for national security and/or Secret Service interest.

Any violation of the statutory and regulatory limitations placed on removal of papers by Secret Service officials who resign or retire will be forwarded to the Office of Professional Responsibility, who shall confer with the Inspector General regarding such violations.

If the private or nonofficial papers of a Secret Service official are kept in the official's office, they shall be filed separately from the official records of the office.

Responsibilities

Reviewing Official

The supervisor of a separating employee will serve as the primary reviewing official (see DHS Form 141-02) for documentary materials being requested for removal by departing employees. (Requests for removal of materials made by Component heads will be coordinated for review as directed by the DHS Chief Records Officer, through the Component Chief Records Officer.)

If documents are being proposed for removal, the reviewing official will:

- a. Obtain a signed Homeland Security Form DHS Form 141-02 from any departing employee desiring to remove documents (paper or electronic media) from the Secret Service.
- b. Review all documents being proposed for removal by an employee to ensure that none of the information being taken contains law enforcement data, trade secrets, national security or privacy material, or other interests protected by law. To do this, the reviewing official may require the requesting employee to provide documentation of concurrence (or seek it directly) in writing, from:
 - the Security Management Division
 - the Office of the Chief Counsel
 - Disclosure officials of the Office of Intergovernmental and Legislative Affairs
 - the Office of Communication and Media Relations
 - Assistant Directors/Executive Chiefs with subject matter responsibility for the content of the material

The Chief Records Officer should also be consulted following the outreach above, as the Chief Records Officer must also sign the DHS Form 141-02 when materials are requested for removal.

- c. Following signature by the Chief Records Officer, forward all signed DHS Form 141-02s to the Office of Human Resources.

Employees

All employees will:

- a. Certify to having read this "Removal of Papers" policy by signing the SSF 3218, "Annual Employee Certification".
- b. Notify the Chief Records Officer, Office of Strategic Planning and Policy, when they are about to remove any documents (paper or electronic media) from the Secret Service.
- c. Sign a DHS Form 141-02, when they resign or retire as part of their Department of Homeland Security - U. S. Secret Service Employee Separation Clearance Procedure.

- d. Be aware of the consequences of violation of the statutory and regulatory limitations on removal of papers.

Office of Human Resources

The Office of Human Resources will:

- a. Obtain a signed DHS Form 141-02, "Documentary Materials Removal/Nonremoval Certification", from all employees when no documents are being removed. This will be accomplished at the time of separation.
- b. Maintain all signed copies of the DHS Form 141-02 for three (3) years after the separation or retirement of an employee from the Secret Service.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001, section 2001.80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER <i>(See Notice below)</i>
-----------	------	--

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS <i>(Type or print)</i>		NAME AND ADDRESS <i>(Type or print)</i>	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS <i>(Type or print)</i>	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

5. ARTICLE	Serial Number	Date of Issue	Initials of Receiver	RETURNED	Serial Number	Date of Issue	Initials of Receiver	RETURNED
				Date and Initials of Supervisor				Date and Initials of Supervisor
Commission Book								
Secret Service Identification								
Badge								
Lapel Emblem Set								
Lapel Emblem Set								
Lapel Emblem Set								
Gun								
Gun								
Holster								
Handcuffs								

I certify, under penalty of law, that I have on this date, _____, returned and have been issued a receipt for all property above charged. I further certify that no official property, counterfeit notes, coins, stamps, or other counterfeit obligations of the United States, or of any foreign country, or copies of any official reports, papers, or documents, whatsoever are in my possession, custody or control.

 (Signature of Witness)

 (Signature of Employee)

CERTIFICATION OF SECURITY DEBRIEFING	NAME OF PERSON DEBRIEFED		FILE NO. 163-802-
	DATE DEBRIEFED	OFFICE ASSIGNED	

I certify that I have received a debriefing and I understand the importance to the national security of continuing to safeguard classified and other information as well as devices of the U.S. Secret Service.

I am aware of my legal and moral responsibility in this regard. I also understand that I will continue to be bound by all security regulations pertaining to the Top Secret clearance I received.

I realize that I am subject to those criminal penalties described by law (18 USC 793, 794, and 798) for the willful or inadvertent disclosure of classified information.

I further certify that I do not have in my possession any official property of the U.S. Secret Service, any official reports or documents, or copies thereof, or any contraband of any type.

Signature of Person being Debriefed

Debriefing Conducted By

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service

Nondisclosure Notification and Agreement for Separating Employees

1. I _____ as a separating employee of the United States Secret Service (Secret Service) intending to be legally bound, acknowledge the provisions of and consent to the terms contained in this Nondisclosure Notification and Agreement (Agreement).
2. This Agreement reaffirms the consent I previously provided as a Secret Service employee via SSF 4322 on _____, given in consideration of my being granted access and proximity to certain information, individuals, and locations, to include access and proximity to Classified information; Sensitive But Unclassified information; any other information of a personal and non-public nature; and individuals, facilities, and locations protected or secured by the Secret Service pursuant to Title 18 of the United States Code, sections 3056(a) and 3056A, or as otherwise designated by the President of the United States.
3. For the purposes of this Agreement, the following definitions apply:

Classified information is any information or material that has been determined by the United States Government pursuant to an Executive Order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r of section 11 of the Atomic Energy Act of 1954; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4 of Executive Order 13526, or under any other Executive order or statute that provides protection for such information in the interest of national security.

Sensitive But Unclassified information is information the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Such information includes: the protective methodologies, practices, and policies of the Secret Service, which have not been specifically prohibited from disclosure by an Executive Order or an Act of Congress to be kept secret in the interest of national security; as well as information that would not be available to the public pursuant to the Freedom of Information Act, Title 5 of the United States Code, section 552 (hereinafter FOIA), exemptions (b)(7)(C), (b)(7)(E), and (b)(7)(F). Sensitive But Unclassified material includes (but is not necessarily limited to) the following types of information:

- **For Official Use Only (FOUO)**, as defined by the Department of Homeland Security, is the term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Within the Secret Service, FOUO includes the following types of information:
 - Protection Sensitive information** - information or material that may be considered sensitive to the Secret Service or its protectees and is generally not known or readily ascertainable outside the Secret Service. Protection Sensitive information may include: information concerning the protective methodologies, practices, and policies of the Secret Service; information of a personal or confidential nature obtained through observation of or proximity to individuals with whom employees come into contact as a result of the Secret Service's protective mission as set out in Title 18 of the United States Code, sections 3056 and 3056A; information concerning the features, structures, and workings of buildings and other spaces protected or secured by the Secret Service pursuant to Title 18 of the United States Code, sections 3056 and 3056A acquired by contact with, observations of, or experiences with such facilities or locations as a result of an employee's duties.
 - Law Enforcement Sensitive information** - information compiled for a law enforcement purpose that if released: (1) could reasonably be expected to interfere with enforcement proceedings; (2) would deprive a person of a right to a fair trial or an impartial adjudication; (3) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (4) could reasonably be expected to disclose the identity of a confidential source; (5) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or (6) could reasonably be expected to endanger the life or physical safety of any individual.
- **Grand Jury information** is information that reveals matters discussed before the grand jury. Protected information includes transcripts of grand jury proceedings, subpoenas and other orders issued by a grand jury, documents shown to the grand jury during an investigation, or the substance of testimony presented to a grand jury.
- **Privacy Act Protected information** is information the release of which may occur only in accordance with the Privacy Act, Title 5 of the United States Code, section 552a.

Initial here: _____

4. Through this Agreement I acknowledge that during the course of my employment with the Secret Service, I may have become aware of or privy to information: the disclosure of which could adversely impact the mission of the Secret Service; the disclosure of which is prohibited under Federal law; the disclosure of which could result in the imposition of civil or criminal penalties against the Secret Service or against me in my personal capacity; the disclosure of which would be in violation of the Privacy Act; and/or the disclosure of which is in violation of the policies and practices of the Secret Service and could result in disciplinary or adverse action being taken against me.
5. Such information may have included Classified information, or Sensitive But Unclassified information (to include For Official Use Only information, Grand Jury information, and Privacy Act Protected information). All such information is considered property of the Secret Service and is to be used for official purposes only.
6. I understand that by being granted access and proximity to such information, and to individuals and locations protected and secured by the Secret Service, the United States Government has placed special confidence and trust in me and that I am obligated to protect and safeguard this information in accordance with the terms of this Agreement.
7. Therefore, I agree that except as authorized or required by law, I shall not disclose such information to anyone outside the Secret Service without prior approval by the Secret Service.
8. I understand and agree that I shall not dispense, disseminate, or otherwise make available to any person, any Classified or Sensitive But Unclassified information obtained by virtue of my employment with the Secret Service, except that which may be provided lawfully through established procedures. This prohibition applies to, but is not limited to, protective and investigative information, information concerning a protectee obtained through proximity to the protectee or observations of the protectee, and information pertaining to employment, change of station, temporary assignments, and other items regarding the personal status of Secret Service employees.
9. I further understand and agree that I may not make available any Classified or Sensitive But Unclassified information obtained by virtue of my employment with the Secret Service on any social media platform.
10. Additionally, as a former employee of the Secret Service, I will not make use of any Classified or Sensitive But Unclassified information for my own purposes or benefit, or for the purposes or benefit of anyone or any entity other than the Secret Service.
11. I understand and agree that the Secret Service has a right to pre-publication review. Prior to any submission for publication, I will submit to the Secret Service for review any book, article, column, or other written work intended for publication that is based upon any knowledge or information I obtained during the course of my employment with the Secret Service. This submission will be made in order for the Secret Service to ensure that no Classified information or Sensitive But Unclassified information is disclosed prior to publication or distribution outside the Secret Service.
12. With respect to publication of information obtained during the course of my employment at the Secret Service, I understand and agree the United States Government will be assigned all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of Classified information or Sensitive But Unclassified information made by me, that is not consistent with the terms of this agreement.
13. I understand that, pursuant to Title 18 of the United States Code, section 709, it is a criminal violation to, except with the written permission of the Director of the Secret Service, knowingly use the words "Secret Service," "Secret Service Uniformed Division," the initials "U.S.S.S.," "U.D." or any colorable imitation of such words or initials in connection with, or as part of any advertisement, circular, book, pamphlet, or other publication, play, motion picture, broadcast, telecast, or other production, in a manner reasonably calculated to convey the impression that any such item, publication, or product, is approved, endorsed, or authorized by or associated in any manner with, the Secret Service or the Secret Service Uniformed Division. Use of the name of the Secret Service in the manner described may be subject to injunction upon complaint of the Secret Service or the Department of Homeland Security. A violation of section 709 is punishable by fine or by imprisonment of not more than one year.
14. I understand and agree that as a result of my employment with the Secret Service, my obligation to maintain the confidentiality and security of information described above remains even after my employment with the Secret Service ends, and continues for so long as such information remains Classified or Sensitive But Unclassified (to include any corresponding successor designations), or otherwise private or protected.

Initial here: _____

15. I understand and agree that the restrictions set forth in this agreement are consistent with and do not supersede, conflict with, or otherwise alter the obligations, rights or liabilities created by Executive Order 13526; section 7211 of Title 5, United States Code (governing disclosures to Congress); section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421, et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

Further, these provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General or the Office of Special Counsel of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

16. **Possession and Release of Agency Documents.** I understand that I am prohibited from utilizing, taking, or making copies of Secret Service documents, records, electronic records, or files for personal use or for personal benefit. Personal benefit includes creating, keeping, or copying a Secret Service document as a memento or for the purpose of providing the document to a personal attorney, personal representative, or representative of the media. I understand and agree that should I wish to retain or take possession of a copy of a Secret Service document as a memento or for any other personal use, I must first request and obtain the permission of my supervisor. If endorsed by the supervisor, I will complete the Secret Service's officially designated "Documentary Materials Removal/Nonremoval Certification" form for further processing, after which approval/non-approval will be determined.

This prohibition and requirement do not apply to personnel documents concerning me (e.g., Standard Forms (SF) 50, performance appraisals, disciplinary documents, annual and sick leave requests); forms completed by me to receive reimbursement, document hours of work, or to meet other Government requirements (e.g., travel vouchers, financial disclosure forms, security clearance forms); documents submitted by me concerning my own grievances or other complaints; and documents provided to me in the course of an administrative action.

This prohibition and requirement do apply to and limit my right to utilize and possess documents and other items authored by me as an employee in the course of my employment with the Secret Service including, but not limited to, investigative reports, administrative studies, legal documents and filings, protective and technical memoranda and analysis, computer code, databases or spreadsheets, and e-mail.

17. I understand and agree that each provision of this Agreement is severable, and that if a challenge was brought to this Agreement, and should a court find any provision or portion of this Agreement to be unenforceable, all other provisions and portions shall remain in full force.

18. My execution of this Agreement does not nullify or affect in any manner any other secrecy or nondisclosure agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

19. This Agreement, consisting of 3 pages, is entered into in good faith, without mental reservation or purpose of evasion.

Typed/Printed Name

Signature

Date

The separating employee's supervisor will forward this completed SSF 4322A to the Security Clearance Division for inclusion in the separating employee's Personnel Security File.

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service
EMPLOYEE SEPARATION CHECKLIST

Name	Last Four of SSN
Personal Phone	Personal Email
Separation Date	Home Address
USSS EOD Date	Supervisor's Name
Type of Separation <input type="checkbox"/> Retirement <input type="checkbox"/> Resignation <input type="checkbox"/> Termination <input type="checkbox"/> Transfer to Another Agency	Agency Transferring To

FORM NO.		DESCRIPTION	DISPOSITION	ATTN.
N/A	<input type="checkbox"/>	Initiate Debriefing – AO Briefing Dashboard	SMD	AO Debriefing Dashboard
N/A	<input type="checkbox"/>	HR Connect personnel action for resignations/transfer to another agency only; transfer to another gov't agency is a "termination" action; EBB will complete for retiring employees	Employee's Office	Ensure you list the employee's personal email and current mailing address withing HR Connect for official purposes
N/A	<input type="checkbox"/>	Separation Official Message	Supervisors must send an OM notifying all parties of the employee's intent to separate (See ATTN.)	BPR (POB, EBB), PRF, FMD, AOD Property Mgmt. Division, CIO, ITG, ISP, SMD
N/A	<input type="checkbox"/>	Check for outstanding Continuing Service Agreement(s)	BPR/POB	
DHS 141-02	<input type="checkbox"/>	Documentary Material Removal Nonremoval Certification	PRF	HUM-19(04); email to (b)(6); (b)(7)(C)
SSF 4322A	<input type="checkbox"/>	Nondisclosure Notification and Agreement for Separating Employees	SMD	AO Debriefing Dashboard
SSF 1776	<input type="checkbox"/>	Certification of Security Debriefing	SMD	AO Briefing Dashboard
SSF 3229	<input type="checkbox"/>	Re-Employment Recommendation	PARIS	
SF 312	<input type="checkbox"/>	Classified Information Nondisclosure Agreement	SMD	AO Debriefing Dashboard
SSF 3106	<input type="checkbox"/>	Employee Separation Clearance	SMD	Email to (b)(6); (b)(7)(C)
SSF 4414	<input type="checkbox"/>	Sensitive Compartmentalized Information Nondisclosure Agreement (found under the Non-Secret Service Form Tab in Forms Library)	SMD	AO Debriefing Dashboard
SSF 1638	<input type="checkbox"/>	Official Property Receipt (signed when returning property)	AOD	AOD-02(02)
SF 8	<input type="checkbox"/>	Unemployment Notice	Employee	
OGE 278	<input type="checkbox"/>	Financial Disclosure Report	LEG	If applicable, email to (b)(6); (b)(7)(C)
SSF 1780	<input type="checkbox"/>	Weapons Receipt	RTC	Baton: forward copy to AOD with the Baton Pistol: send copy with weapon to RTC via registered mail Retain a copy in Admin File 501.022; transfer assets in Sunflower
SSF 4073	<input type="checkbox"/>	Retired (Firearm) Identification Card Request and Waiver Form	FSD	Mail hardcopy to Brendan Westphal (FSD); attach photo/NCIC checks
SSF 4073C	<input type="checkbox"/>	Documentation of "Good Standing" (LEOSA)	FSD	ITG-07(01); mail hardcopy to Brendan Westphal (FSD)

N/A	<input type="checkbox"/>	Have employee complete the USSS Separation Survey		HUM quick links or HBS "current surveys"
N/A	<input type="checkbox"/>	Run Sunflower individual property report		
N/A	<input type="checkbox"/>	Send Official Message to Deactivate PIV after employee departure	SMD	
N/A	<input type="checkbox"/>	Get approval from AOD in Sunflower for PIV disposal; destroy PIV card locally		
N/A	<input type="checkbox"/>	Active Directory Account Disabled		Email request to (b)(6); (b)(7)(C) with effective date
N/A	<input type="checkbox"/>	OSR (Office Security Rep) submits a ticket via the IT Portal requesting the account be disabled. Ticket should be assigned to Cyber Security		IT Portal/Cyber Security
N/A	<input type="checkbox"/>	Turn in Accountable Property		See accountable property checklist below
N/A	<input type="checkbox"/>	Timecard (WebTA) – timekeeper make the appropriate "status change" entry	Employee's timekeeper	TAM-03
SSF 3115VIB	<input type="checkbox"/>	Farewell Logo Mat (employee's preference – yes or no)	FSD/GDB	Email request to (b)(6); (b)(7)(C)
N/A	<input type="checkbox"/>	Retirement Wall (retired employee only)	BPR	BPR/Benefits (Retirement Wall) Dashboard
N/A	<input type="checkbox"/>	Close USA Performance Profile		USA Performance

PROPERTY CHECKLIST

ITEM	SEND TO	DESTROY LOCALLY	MEMO/EMAIL
<input type="checkbox"/> Badges (LG/SM)	AOD - transfer asset in Sunflower; retiring agents – can be encased in Lucite (obtain order form from BPR/EBB prior to official retirement date)		Memo and email to AOD Liaison
<input type="checkbox"/> Ballistic Vest	AOD – mail vest to AOD warehouse; transfer asset in Sunflower; attach date and tracking info; RTC-05(02)		Memo and email to AOD Liaison
<input type="checkbox"/> Baton	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Handcuffs	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Lapel Pins	AOD – transfer asset in Sunflower; attach date and tracking info		Memo and email to AOD Liaison
<input type="checkbox"/> Radio – Handheld	Return radio and accessories to CIO Radio, transfer radio in Sunflower; attach date and tracking to: (b)(6); (b)(7)(C) or more info; Portables Systems Group (b)(6);		
<input type="checkbox"/> Gas Card	Request permission for destruction, AOD-12(04)	X	Memo and email to (b)(6); (b)(7)(C)
<input type="checkbox"/> Commission Book	Transfer to SMD in Sunflower (Resignation/Transfer to Other Agency) or BPR-EBB (Retirement); convert to award in Sunflower if employee wants it stamped "retired" (BPR- (b)(6); (b)(7)(C))		Memo and email
<input type="checkbox"/> DHS Card/Employee ID Card	Transfer to SMD in Sunflower (Resignation/Transfer to Other Agency) or BPR-EBB (Retirement – APT Only)		Memo and email
<input type="checkbox"/> Laptop	CIO or Regional CIO Rep; Reassign in Sunflower		
<input type="checkbox"/> PIV Card	After OM is sent, put up for disposal in Sunflower; then Final Event and destroy locally	X	SMD Deactivation Official Email
<input type="checkbox"/> GETS Calling Card	Email for deactivation; Final Event in Sunflower once deactivated	X	
<input type="checkbox"/> Thumb Drive	Put up for disposal in Sunflower; then Final Event and destroy locally	X	
<input type="checkbox"/> Gun	Send to RTC; attach date and tracking info		
<input type="checkbox"/> Radio	Send to CIO-16/RCB (Call (b)(6); drop code before shipping)		Memo
<input type="checkbox"/> Cell Phone	Wipe and keep as space; CIO-04(06); Wireless Communication Section (b)(6); (b)(6);		Disposal Procedures

<input type="checkbox"/>	Purchase Card	Approving official send email for cancellation after all outstanding transactions are verified in TOPS; FMD-18(02)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	Fleet Card and/or WEX Card	Send email for cancellation after all outstanding transactions are verified; AOD-12(04)	X	Email (b)(6)
<input type="checkbox"/>	CBA Travel Card	Send email for cancellation after all outstanding transactions are verified; FMD-14(02)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	IBA Travel Card	Send email for cancellation after all outstanding transactions are verified; AOD-12(04)	X	Email (b)(6); (b)(7)(C)
<input type="checkbox"/>	Official Passport	All diplomatic/official passports must be returned to Liaison Division, Passport and Visa Office (LIA/PPT); LIA-04		Coordinate with LIA/PPS at (b)(6);
<input type="checkbox"/>	Gas mask	ATTN: TSD-CBSM (Equipment Return), (b)(6); (b)(7)(C) Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6)		Memo
<input type="checkbox"/>	Gas Mask Carrier	ATTN: TSD-CBSM (Equipment Return), (b)(6); (b)(7)(C) Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6)		Memo
<input type="checkbox"/>	Chemical Biological Protective Ensemble (CBPE Kit)	ATTN: TSD-CBSM (Equipment Return), (b)(6); (b)(7)(C) Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6)		Memo
<input type="checkbox"/>	Issued TSD-CBPE Carrying Bag	ATTN: TSD-CBSM (Equipment Return), (b)(6); (b)(7)(C) Hyattsville, MD 20785; shipping notification w/ tracking number sent to (b)(6)		Memo
<input type="checkbox"/>	Raid Jacket	Keep in office		
<input type="checkbox"/>	Office Keys	Keep in office		
<input type="checkbox"/>	Garage Pass	Keep in office if GOV; return to AOD if POV – AOD-10(02)		
<input type="checkbox"/>	Government Vehicle	Keep in office (car key, placard, gas card)		
<input type="checkbox"/>	Classified Courier Card	Send to SMD; attach date and tracking information		
<input type="checkbox"/>	Shout Nanos	Return to IPD		
<input type="checkbox"/>	Hotspot	Return to IPD or CIO, which it was assigned from		
<input type="checkbox"/>	Local Airport Access Pass	Keep in office		

[Find your AOD property representative here](#)

[Find your BPR liaison here](#)

Form Processed by (Name/Date):

Supervisor:

Supervisor Signature:

Note: For updates to this form, contact the Benefits and Payroll Division (BPR) at (b)(6); (b)(7)(C)

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service
EMPLOYEE SEPARATION CLEARANCE
(see instructions on page 3)

SECTION I - EMPLOYEE DATA

1. NAME (First, Last, MI):		2. SOCIAL SECURITY NUMBER:	3. DEPARTURE DATE:
4. ORGANIZATIONAL UNIT AND POD:	5. TITLE AND GRADE OF PRESENT POSITION:	6. TELEPHONE NUMBER (include a/c): Office (needed): Home:	
7. ADDRESS (including ZIP code):			
8. E-MAIL ADDRESS (personal):			

SECTION II - RECORD OF CLEARANCES (To be completed by officials indicated).

PART ONE. ADMINISTRATIVE OPERATIONS DIVISION, PROPERTY MANAGEMENT BRANCH

No unresolved reports of damaged, lost and/or stolen property. Reports of damaged, lost and/or stolen property pending; pertinent information is attached.

Did the employee participate in the Public Transportation Incentive Program (PTIP)? Yes No If yes, have benefits been canceled? Yes No

Did the employee participate in the Executive Parking Program? Yes No If yes, has the employee returned his/her parking pass? Yes No

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - PROPERTY MANAGEMENT BRANCH:	

PART TWO. LIAISON DIVISION, PASSPORT AND VISA OFFICE - The above named employee's diplomatic/official passport status has been reviewed and:

All diplomatic/official passports must be returned to the Passport and Visa Office without exception

If employee is retiring, request the diplomatic/official passport as a souvenir.

If employee is transferring to the private sector, the passport(s) will be returned to Department of State for destruction.

If employee anticipates being hired as a rehired annuitant, Liaison Division will retain the passport(s).

If employee is transferring to another agency, passport(s) will be returned to Department of State with a request to transfer to the gaining agency.

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - LIAISON DIVISION, PASSPORT AND VISA OFFICE:	

PART THREE. FINANCIAL MANAGEMENT DIVISION - The above named employee's fiscal records have been reviewed and the employee is:

Not in debt to the Secret Service and is cleared for release. In debt to the Secret Service, pertinent information attached. Other

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - FINANCE AND ACCOUNTING BRANCH:	

PART FOUR. BENEFITS AND PAYROLL DIVISION (Payroll Operations Branch) - The above named employee's Continued Service Agreement record(s) has been reviewed and the employee is:

Not in debt to the Secret Service and is cleared for release. In debt to the Secret Service, pertinent information attached. Other

NON-HUMAN E-MAIL ROUTER:	DATE:
SIGNATURE - BENEFITS AND PAYROLL DIVISION:	

PART FIVE. Supervisor or Delegate will verify the following:

- A. All separation actions must be entered on or before the effective date or the separation to avoid delay in processing the annual lump sum payment (see HUM-19(04)). Please be sure to enter the separation action accordingly (Resignation from the federal government vs. Transfer to another federal agency) as benefits could be impacted. Please check appropriate line:
- SF 52, Request for Personnel Action, has been forwarded to the Benefits and Payroll Division upon notification of the separation date. (See Human Resources Manual section HUM-19(04).)
 - Employee is separating without giving a two-week notice, therefore, the Benefits and Payroll Division was notified by sending a fax copy of the SF 52. The SF 52 will be forwarded to the Benefits and Payroll Division as soon as possible thereafter. (See Human Resources Manual section HUM-19(04).)
- B. Procedures outlined in Human Resources Manual section HUM-19(04) have been complied with as regards notifying the Financial Management Division of the intended separation.
- NOTE:** Field Offices are to use an Official Message to accomplish this requirement if there are time constraints.

PART FIVE (CONTINUED). Supervisor or Delegate will verify the following:

- C. Accountable items and property issued to the above employee have been collected and will be disposed of according to the procedures of Office of the Director Manual, section AOD-02(05).
Please check appropriate line:
_____ All issued accountable items and property were returned in good condition.
_____ Circumstances concerning unreturned or damaged accountable items and property have been reported in accordance with Office of the Director Manual, section AOD-06(05).
- D. _____ SF 8, "Notice to Federal Employee About Unemployment Insurance," has been issued per Human Resources Manual, section HUM-19(04).
- E. _____ Employee has contacted the Office of Human Resources, Benefits and Payroll Division, Employee Benefits Branch at BPR-Benefits@uss.s.dhs.gov, concerning health, life, and retirement benefits. Name of Employee Benefits Branch employee that separating employee contacted: _____ Date contacted: _____
- F. _____ SSF 3229, "Re-Employment Recommendation," has been completed and forwarded to the Office of Investigations, Investigative Support Division.
- G. _____ SSF 4322A, "Nondisclosure Notification and Agreement for Separating Employees," has been completed and forwarded to the Security Management Division for inclusion in the Employee's Personnel Security File.
- H. _____ Employee Separation Survey has been completed via Secret Service MSForms (this survey is anonymous).
- I. _____ Employee has read the National Archives and Records Administration (NARA) publication Documenting Your Public Service; and DHS Form 141-02, "Documentary Materials Removal/ Nonremoval Certification," has been provided, signed as appropriate, and forwarded to the Performance Management and Employee Relations Division (PRF).
- J. _____ Employee has completed the period of service agreed upon for Government-funded training per Training Manual section RTC-02(02).
(Law Enforcement Employees Only) Supervisor has initiated SSF 4073C, "Documentation of "Good Standing" (LEOSA)," and provided to Office of Integrity.
- K. _____ Employee is aware of process for requesting a LEOSA card and has access to the SSF 4073, Retired/Former Employee (Firearm) Identification Card Request and Waiver Form and associated forms in the SSF 4073 series. (See ITG-02)
- L. _____ Employee has properly closed out of any non-USSS accounts or systems (e.g., Cornerstone Services on Demand (CSOD), etc.)
- M. _____ Employee has contacted the Office of the Chief Counsel/Ethics Staff to obtain post-government employee guidance.
- N. _____ (OGE Form 278 Public Financial Disclosure Report Filers Only) Employee has contacted the Office of the Chief Counsel, Secret Service Ethics Program at ethics@uss.s.dhs.gov.

PART SIX. DEBRIEFING CERTIFICATION - See Human Resources Manual section SCD-02(01), for authorized debriefing officials. The above named individual has been properly debriefed and: _____ has executed SSF 1776 _____ has executed other appropriate debriefing forms
_____ (Top Secret Clearance)

SIGNATURE OF DEBRIEFING OFFICIAL:	DATE:
SIGNATURE OF SUPERVISOR OR DELEGATE:	DATE:

SECTION III - EMPLOYEE CERTIFICATION

I, the undersigned, make the following statement in connection with my separation from U.S. Secret Service subject to exceptions, if any, which I have fully explained below.

- a. I have returned to the responsible official all Government property and identification for which I was accountable or which I had in my possession.
- b. I have no indebtedness to the U.S. Secret Service for travel advances, imprest fund allowances, advanced leave, overpayment of salary, or other.
- c. I have no unsatisfied period of obligated service for travel or transportation to my first post of duty, to a new post of duty, or for training.

- d. I have returned to responsible officials all data in any form such as internal management documents, written information of a confidential nature, reference materials, or other documents containing data of an official nature; furthermore, I have not copied nor retained any such data in my possession.
- e. I agree not to reveal to any person any classified information, information of a confidential nature, information for limited official use, sensitive information, or any other information that is for official use only, of which I have knowledge, unless officially authorized to do so by appropriate officials of the U.S. Secret Service.

EMPLOYEE'S STATEMENT OF EXCEPTIONS:

SIGNATURE OF EMPLOYEE:	DATE:
------------------------	-------

SECTION IV - SUPERVISOR'S STATEMENT OF EXCEPTIONS

SIGNATURE OF SUPERVISOR OR DELEGATE:	DATE:
--------------------------------------	-------

INSTRUCTIONS

This form is to be initiated by the separating employee's supervisor on the last pay period of employment. Separating employees are those who are either resigning, retiring, transferring to another Government agency or otherwise leaving the employ of the Service.

A. Procedures for Separating Field Employees

Field SAICs will:

1. Complete Section I; Section II, Part Five;
2. Explain Employee Certification and have employee sign in Section III;
3. Complete Section IV, if applicable; and
4. Sign form in Section IV where indicated and forward original copy to Administrative Operations Division, Property Management Branch.

B. Procedures for Separating Headquarters Employees

Appropriate Headquarters supervisors will:

1. Complete Section I; Section II, Part Five;
2. Explain Employee Certification and have employee sign in Section III;
3. Complete Section IV, if applicable;
4. Sign form in Section IV where indicated; and
5. Instruct employee to hand carry original copy to the Administrative Operations Division (Property Management Branch), the Liaison Division (Passport and Visa Office) if applicable, the Financial Management Division, and the Benefits and Payroll Division for signature in Section II; and ultimately hand carry original copy to the official responsible for his/her debriefing (Security Management Division).

Headquarters employees who are separating will:

1. Hand carry the completed original form to the Administrative Operations Division, Property Management Branch, for signature;
2. Hand carry the completed original form to the Liaison Division, Passport and Visa Office, if applicable, for passport status review;
3. Hand carry the completed original form to the Financial Management Division, Accounting Branch, for determination of employee indebtedness;
4. Hand carry the completed original form to the Benefits and Payroll Division for signature; and
5. Hand carry the completed original form to the Security Management Division for signature. The Security Management Division will retain the form for inclusion in employee's Personnel Security File.

PRIVACY ACT STATEMENT: Executive Order 9397 authorizes use of the Social Security number to identify and distinguish between individuals with similar or identical names or initials. Furnishing your Social Security number, as well as other personal data, is voluntary. Failure to provide this information may result in delays in issuance of final pay checks and other benefits.

EMPLOYEE PLEASE NOTE

Clearances must be verified by Financial Management Division before release of FINAL SALARY and LUMP SUM LEAVE (if appropriate) checks.

DEPARTMENT OF HOMELAND SECURITY
United States Secret Service

DOCUMENTATION OF RECORDS RETENTION ACTIVITIES FOR MOBILE DEVICES

As required by the DHS Secretary's Decision Memorandum signed September 14, 2022, and effective November 1, 2022:

Prior to offboarding or erasure of their mobile device(s) for any reason, each employee must document that they have examined their mobile device(s) for any records sent or received that were created through electronic messaging.

Please review the instructions in the following, step-by-step guides:

[DHS Records Management 101 Job Aid](#)

[USSS Preserve Content Guide for iPhone and iPad](#)

then select the applicable statement below, before submitting this form.

- I HAVE** created or received electronic messages that would be considered a Federal record, and:
- I have retained those records.
 - My retention of these records follows DHS policy and guidance.
 - These records are filed in a standard accessible location (screenshots have been saved to my Pictures folder in my OneDrive account, and e-mailed to my Secret Service e-mail address).
 - I have forwarded any records created on personal devices or accounts due to exigent circumstances while conducting official government business to a government account and have stored them in compliance with DHS policy and guidance.
 - I have complied with any preservation request, including legal holds, and have preserved all records responsive to the preservation request(s) in a manner accessible by Department or Secret Service counsel.
- I HAVE NOT** created or received any electronic messages that would be considered a Federal record, and that would require action on my part in order to be retained.

SUBMIT

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 26 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

Backup

Backup content (if needed). A guide for preserving content can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up **and are near a Blueline device to complete the enrollment process**, wipe your device to enroll in Intune. *Go to “Settings->General->Reset->Erase All Content and Settings”*

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

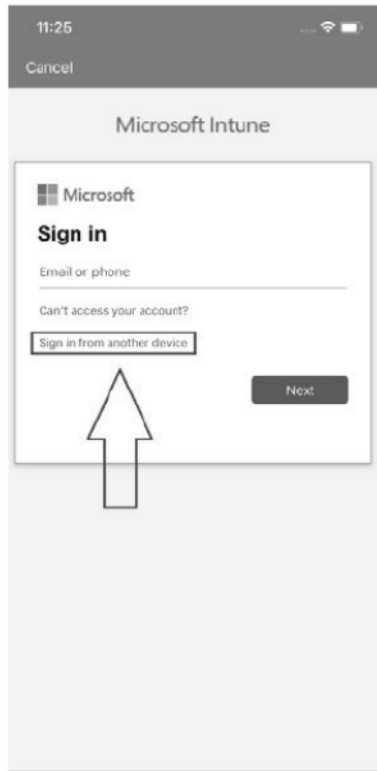
- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, immediately followed by an error message regarding “Guided Access” – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select "Sign in"

On the iPhone/iPad you are enrolling, **Select "Sign in from another device"**



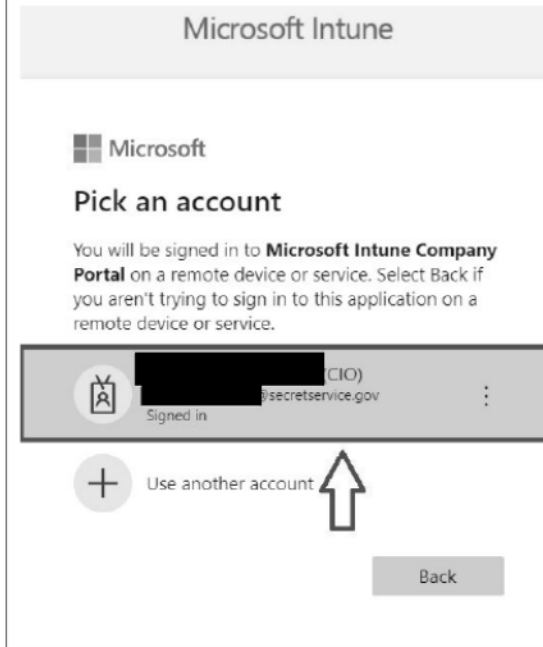
It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.



On your blue line PC, go to the website listed in the prior step. Enter the code your see on your phone from the prior step (**This is not case sensitive**).



On your blue line PC, select your **@secretservice.gov** account. If your account is not listed and it asks for you to type it in, use your Teams address (usually **[redacted]@secretservice.gov**)



On your blue line PC, select "Sign in as current user"



Enrollment Continued...

On your blue line PC, once successful, you will see the below message and will be done with the PC.

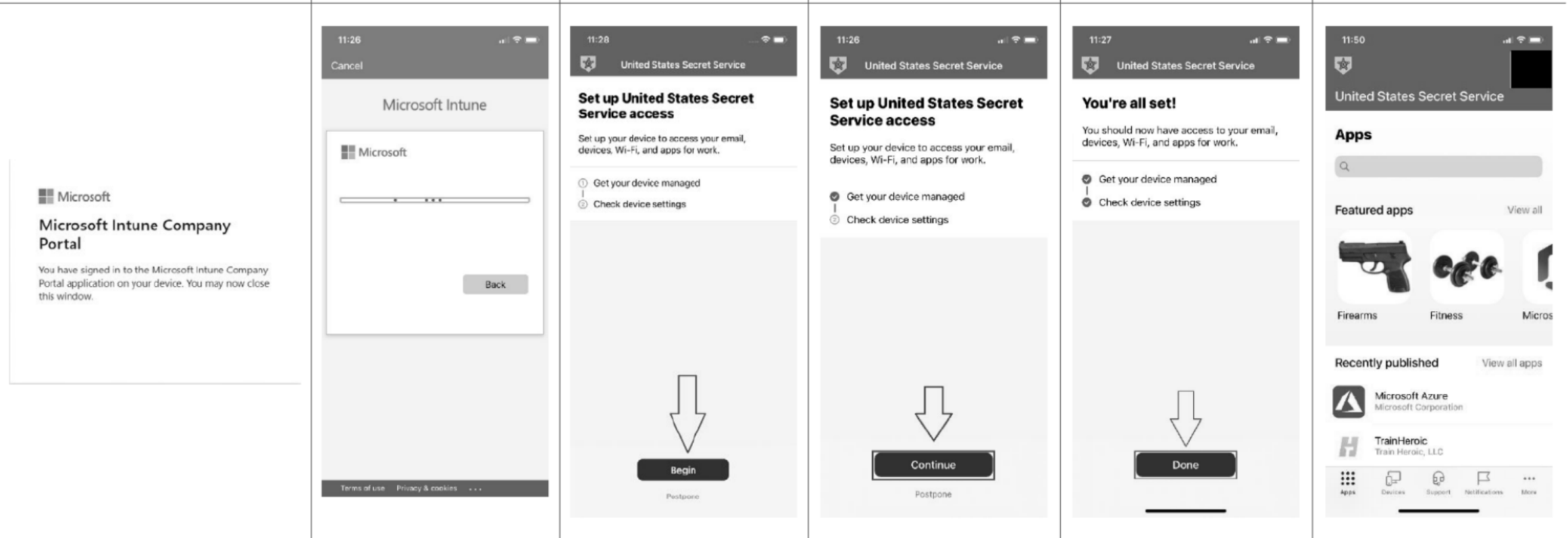
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 27 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

Backup

Backup content (if needed). A guide for preserving content can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up and are at a **USSS blue line connected or USSS VPN connected PC to complete the enrollment process**, wipe your device to enroll in Intune. Go to “Settings->General->Reset->Erase All Content and Settings”

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, immediately followed by an error message regarding “Guided Access” – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select **“Sign in”**

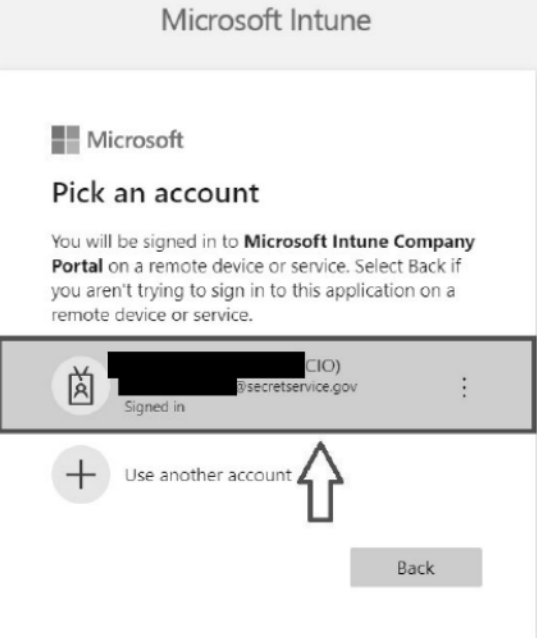
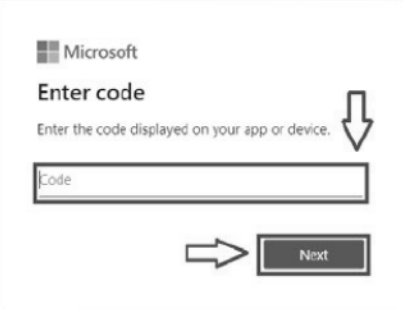
On the iPhone/iPad you are enrolling, **Select “Sign in from another device”**

It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.

On your USSS blue line connected or USSS VPN connected PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step **(This is not case sensitive)**.

On your USSS blue line connected or USSS VPN connected PC, select your **@secretservice.gov** account. If your account is not listed and it asks for you to type it in, use your Teams address **(usually [redacted]@secretservice.gov)**

On your USSS blue line connected or USSS VPN connected PC, select “Sign in as current user”



Enrollment Continued...

On your USSS blue line connected or USSS VPN connected PC, once successful, you will see the below message and will be done with the PC.




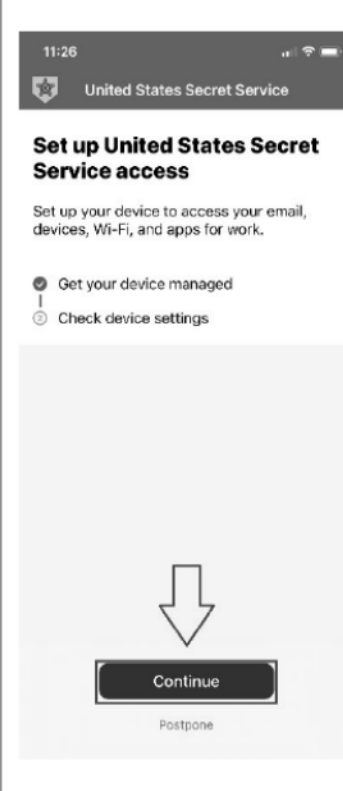
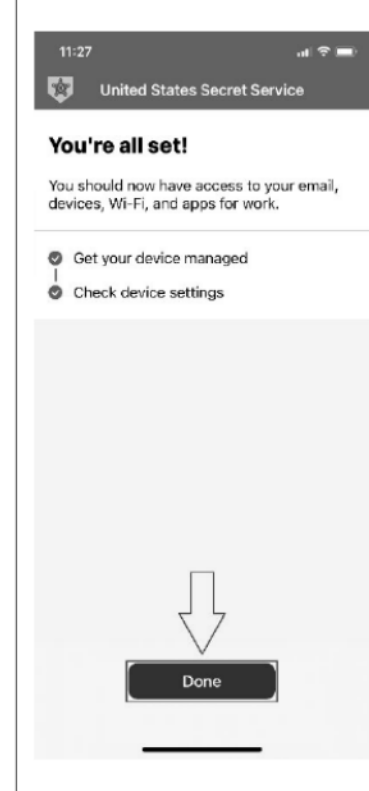
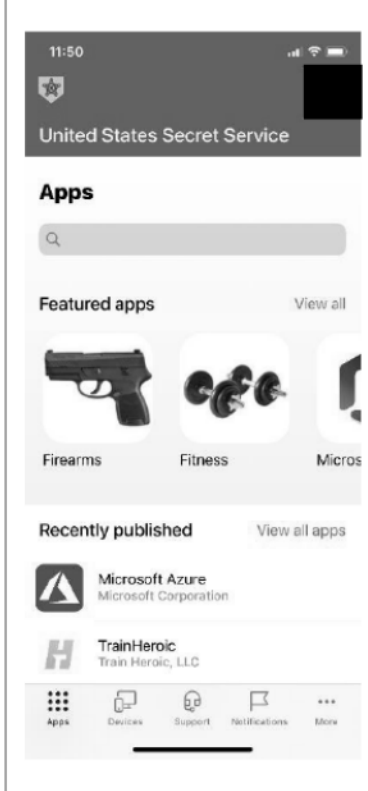
The iPhone will then display the below while moving on to the next steps.

At this step, select “Begin” and wait.

Select “Continue”

Select “Done”

You will then see something like the below.

					
--	---	--	--	--	--

Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 28 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

*Do **NOT** start the enrollment process **WITHOUT** being in front of a USSS blue line connected or USSS VPN connected PC. If you do, you will not be able to enroll your device. The only way to complete an enrollment, is if you are at a PC described above. There is **NOTHING** the OCIO can do to enroll your iPhone/iPad, if you are not in at a PC described above.*

*At **NO** point does the instructions below describe entering credentials on the iPhone/iPad, during the enrollment process. If you enter credentials on the phone iPhone/iPad during your enrollment, you are doing it wrong and your enrollment will fail.*

Backup

Backup content (if needed). A guide for preserving content can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up and are at a **USSS blue line connected or USSS VPN connected PC to complete the enrollment process**, wipe your device to enroll in Intune. Go to “Settings->General->Reset->Erase All Content and Settings”

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, immediately followed by an error message regarding “Guided Access” – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select **“Sign in”**

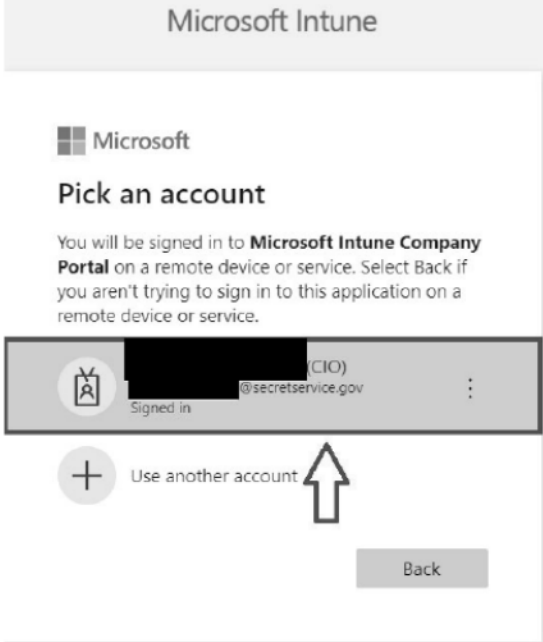
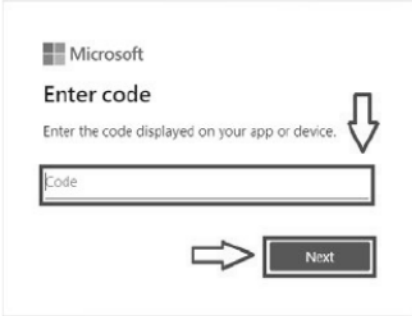
On the iPhone/iPad you are enrolling, **Select “Sign in from another device”**

It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.

On your USSS blue line connected or USSS VPN connected PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step **(This is not case sensitive)**.

On your USSS blue line connected or USSS VPN connected PC, select your **@secretservice.gov** account. If your account is not listed and it asks for you to type it in, use your Teams address **(usually [redacted]@secretservice.gov)**

On your USSS blue line connected or USSS VPN connected PC, select “Sign in as current user”



Enrollment Continued...

On your USSS blue line connected or USSS VPN connected PC, once successful, you will see the below message and will be done with the PC.

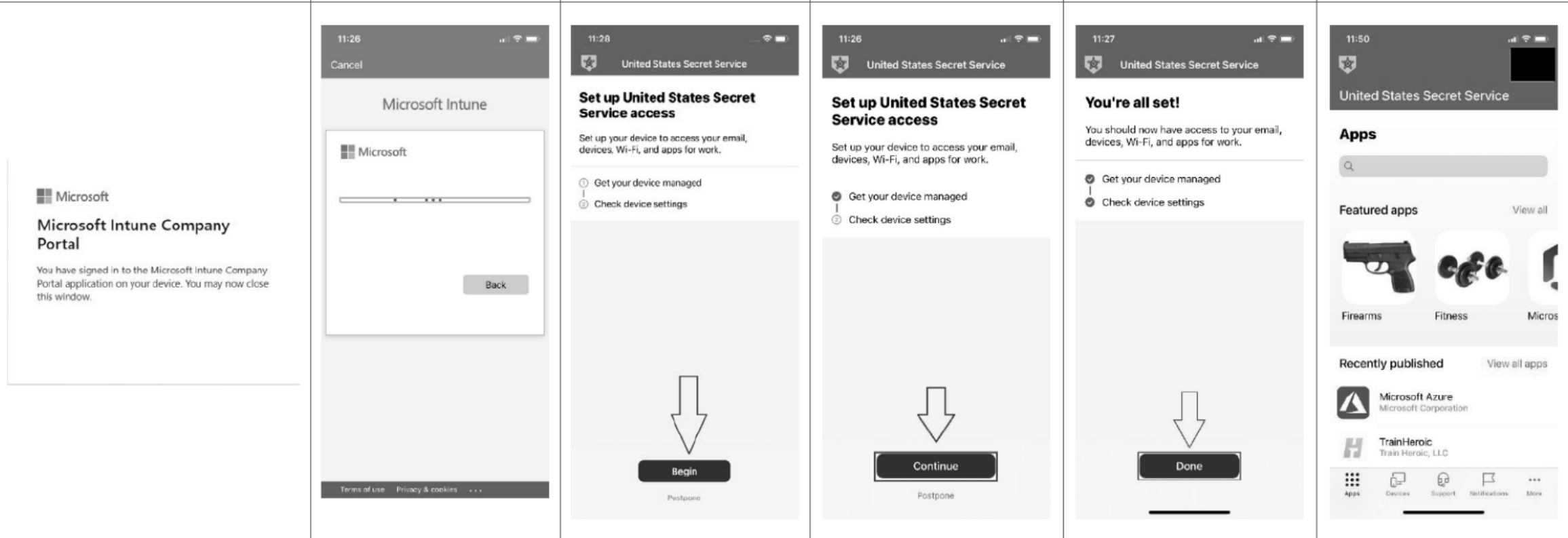
The iPhone will then display the below while moving on to the next steps.

At this step, select “Begin” and wait.

Select “Continue”

Select “Done”

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 28 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

*Do **NOT** start the enrollment process **WITHOUT** being in front of a USSS blue line connected or USSS VPN connected PC. If you do, you will not be able to enroll your device. The only way to complete an enrollment, is if you are at a PC described above. Unfortunately there is **NOTHING** the OCIO can do to enroll your iPhone/iPad, if you are not at a PC described above.*

*At **NO** point does the instructions below describe entering credentials on the iPhone/iPad, during the enrollment process. If you enter credentials on the iPhone/iPad during your enrollment, you are doing it wrong and your enrollment will fail.*

Backup

Backup content (if needed). A guide for preserving content can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up **and are at a USSS blue line connected or USSS VPN connected PC to complete the enrollment process**, wipe your device to enroll in Intune. Go to “Settings->General->Reset->Erase All Content and Settings”

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, immediately followed by an error message regarding “Guided Access” – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select **“Sign in”**

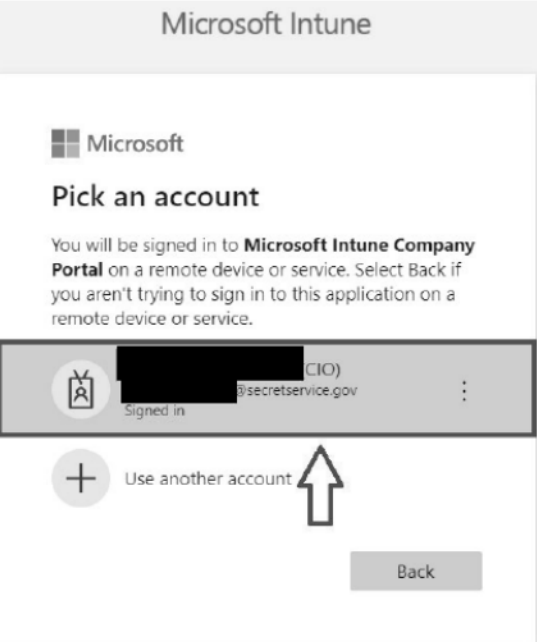
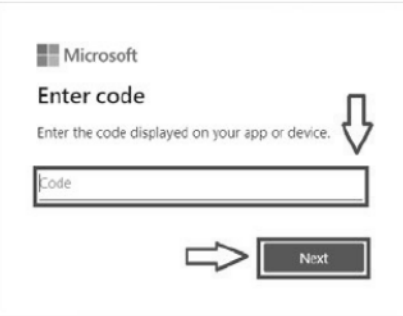
On the iPhone/iPad you are enrolling, **“Sign in from another device”**

It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.

On your USSS blue line connected or USSS VPN connected PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step **(This is not case sensitive)**.

On your USSS blue line connected or USSS VPN connected PC, select your **@secretservice.gov** account. If your account is not listed and it asks for you to type it in, use your Teams address **(usually [redacted]@secretservice.gov)**

On your USSS blue line connected or USSS VPN connected PC, select **“Sign in as current user”**





Enrollment Continued...

On your USSS blue line connected or USSS VPN connected PC, once successful, you will see the below message and will be done with the PC.

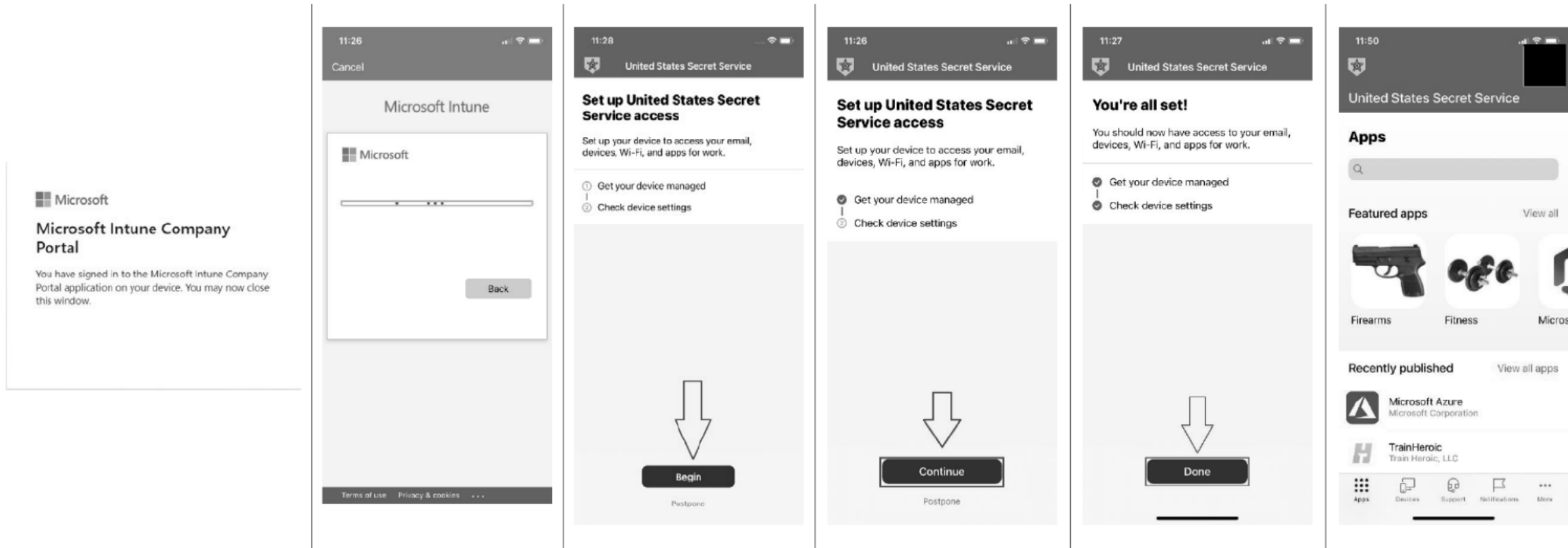
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.

- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Apr 13 2021 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check Messages](#)

[Check Contacts](#)

[Check Notes](#)

[Check Files](#)

[Check Voice Memos](#)

[FAQ](#)

USSS Preserve Content Guide for iPhone & iPad


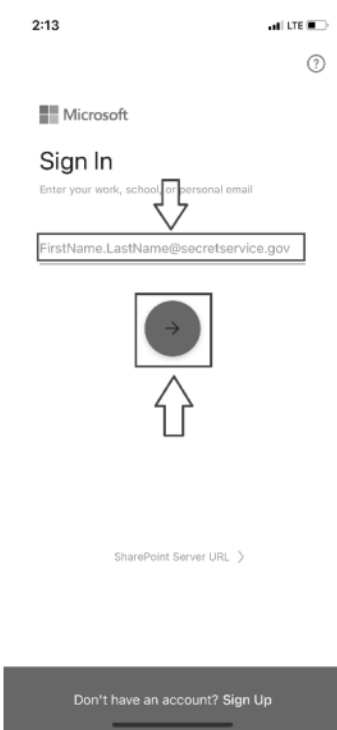


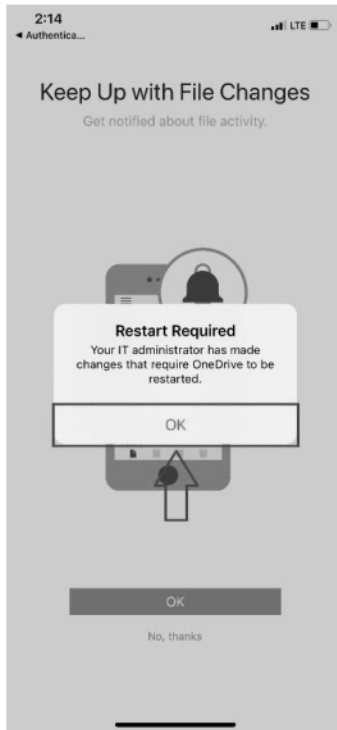
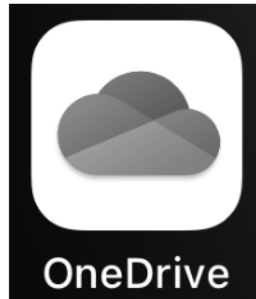

[Table of Contents](#)

Rev. Apr 13 2021 RLT

Check Photos

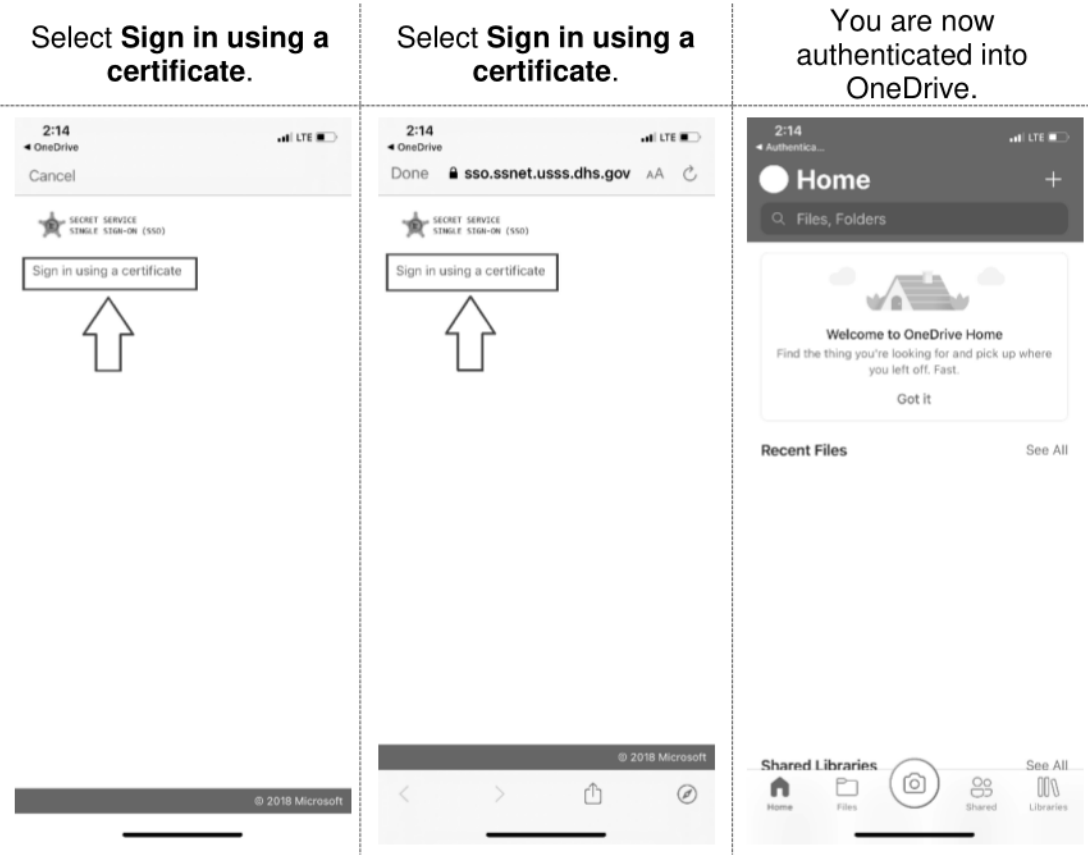
Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to Teams via your mobile device. If you have, continue to these steps [here](#).

Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

Never O365 Authenticated Continued....

USSS Preserve Content Guide for iPhone & iPad


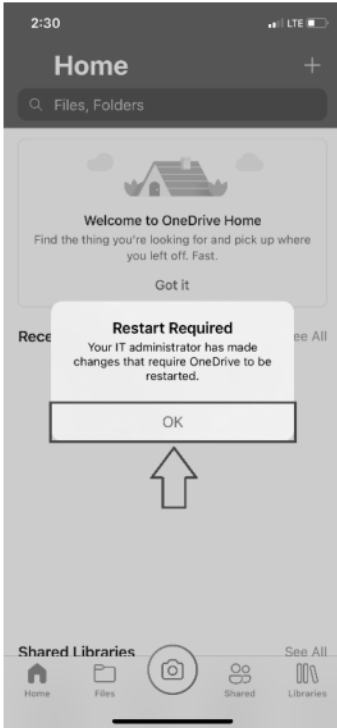




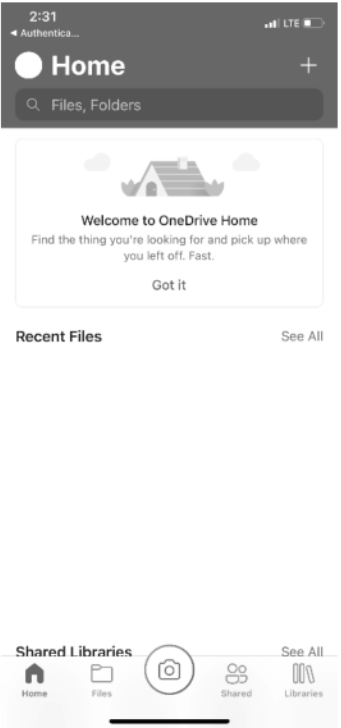


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

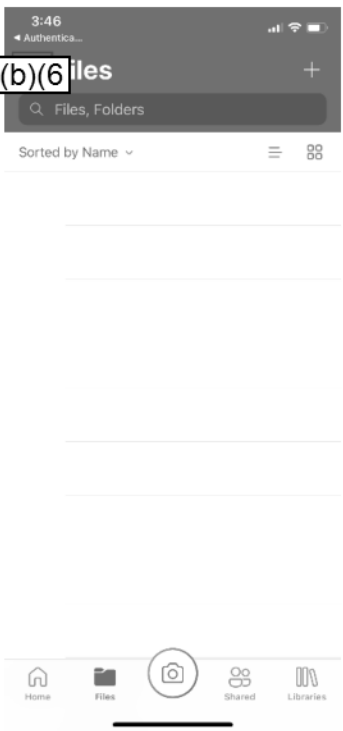
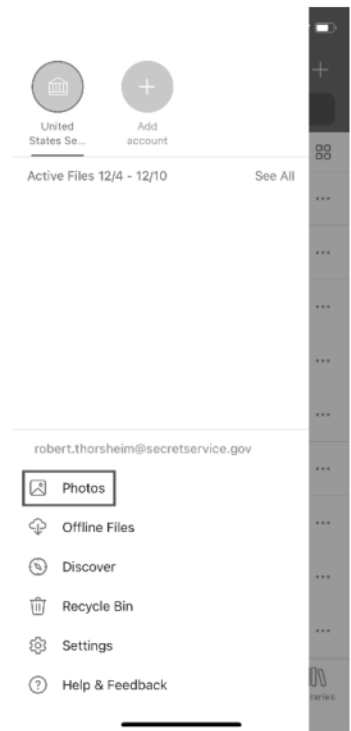

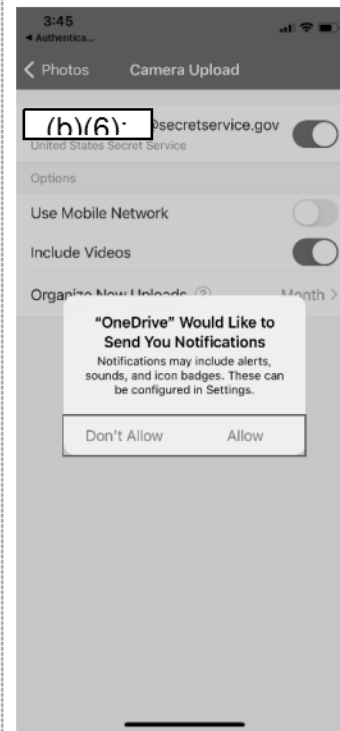
Rev. Apr 13 2021 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to Teams via your mobile device.*

Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#). **Note: it is best to be connected to Wi-Fi to perform these transfers.***

<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

USSS Preserve Content Guide for iPhone & iPad

Selected items: **Note: it is best to be connected to Wi-Fi to perform these transfers.**

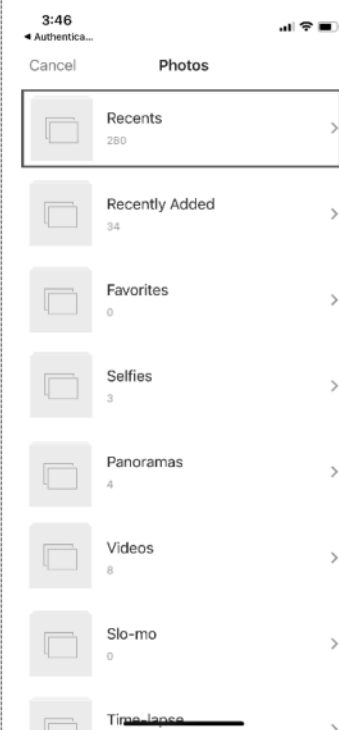
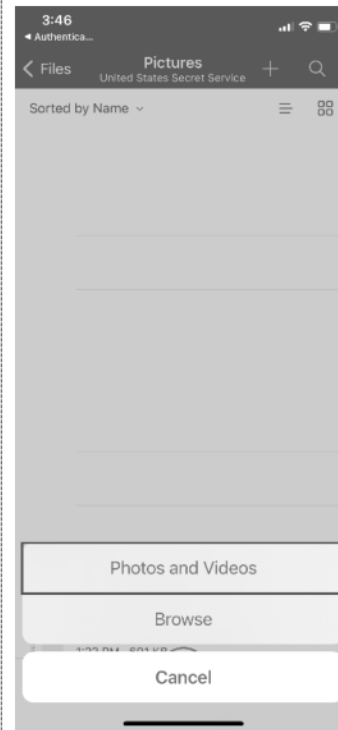
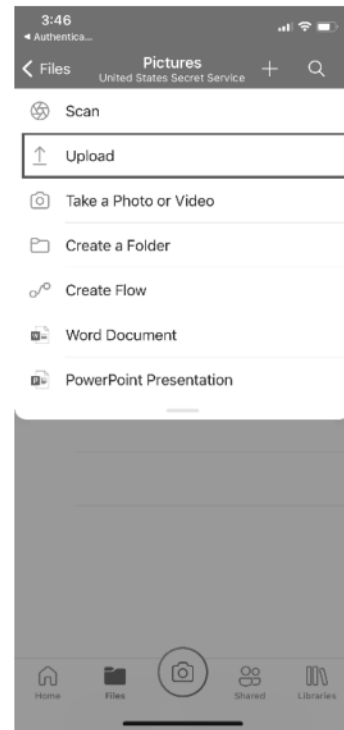
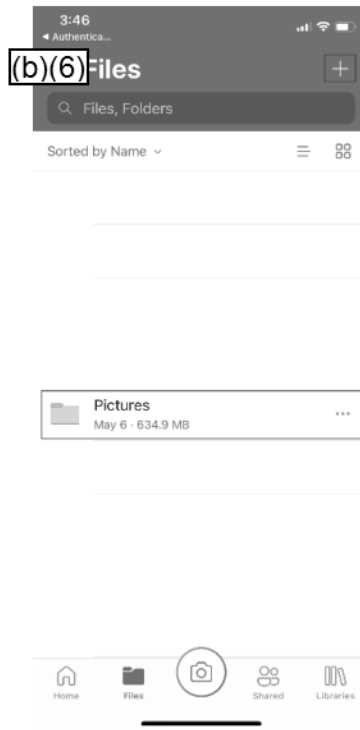
From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

Select **Upload**.

Select **Photos and Videos**.

Select **Recents**.

Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Apr 13 2021 RLT

Check Messages

Verify if you have any Messages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

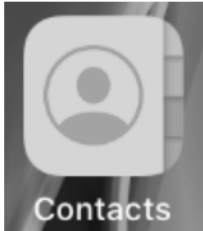
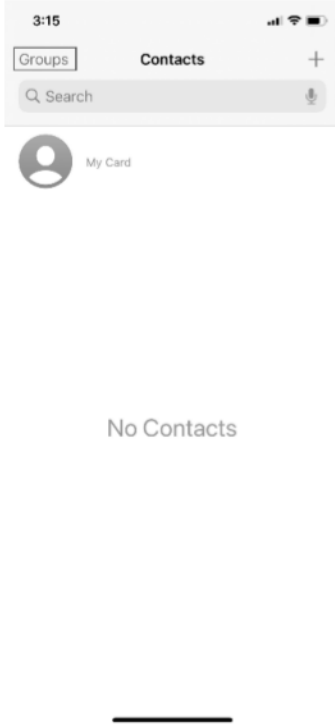
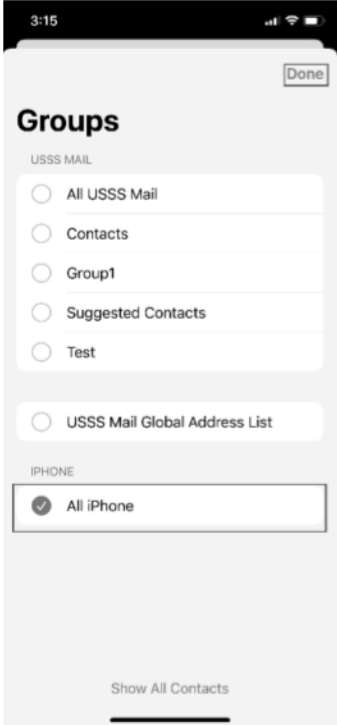
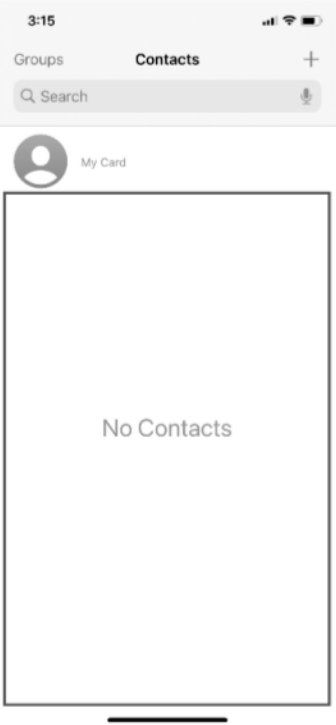
iMessage Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

Check Contacts

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure <i>only</i> All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be preserved. If so, <i>add them to your contacts within Outlook from your PC.</i>
			
			<p>If you followed the step correctly for making sure <i>only</i> All iPhone was selected, then you will see contacts that are saved locally to your device. If you don't see any contacts, that means all of your contacts are already getting saved to Outlook.</p>

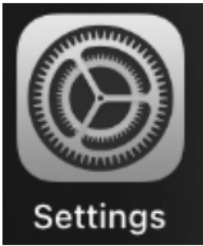
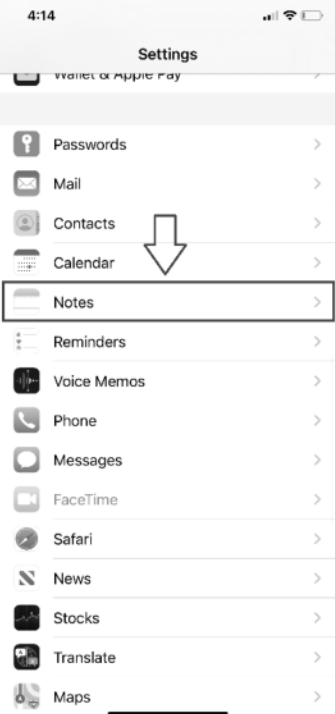
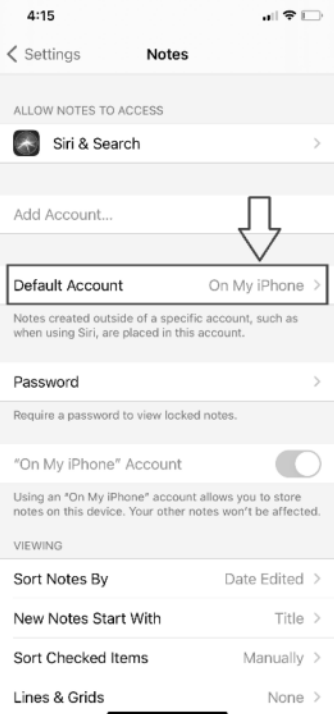
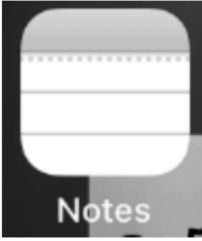

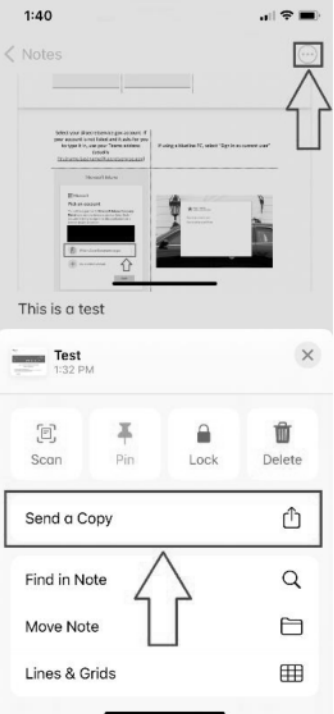
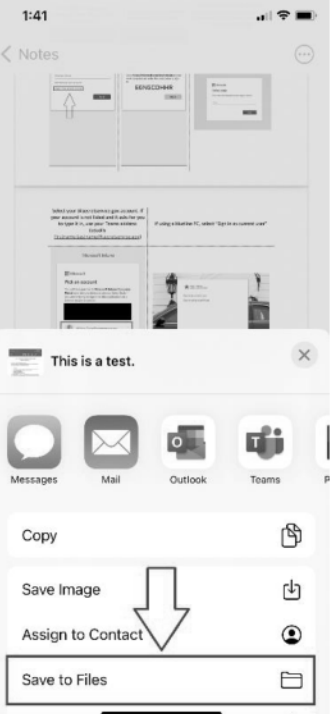
USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Apr 13 2021 RLT

Check Notes

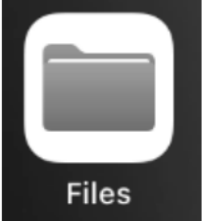
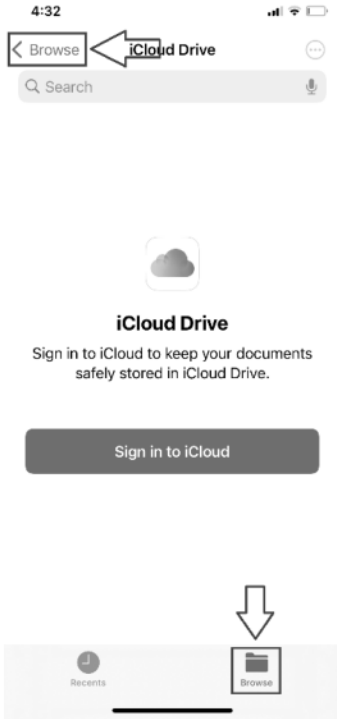
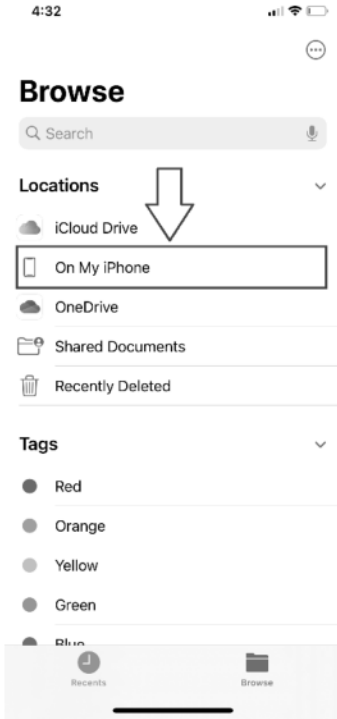

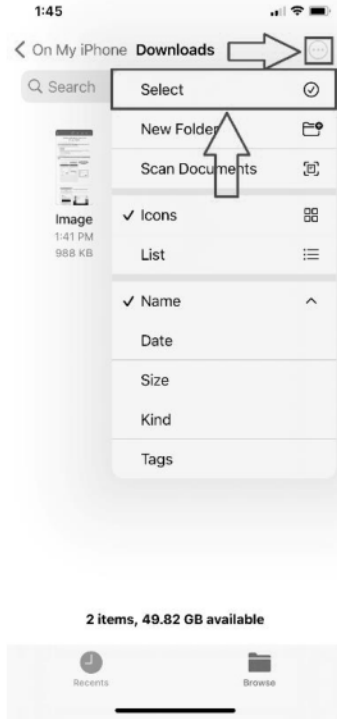

Follow the steps below to determine if you have any notes saved locally on your mobile device.

<p>Open Settings.</p>	<p>Select Notes.</p>	<p>Change Default Account to On My iPhone.</p>	<p>Open Notes.</p>	<p>Determine if there are any Notes saved On My iPhone that need saved within Notes.</p>	<p>Open the Note that you want to preserve. Select Options in upper right hand corner. Select Send a Copy</p>	<p>Select Save to Files. Continue to Check Files steps here.</p>
						

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.	Selection Options in upper right hand corner. Select Select .	Select the files that you want to preserve. Select Share in the lower left hand corner.
					

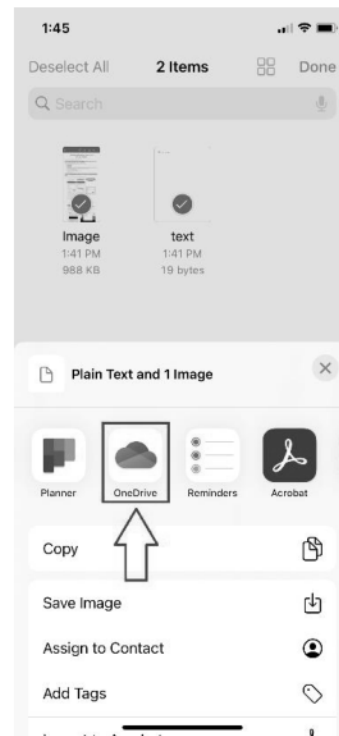
USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

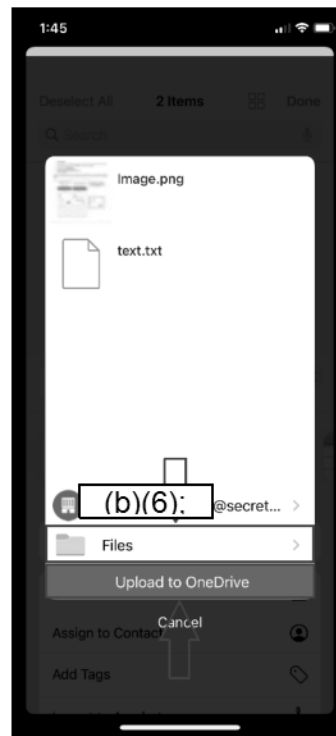
Rev. Apr 13 2021 RLT

Check Files Continued....

Select **OneDrive**.



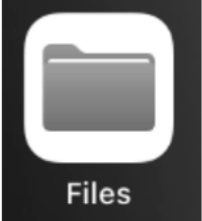
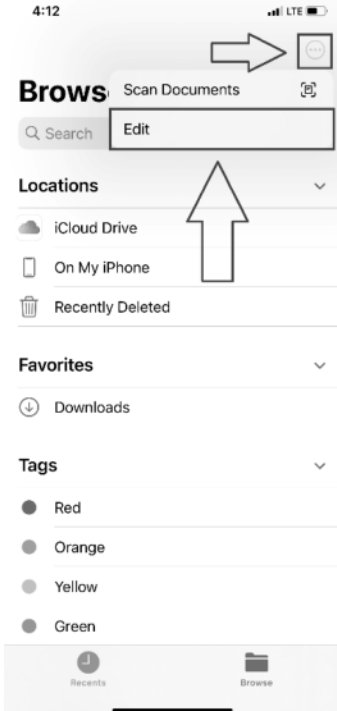
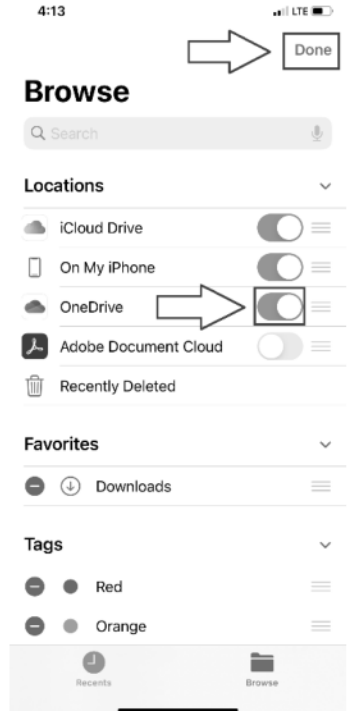

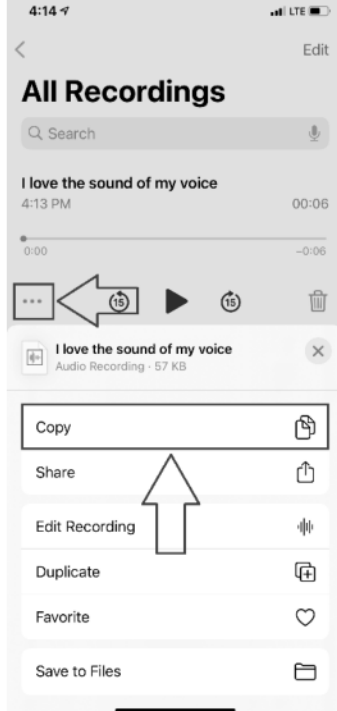
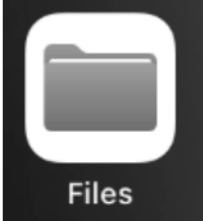
Choose the folder that you want your files to be saved in. Select **Upload to OneDrive**.



USSS Preserve Content Guide for iPhone & iPad

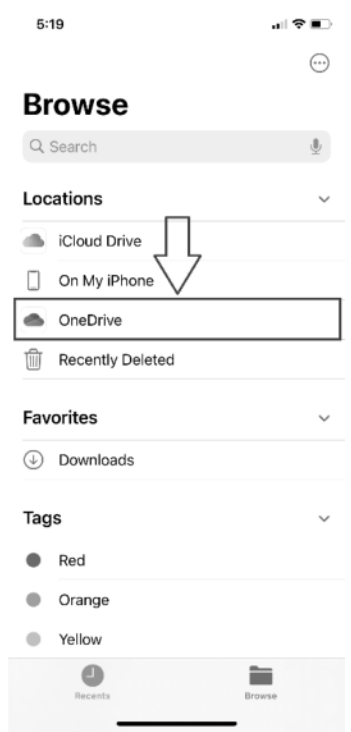
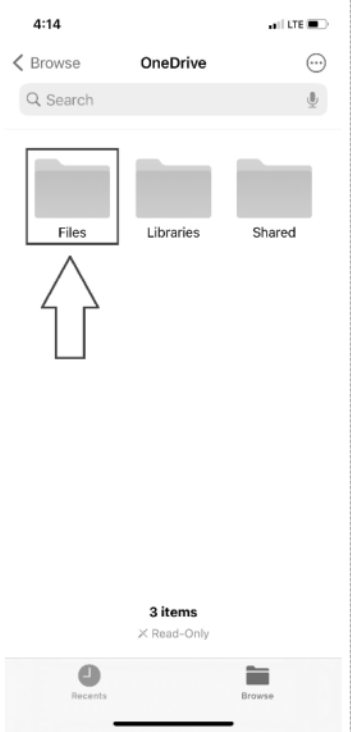
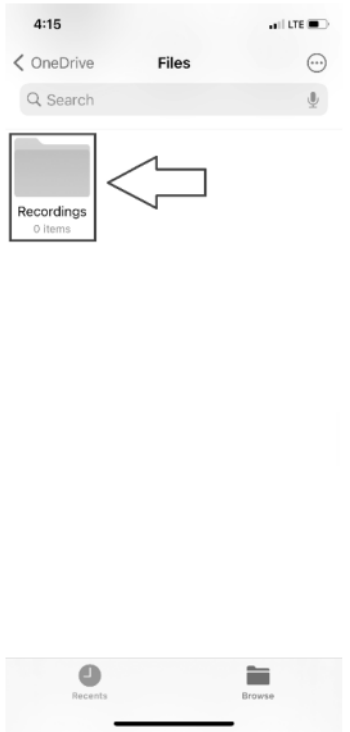
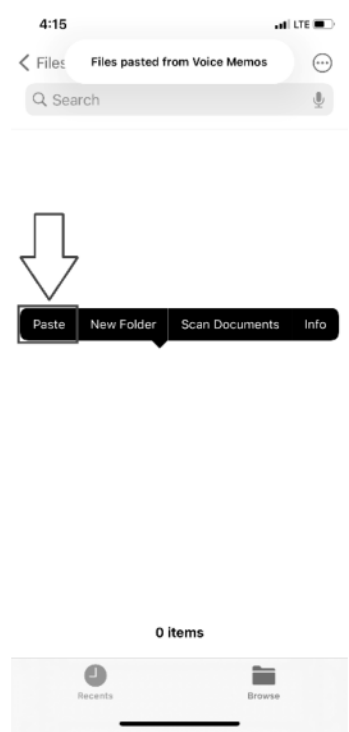
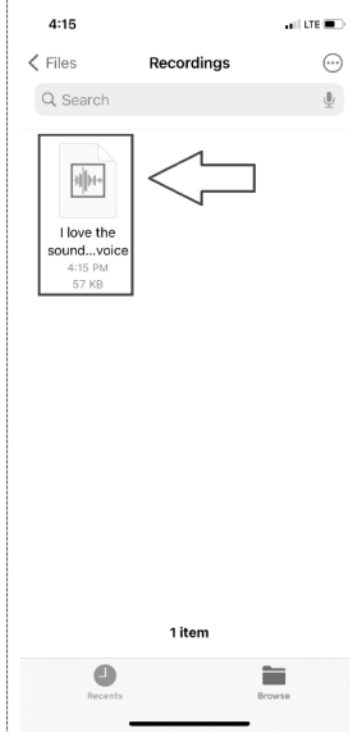
Check Voice Memos

Follow the steps below to determine if you have any files saved locally on your mobile device.

<p>Once you have authenticated to OneDrive, open Files.</p>	<p>Select Options (3 dots) in upper right. Select Edit.</p>	<p>Toggle On OneDrive. Select Done.</p>	<p>Select Voice Memos.</p>	<p>Selection Options (3 dots) in lower left of recorded voice memo. Select Copy.</p>	<p>Open Files.</p>
					

USSS Preserve Content Guide for iPhone & iPad

Check Voice Memos Continued....

<p>Select OneDrive.</p>	<p>Select Files.</p>	<p>Choose the folder that you want your files to be saved in. Or create a new folder to save your Voice Memos.</p>	<p>Press and hold in empty area of screen. Select Paste.</p>	<p>You can see that your Voice Memo is now in OneDrive. You can view this in the OneDrive app on your phone or find the file within OneDrive from your PC.</p>
				

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Apr 13 2021 RLT

FAQ

Please see below for Frequently Asked Questions that have been received regarding preserving content.

Can I backup my Photos?

Yes. Please follow the steps described [here](#).

Can I backup my Messages?

No. You can take screenshots of your messages and backup those screenshots. Please follow the steps described [here](#).

Can I backup my iMessage Groups?

No. You can document your iMessage Groups and recreate them. Please follow the steps described [here](#).

Can I backup my Contacts?

Yes, contacts sync automatically to your Outlook account. If your contacts are saved locally, you will have to follow steps described [here](#).

Can I backup my Notes?

Yes, notes sync automatically to your Outlook account. If your notes are saved locally, you will have to follow steps described [here](#).

Can I backup my Files?

Yes. Please follow the steps described [here](#).

Can I backup my Voice Memos?

Yes. Please follow the steps described [here](#).

Can I backup my documents in Adobe Reader?

Yes. They can be backed-up from the Files app. Steps for backing up documents from the Files app can be found [here](#).

Can I backup my files in iTAK?

Yes. They can be backed-up from the Files app. Steps for backing up documents from the Files app can be found [here](#).

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Apr 13 2021 RLT

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check iMessages](#)

[Check Contacts](#)

[Check Notes](#)


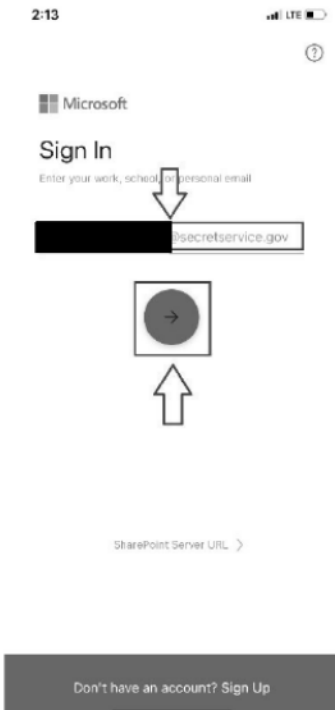



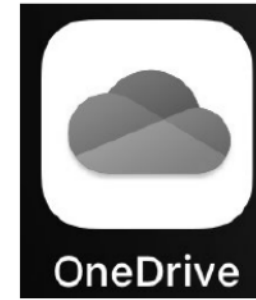
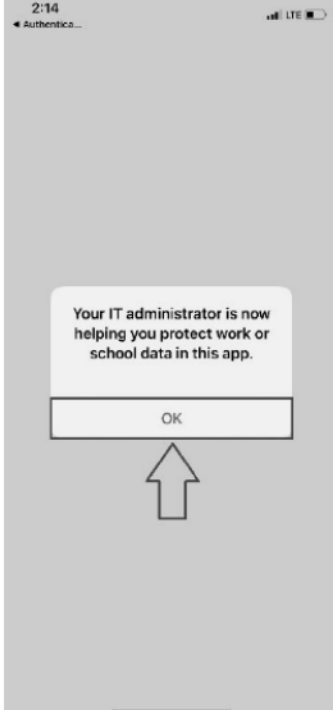
[Check Files](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to O365 via your mobile device (e.g. Teams). If you have, continue to these steps [here](#).

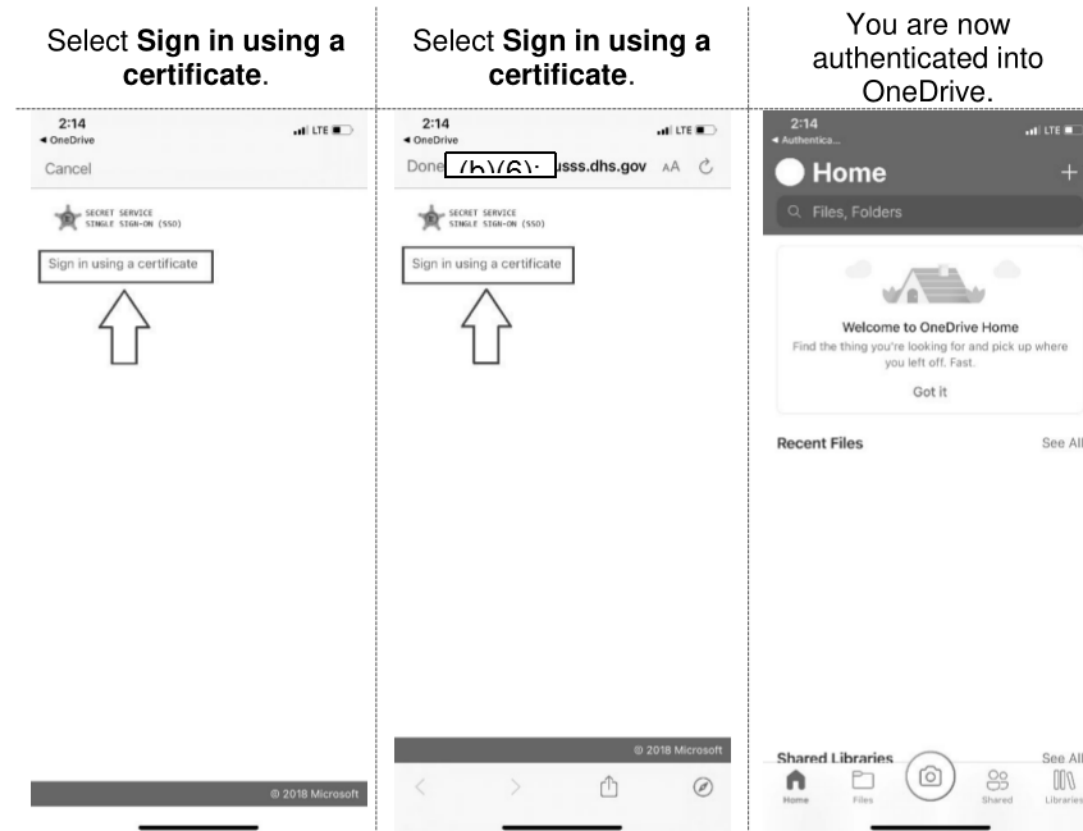
Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Never O365 Authenticated Continued....


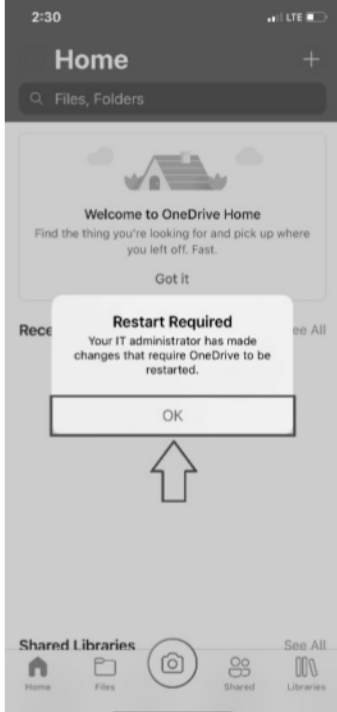
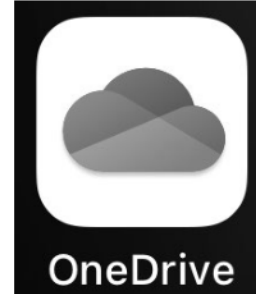



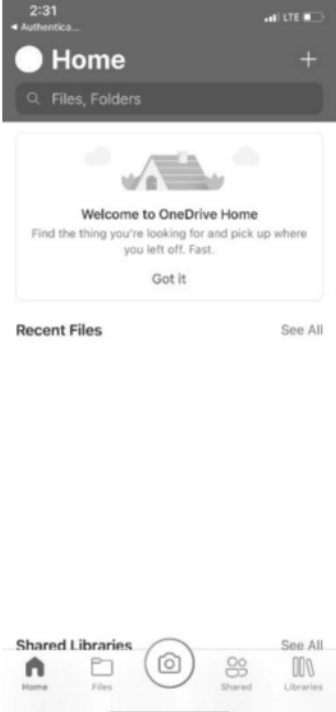


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to O365 via your mobile device (e.g. Teams).*

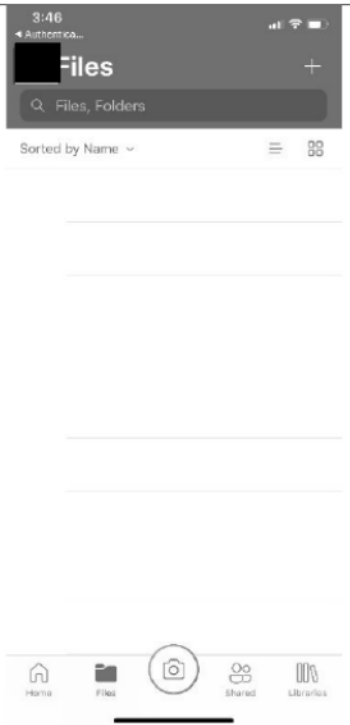

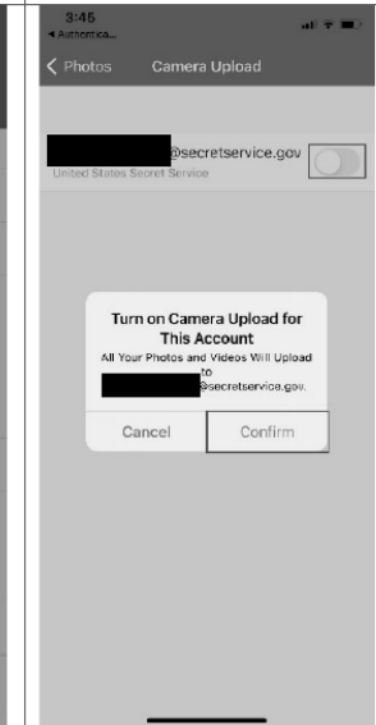
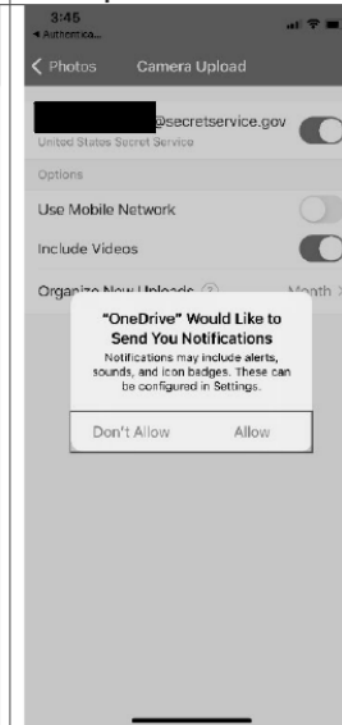
Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#).*

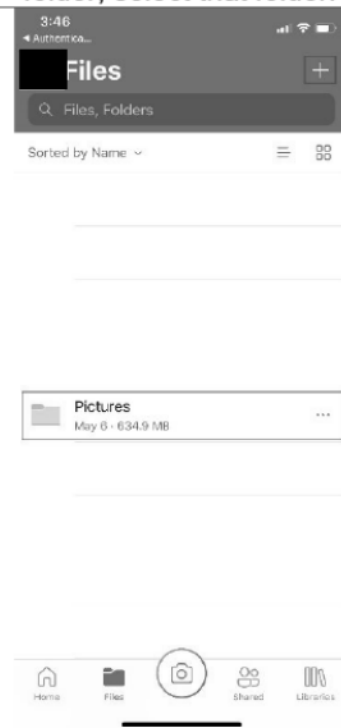
<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

USSS Preserve Content Guide for iPhone & iPad

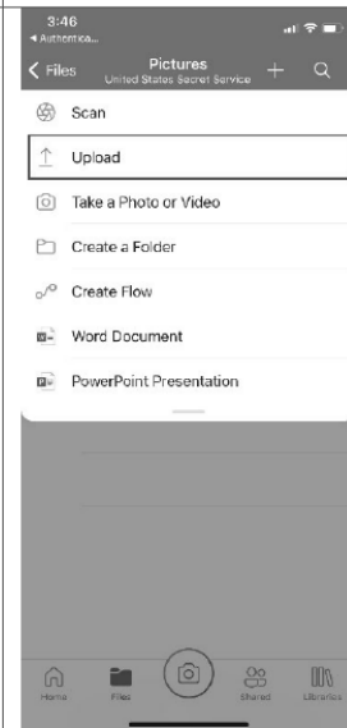
Selected items

From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

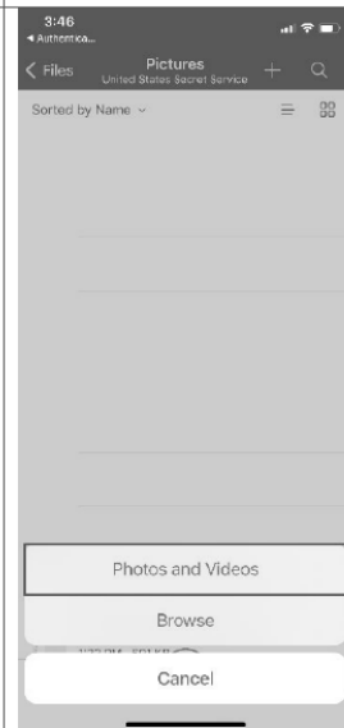
Select **Upload**.



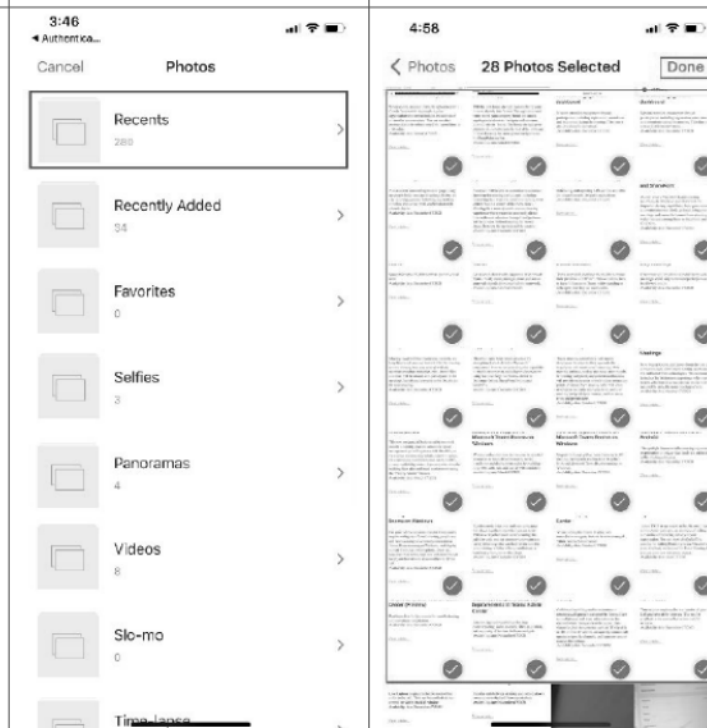
Select **Photos and Videos**.



Select **Recents**.



Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Check iMessages

Verify if you have any iMessages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

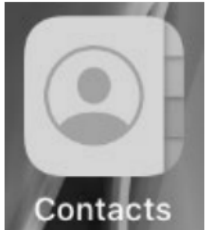
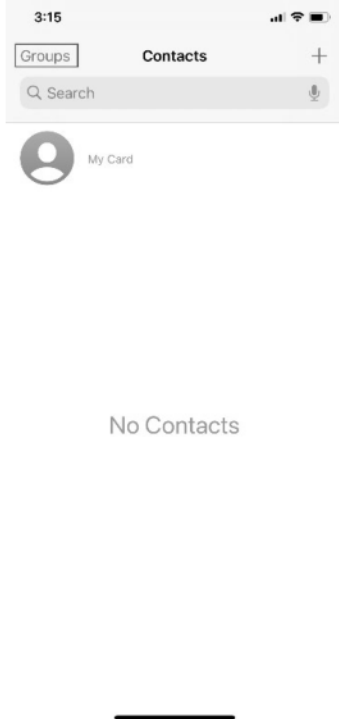
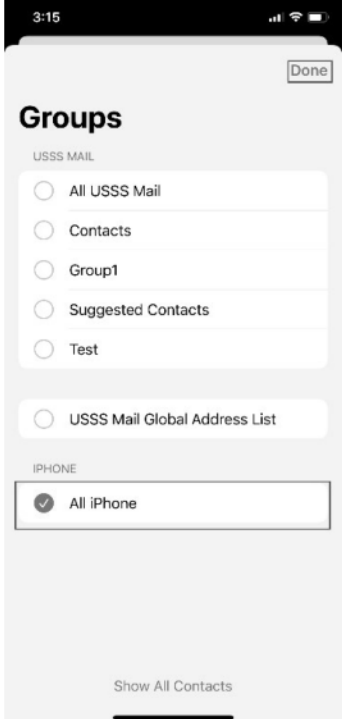
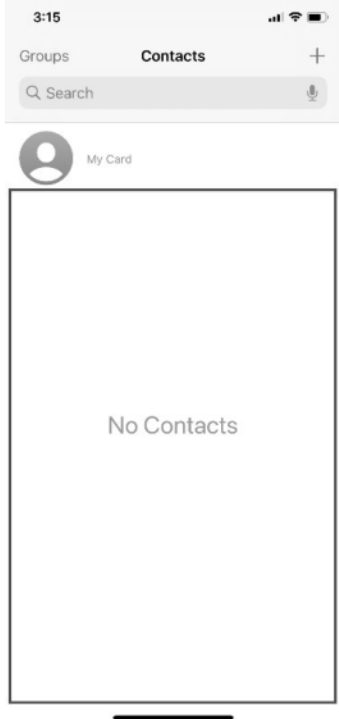
iMessages Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#).

USSS Preserve Content Guide for iPhone & iPad

Check Contacts

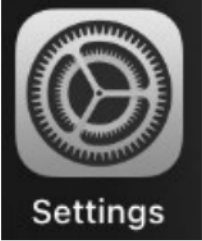
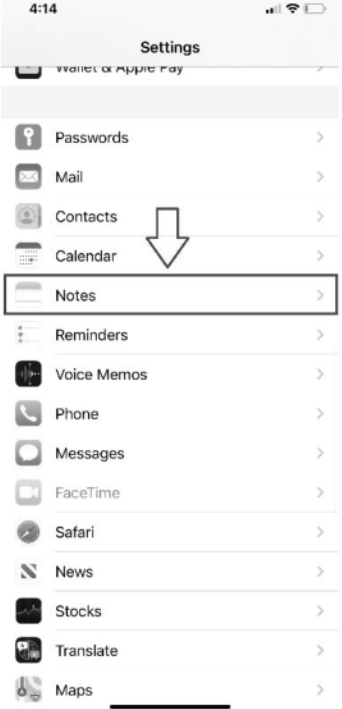

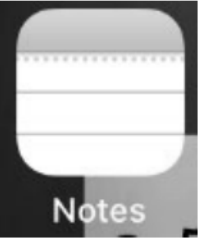

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure just All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be added to your contacts within Outlook.
			

USSS Preserve Content Guide for iPhone & iPad

Check Notes

Follow the steps below to determine if you have any notes saved locally on your mobile device.

Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Outlook.
				

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

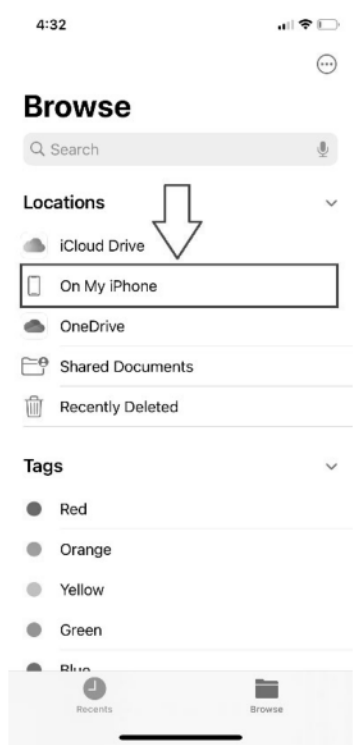
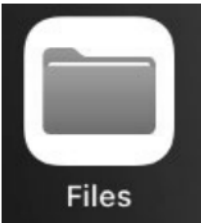
Open **Files**.

Select **Browse** in the lower right. Select **Browse** in the upper left.

Select **On My iPhone**.

Check Files and Folders, to see if you have any content that need preserved.

USSS Preserve Content Guide for iPhone & iPad



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check iMessages](#)

[Check Contacts](#)

[Check Notes](#)


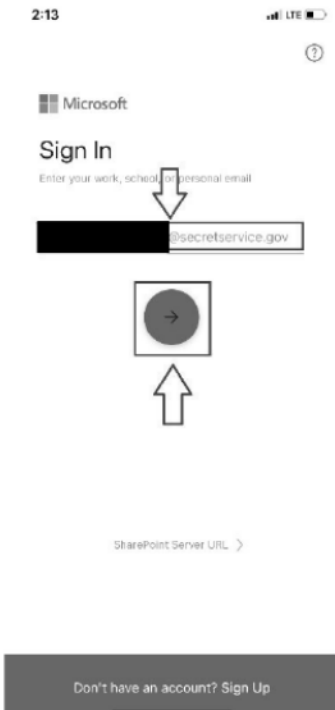


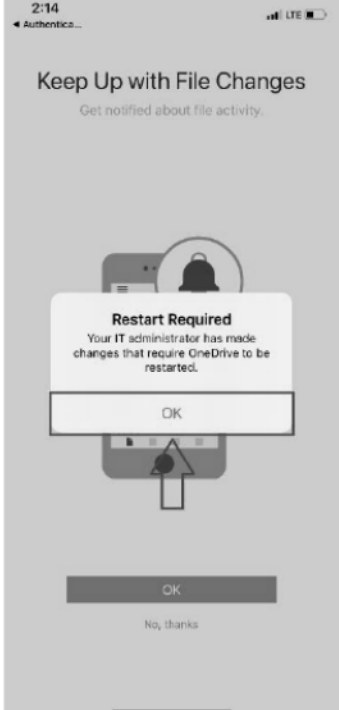
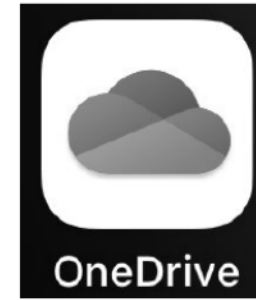
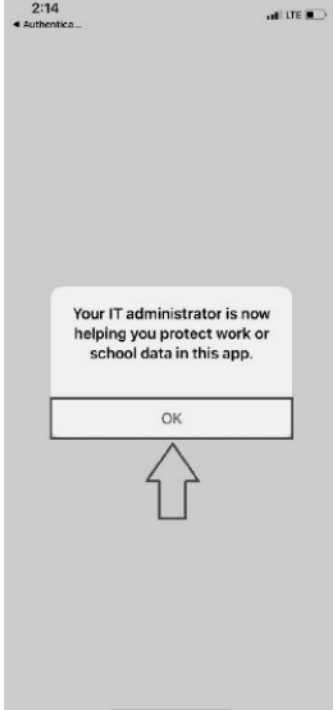
[Check Files](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to O365 via your mobile device (e.g. Teams). If you have, continue to these steps [here](#).

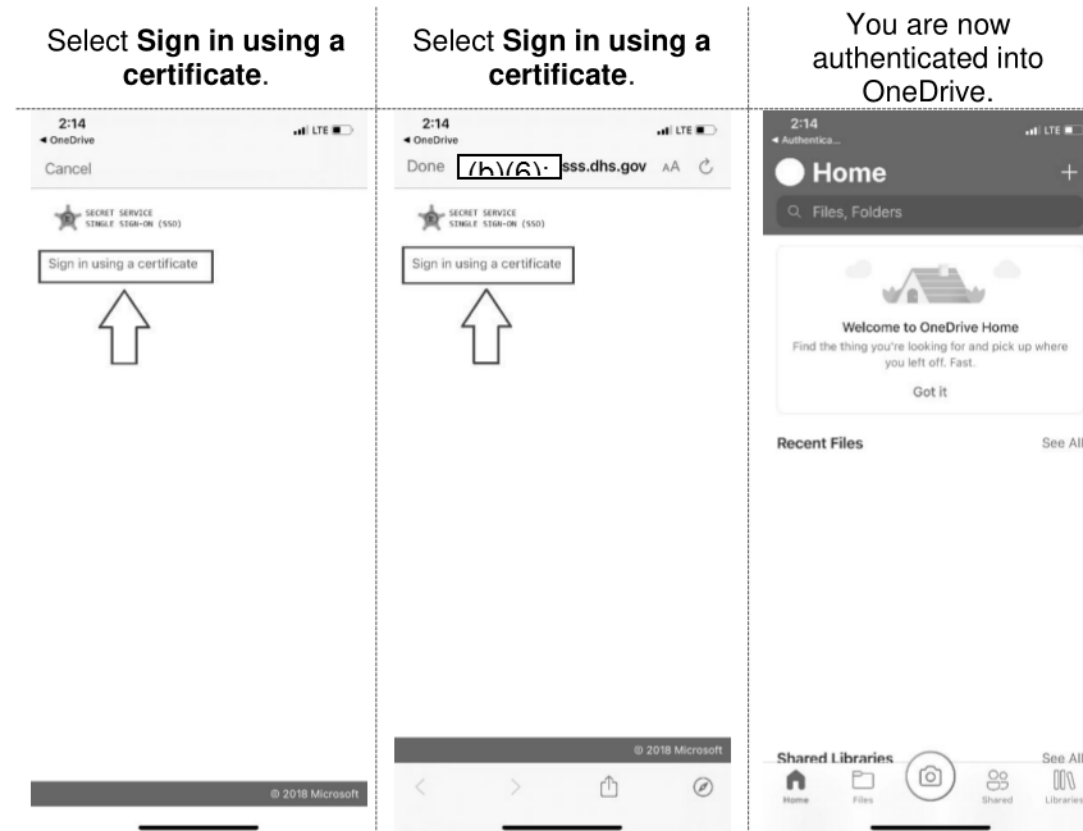
Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Never O365 Authenticated Continued....


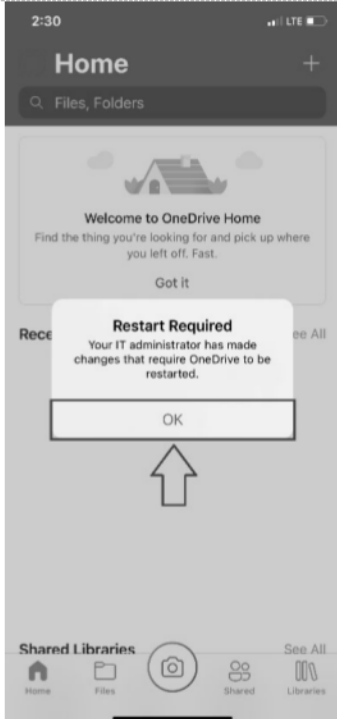




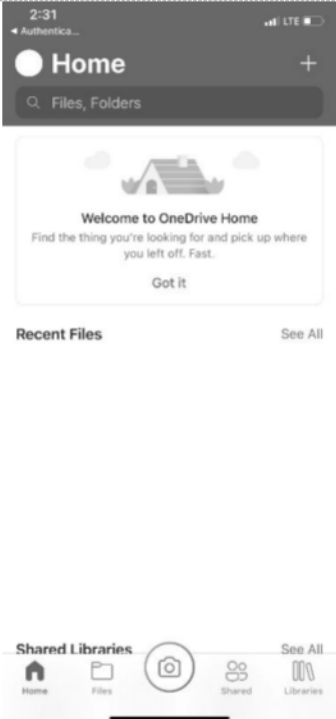


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

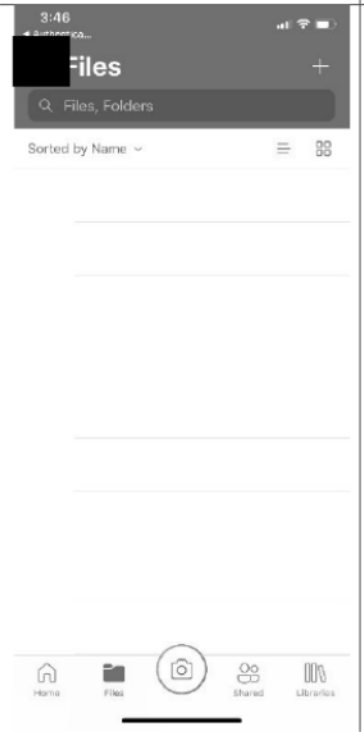

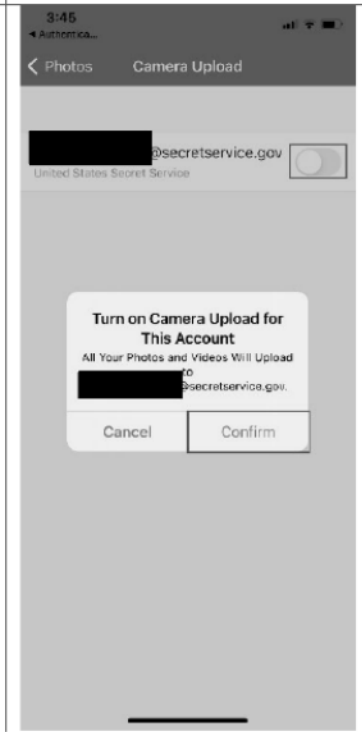
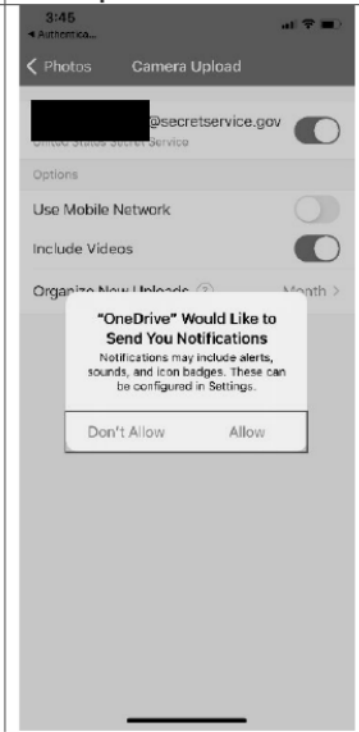
Rev. Jan 15 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to O365 via your mobile device (e.g. Teams).*

Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#).*

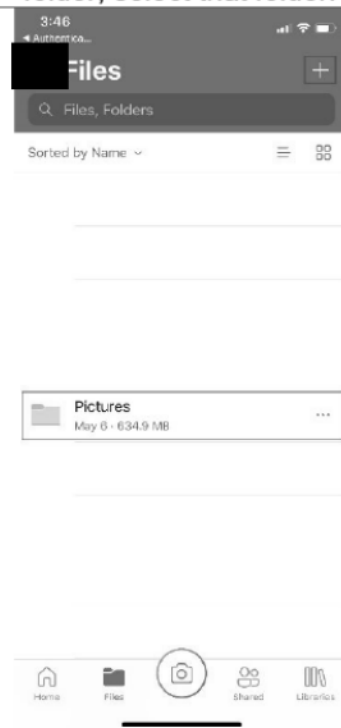
<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

USSS Preserve Content Guide for iPhone & iPad

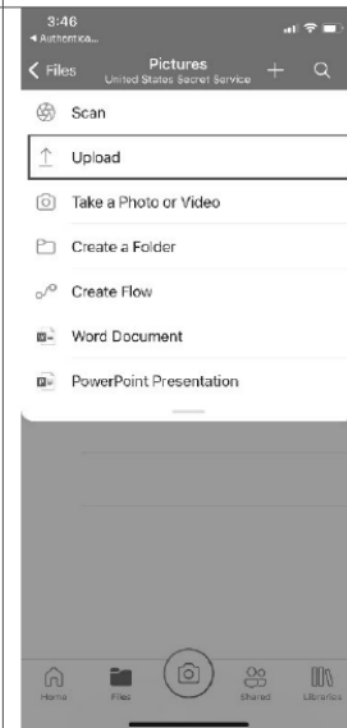
Selected items

From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

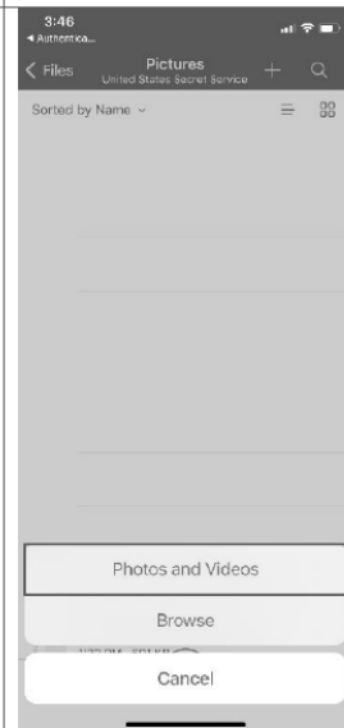
Select **Upload**.



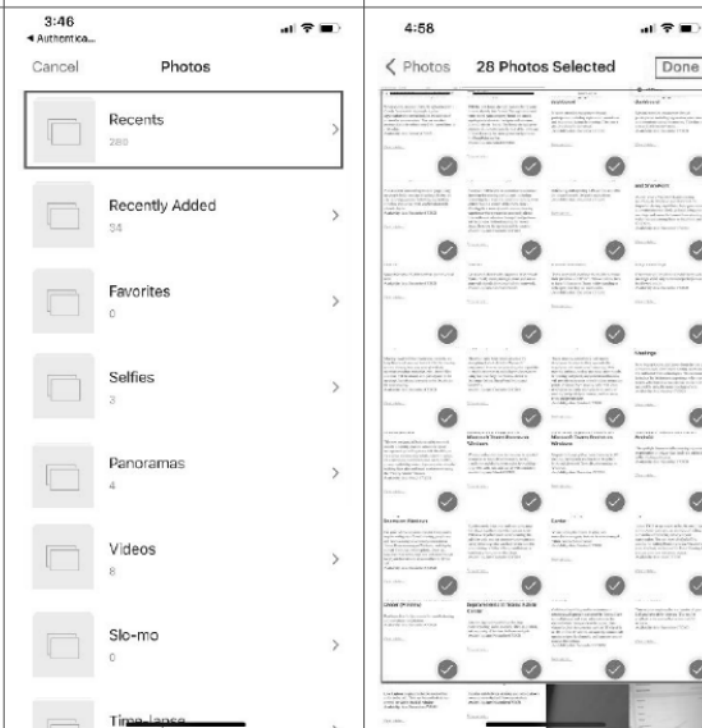
Select **Photos and Videos**.



Select **Recents**.



Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

Check iMessages

Verify if you have any iMessages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

iMessages Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Check Contacts

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open **Contacts**.

Open **Groups**.

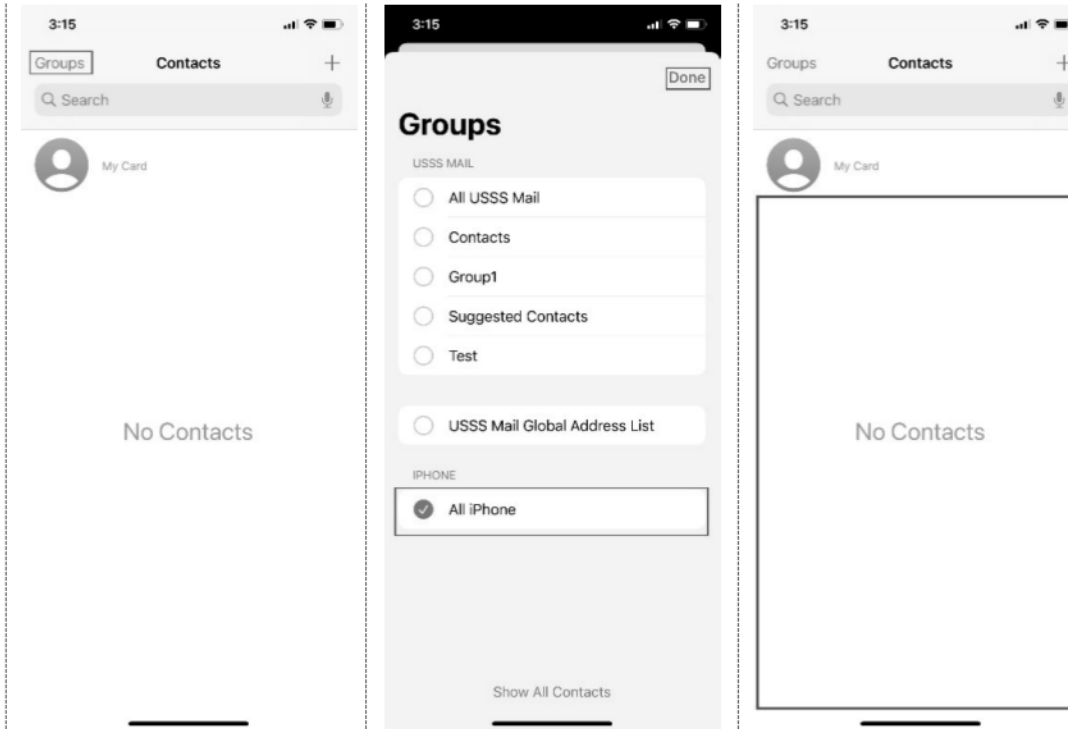
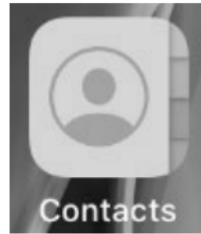
Make sure just **All iPhone** is selected. Select **Done**.

Review contacts to determine if any of them need to be added to your contacts within Outlook.

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

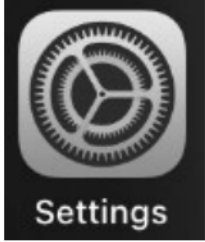
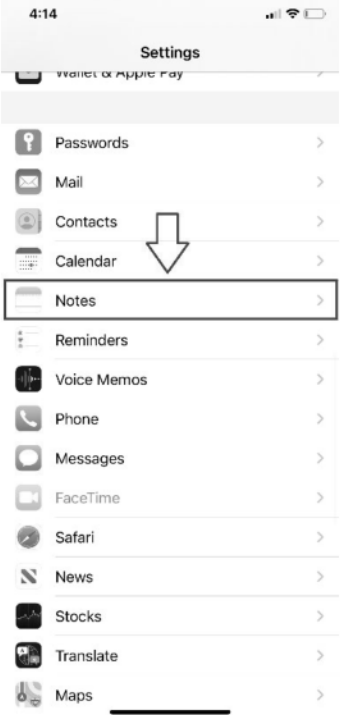



Rev. Jan 15 2020 RLT



Check Notes

Follow the steps below to determine if you have any notes saved locally on your mobile device.

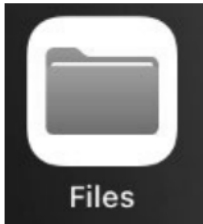

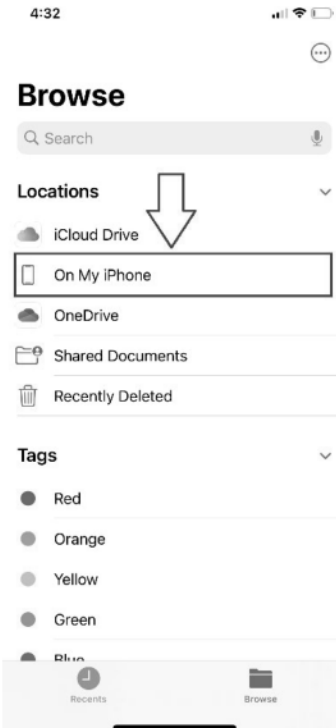

USSS Preserve Content Guide for iPhone & iPad

Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Outlook.
	 <p>A screenshot of the iPhone Settings app. The 'Notes' option is highlighted with a white box and a downward-pointing arrow.</p>	 <p>A screenshot of the iPhone Notes settings. The 'Default Account' is set to 'On My iPhone', which is highlighted with a white box and a downward-pointing arrow.</p>		 <p>A screenshot of the iPhone Notes app showing the 'Folders' view. The 'On My iPhone' folder is highlighted with a white box and a downward-pointing arrow.</p>

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.
			

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check iMessages](#)

[Check Contacts](#)

[Check Notes](#)


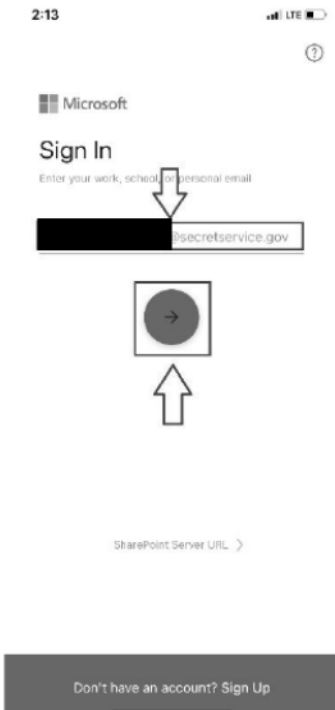
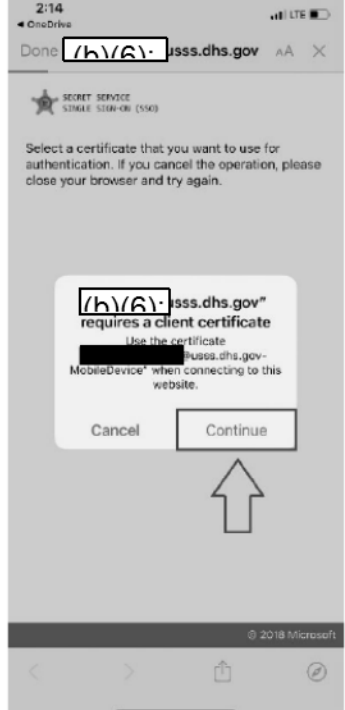

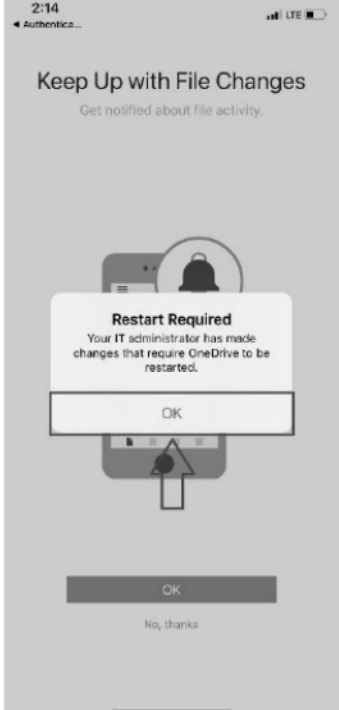
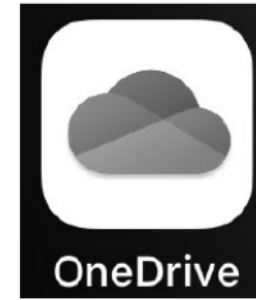
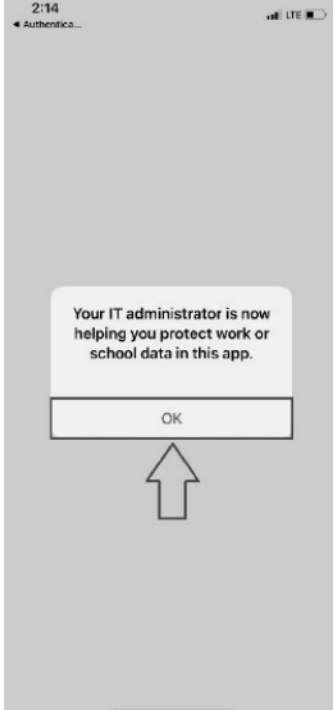
[Check Files](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to O365 via your mobile device (e.g. Teams). If you have, continue to these steps [here](#).

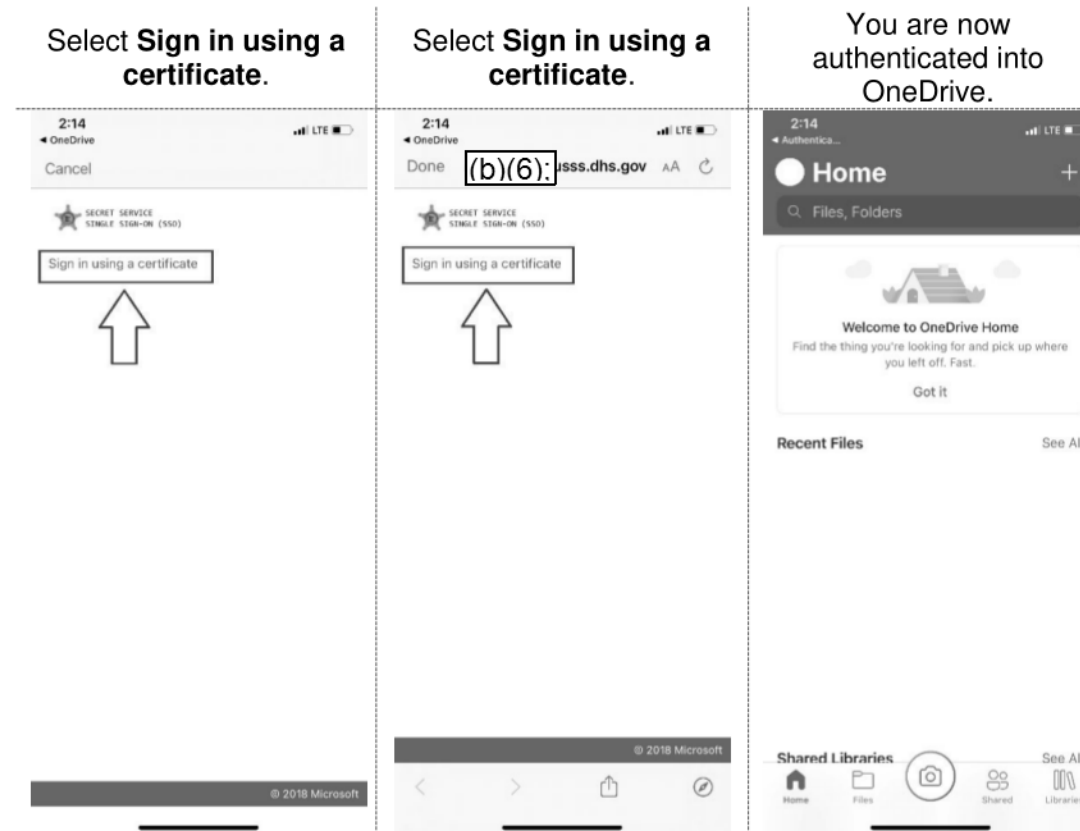
Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Never O365 Authenticated Continued....


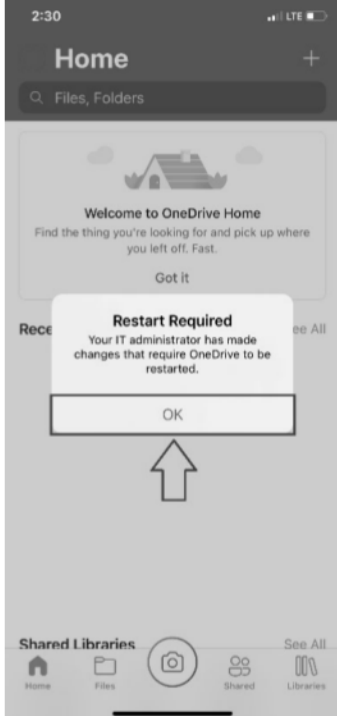

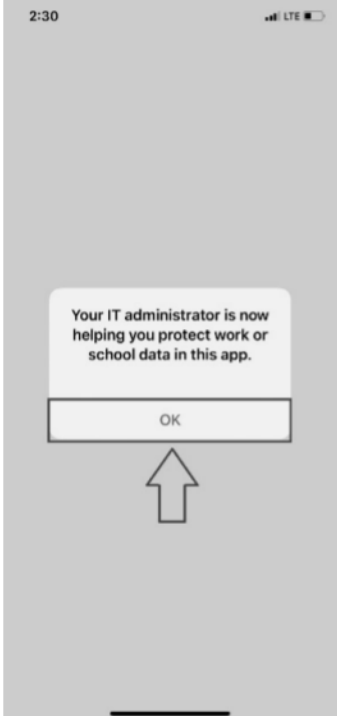

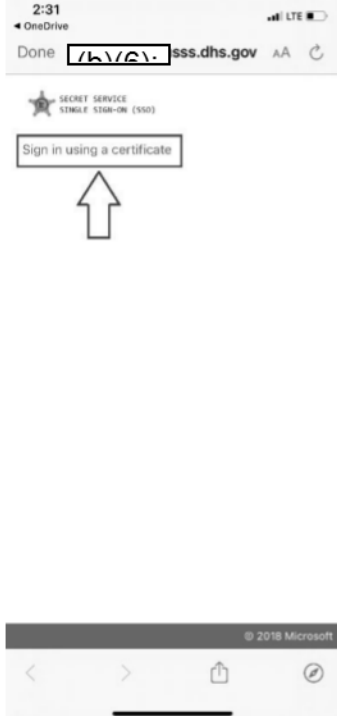
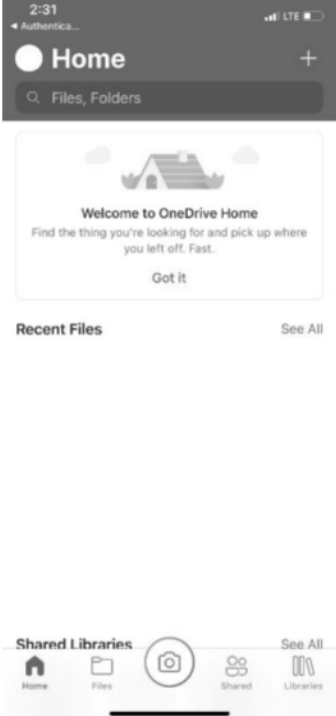


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to O365 via your mobile device (e.g. Teams).*

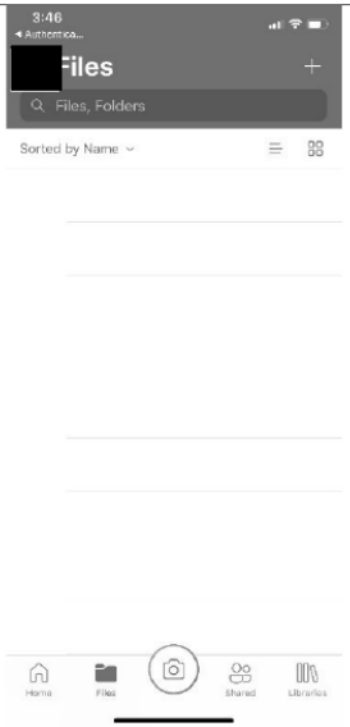

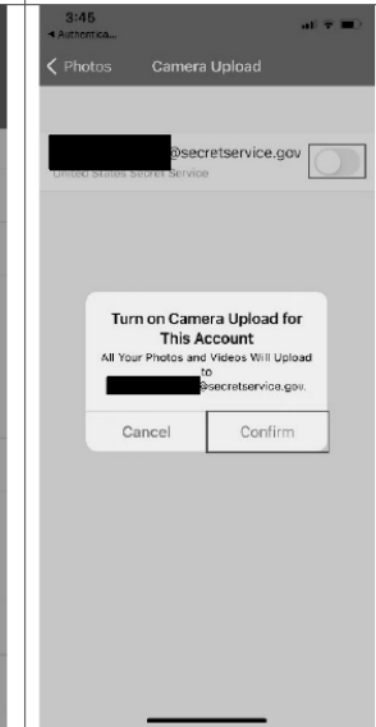
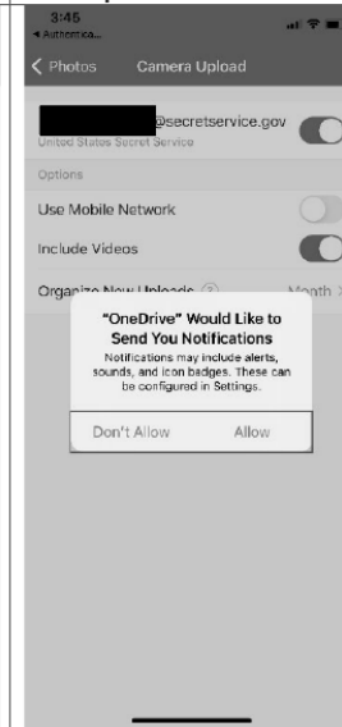
Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#).*

<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

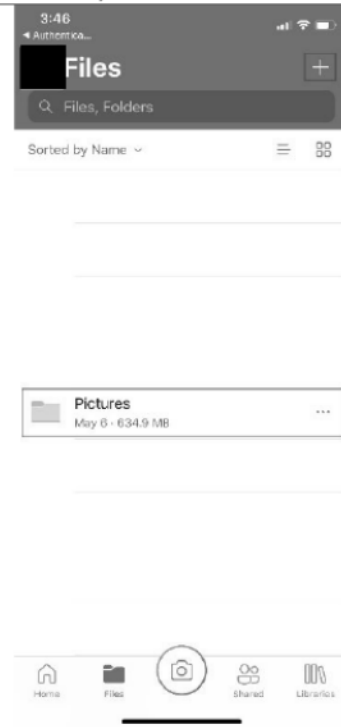
USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

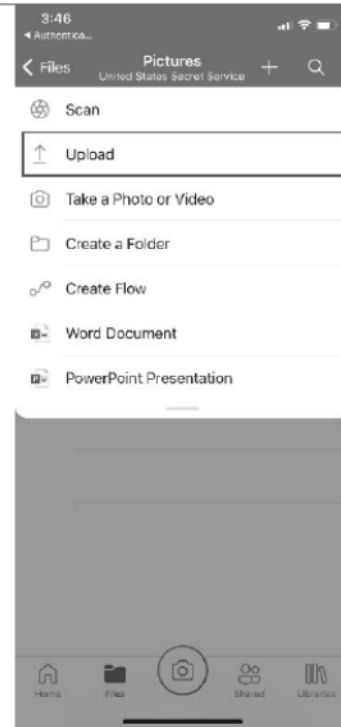
Rev. Jan 15 2020 RLT

Selected items

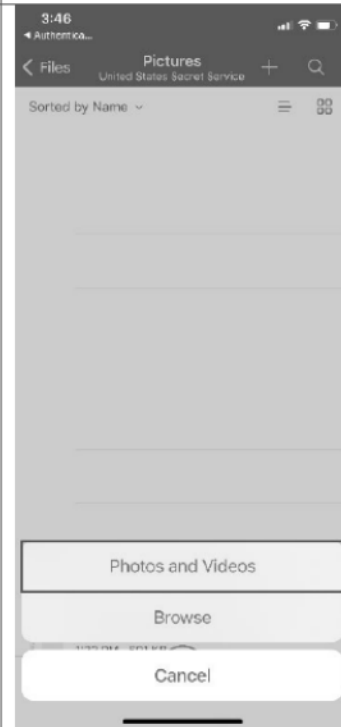
From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.



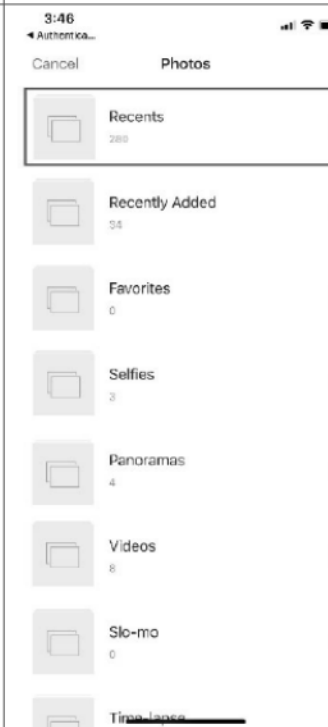
Select **Upload**.



Select **Photos and Videos**.



Select **Recents**.



Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Check iMessages

Verify if you have any iMessages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

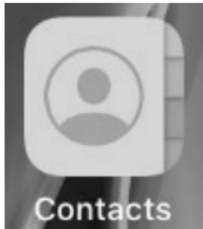
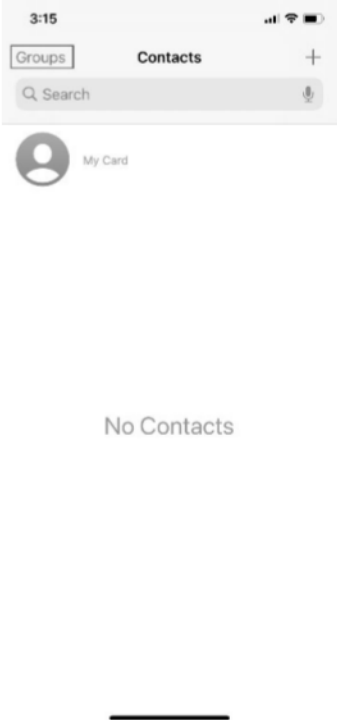
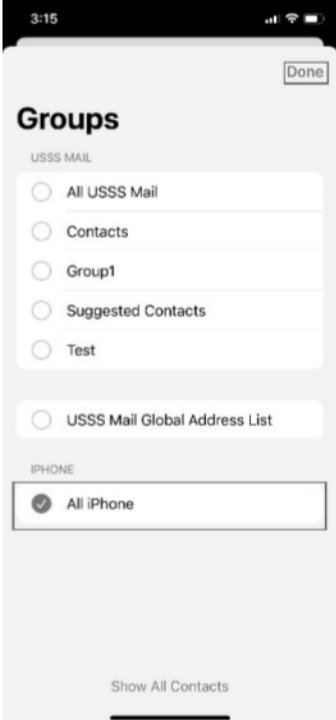

iMessages Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

Check Contacts




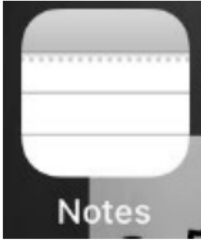

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure just All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be added to your contacts within Outlook.
			

USSS Preserve Content Guide for iPhone & iPad

Check Notes

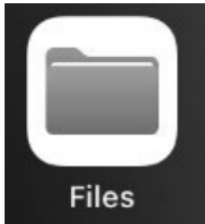

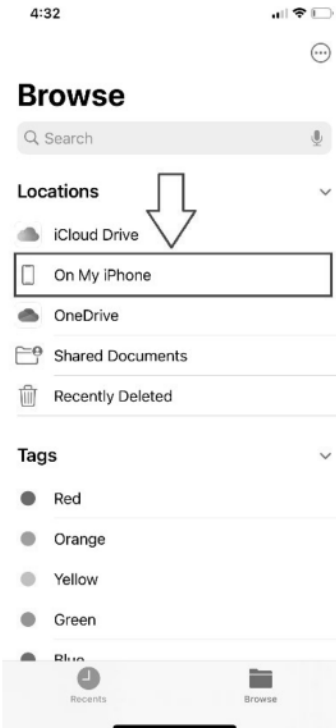

Follow the steps below to determine if you have any notes saved locally on your mobile device.

Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Outlook.
				

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.
			

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check iMessages](#)

[Check Contacts](#)

[Check Notes](#)


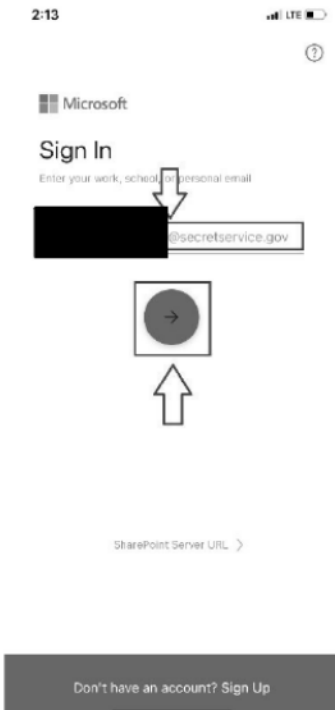


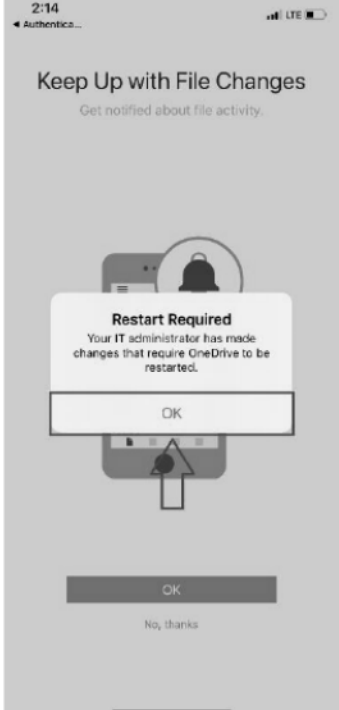
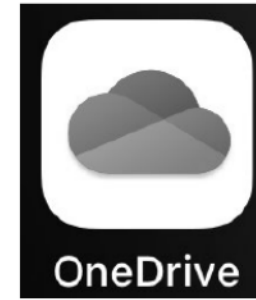
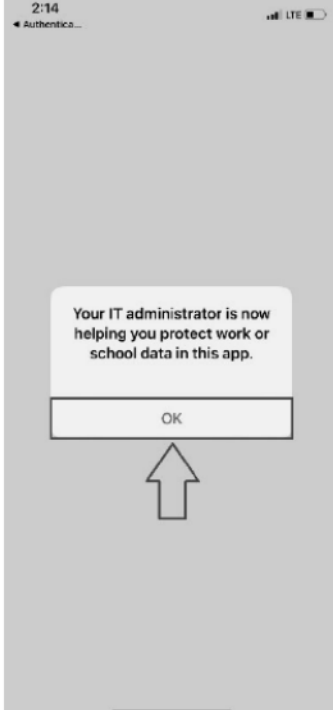
[Check Files](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to O365 via your mobile device (e.g. Teams). If you have, continue to these steps [here](#).

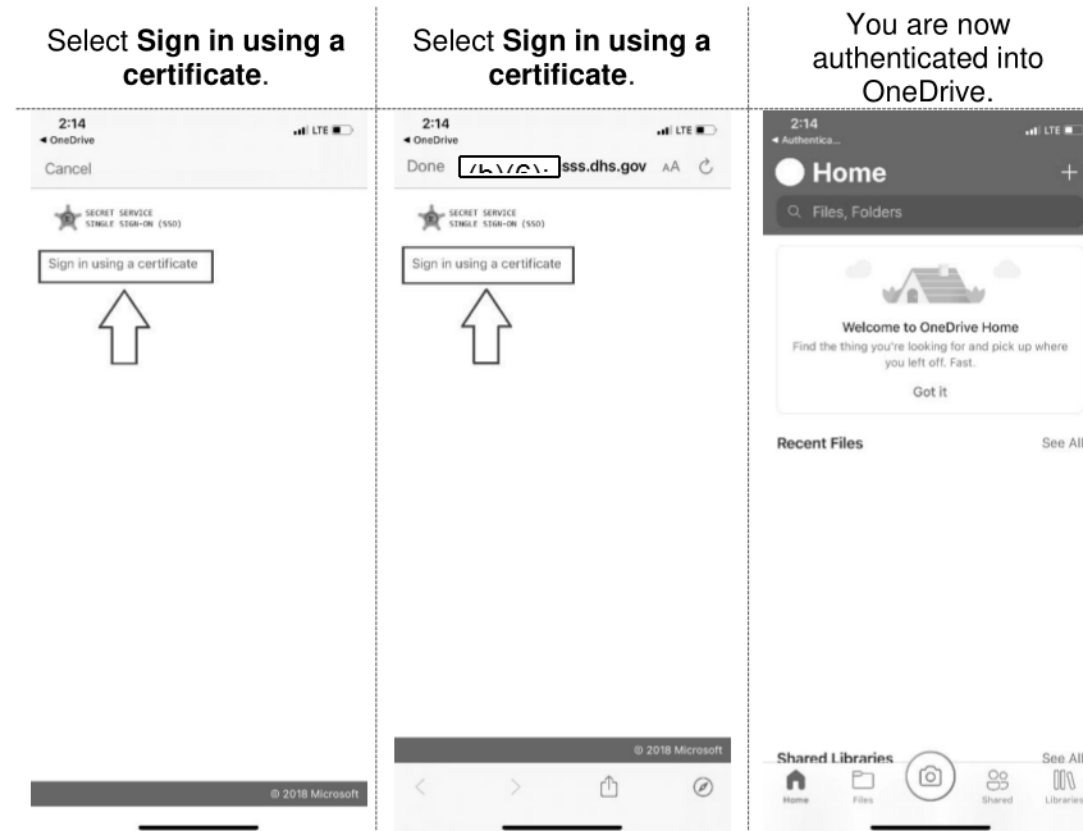
Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Never O365 Authenticated Continued....


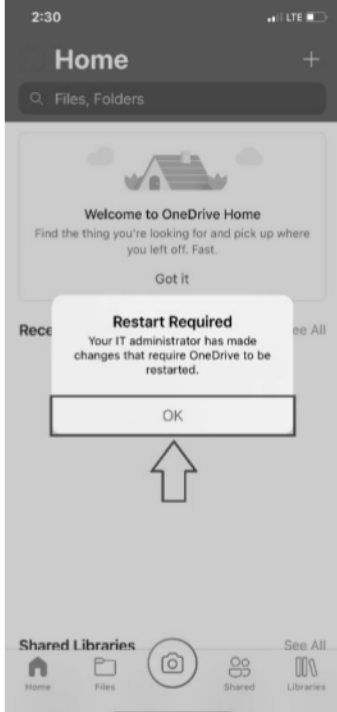
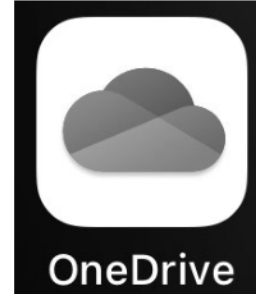



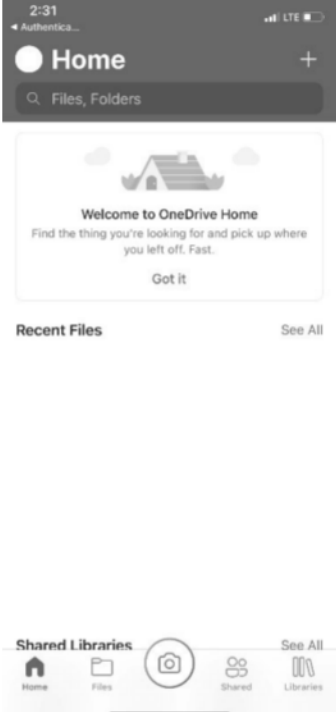


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

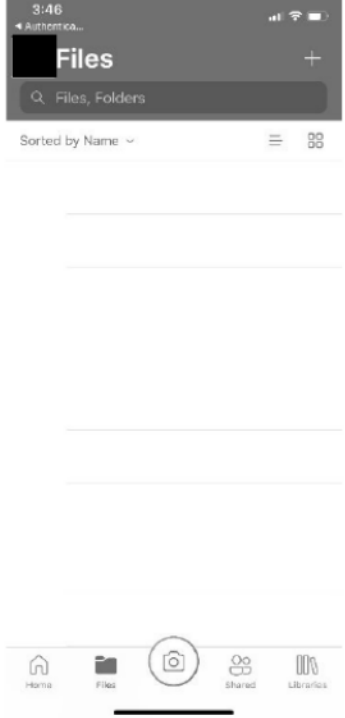
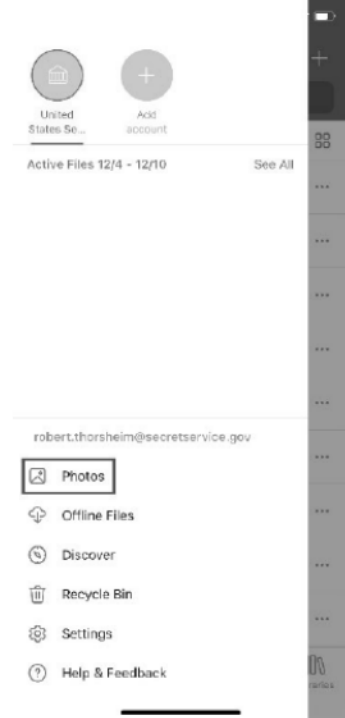
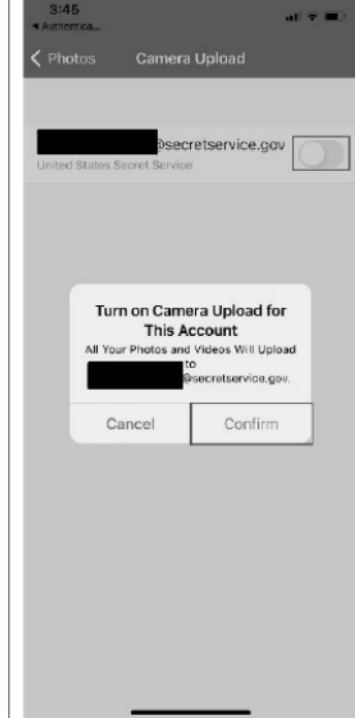
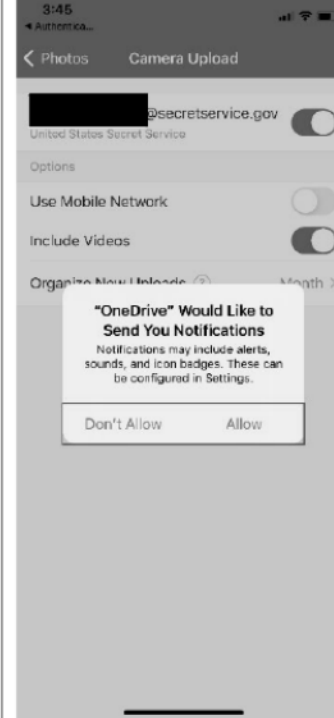
Rev. Jan 15 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to O365 via your mobile device (e.g. Teams).*

Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#). **Note: it is best to be connected to Wi-Fi to perform these transfers.***

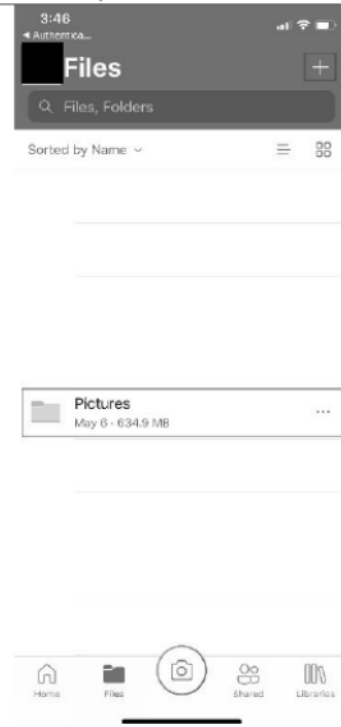
<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

USSS Preserve Content Guide for iPhone & iPad

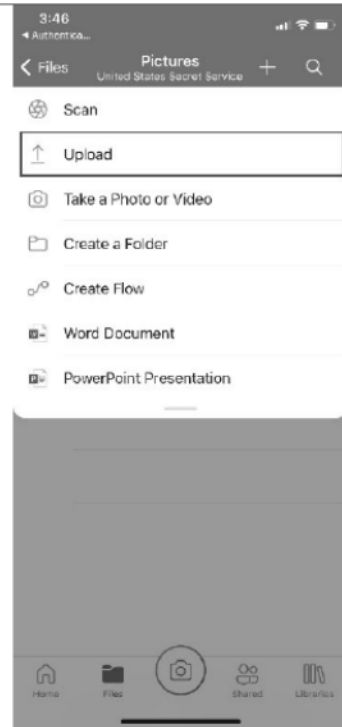
Selected items: **Note: it is best to be connected to Wi-Fi to perform these transfers.**

From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

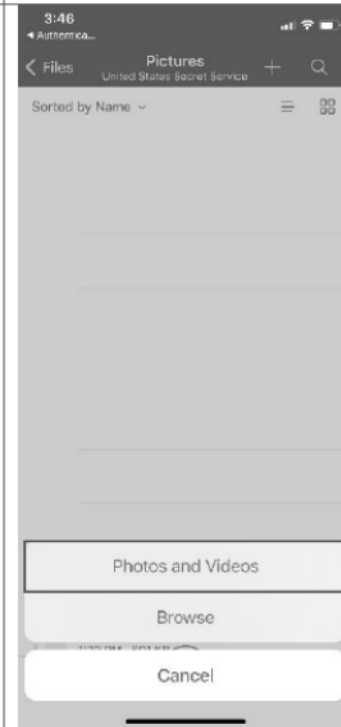
Select **Upload**.



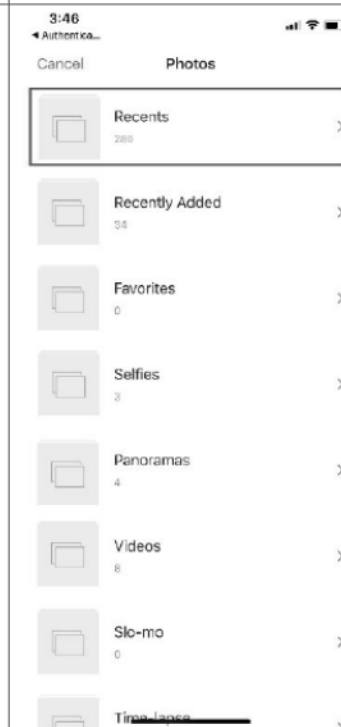
Select **Photos and Videos**.



Select **Recents**.



Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 15 2020 RLT

Check iMessages

Verify if you have any iMessages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

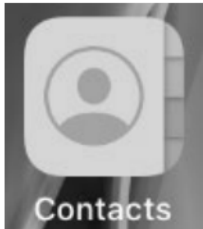
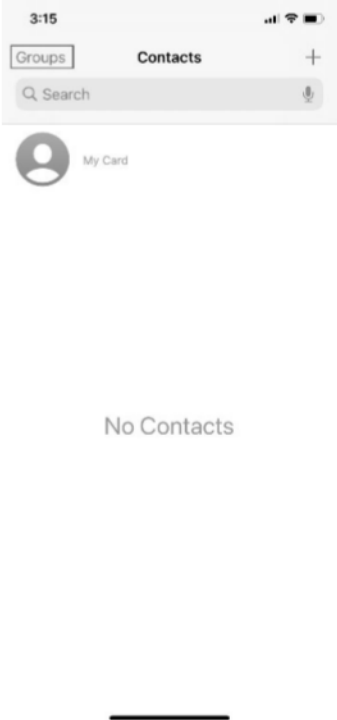
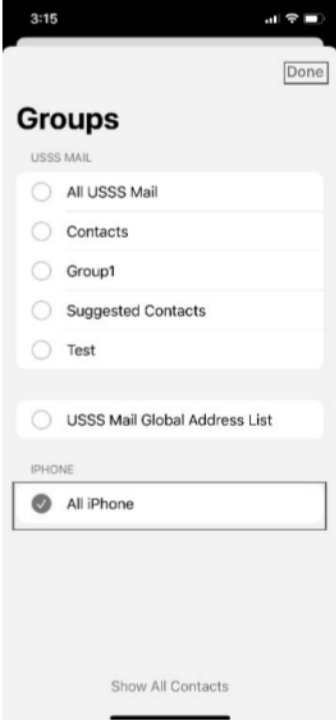

iMessages Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

Check Contacts



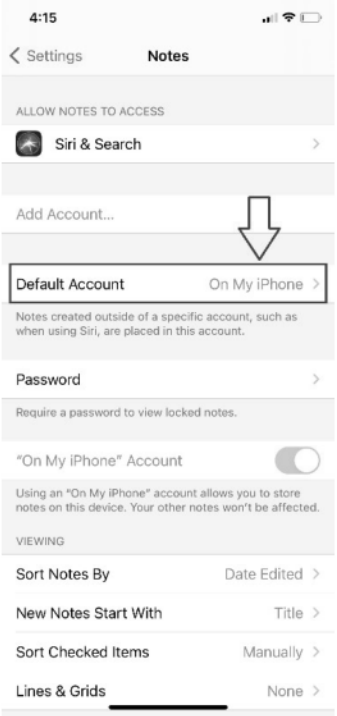
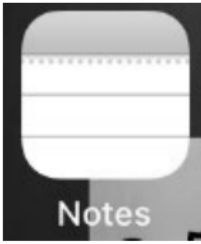

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure just All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be added to your contacts within Outlook.
			

USSS Preserve Content Guide for iPhone & iPad

Check Notes

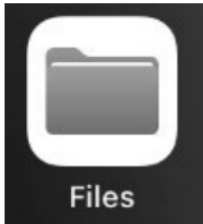

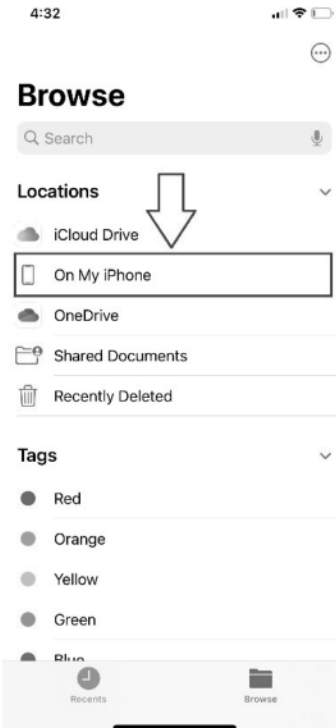

Follow the steps below to determine if you have any notes saved locally on your mobile device.

Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Outlook.
				

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.
			

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 22 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check iMessages](#)

[Check Contacts](#)

[Check Notes](#)


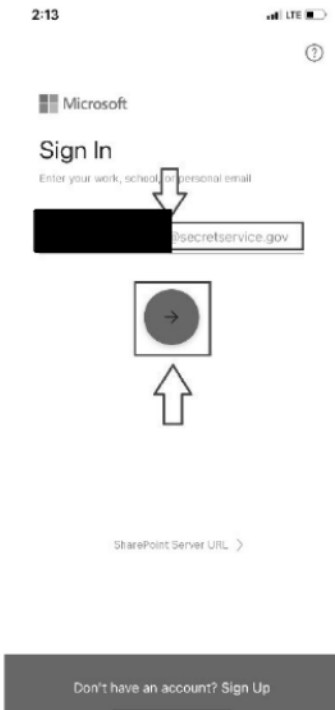



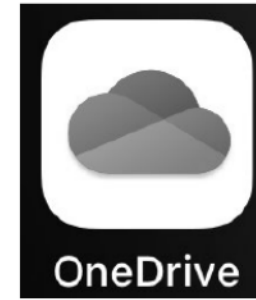
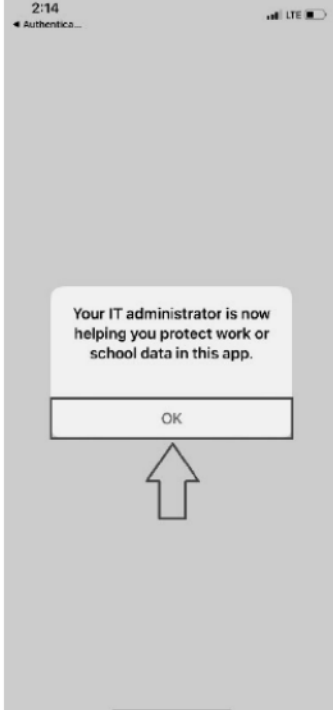
[Check Files](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to Teams via your mobile device. If you have, continue to these steps [here](#).

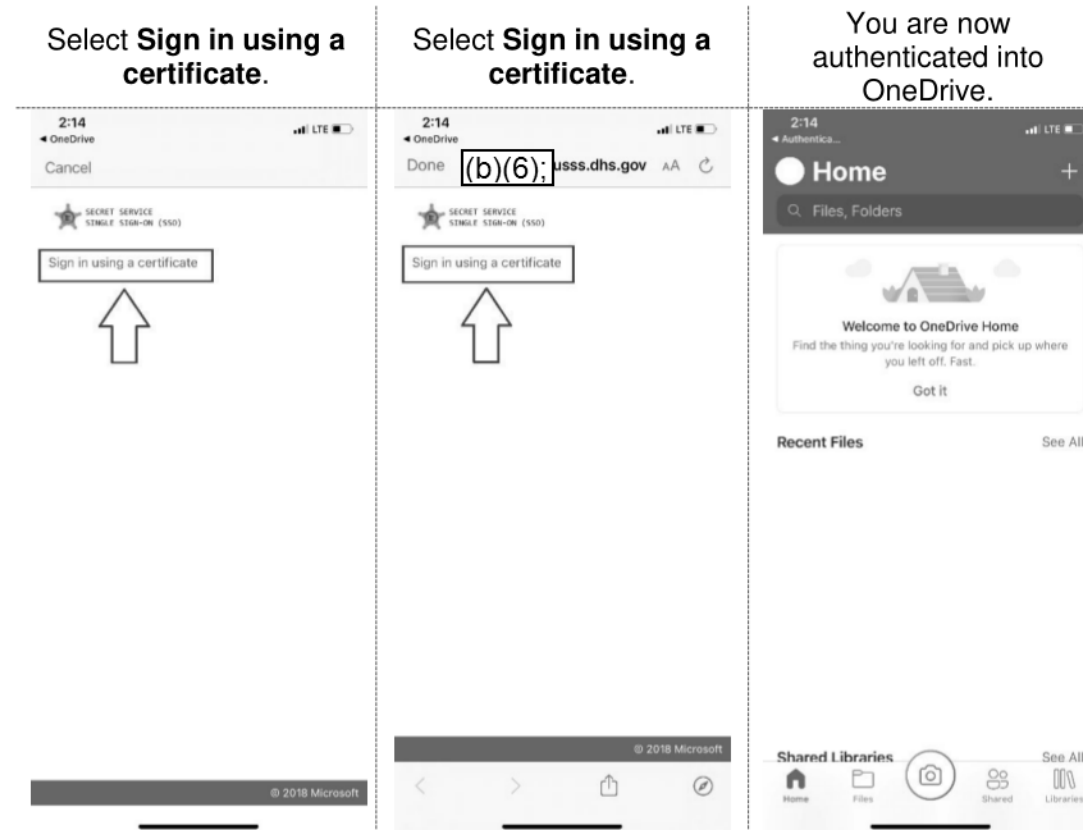
Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 22 2020 RLT

Never O365 Authenticated Continued....


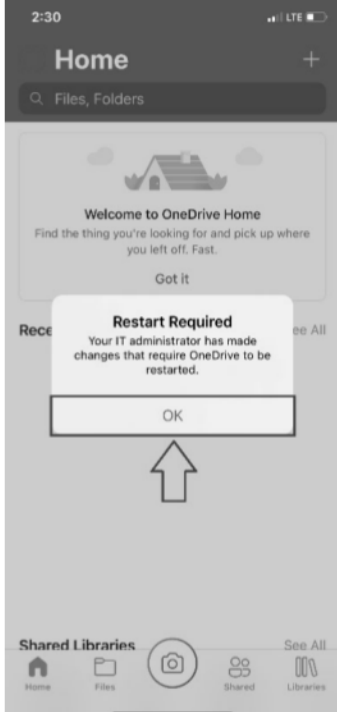
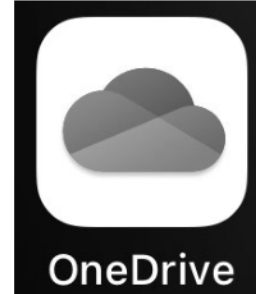



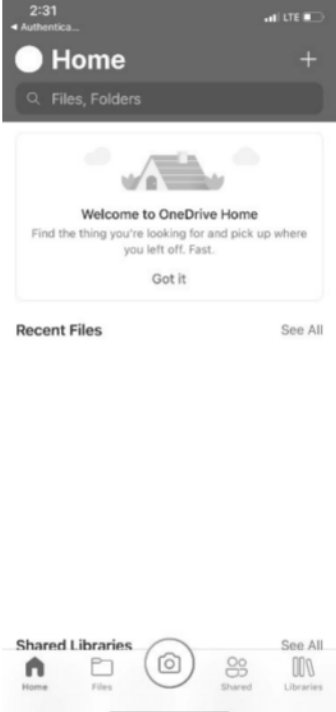


USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

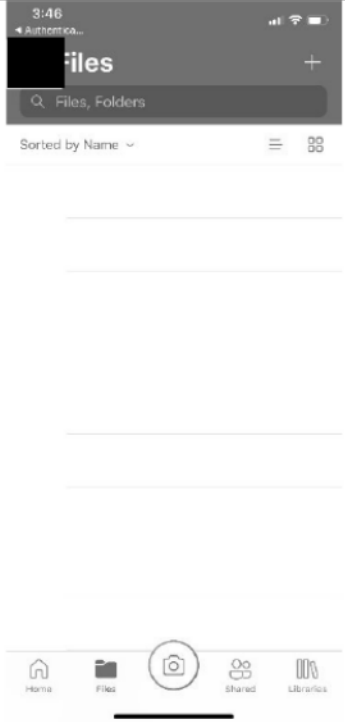

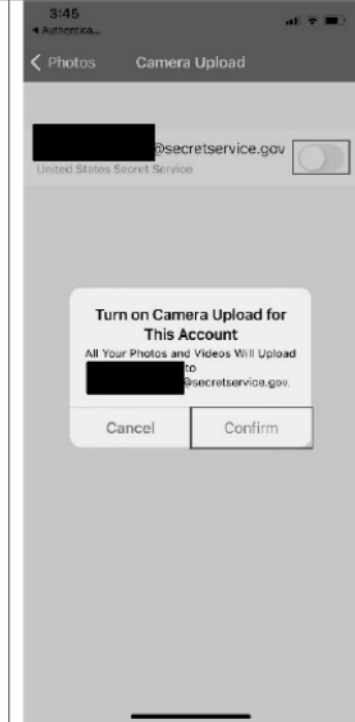
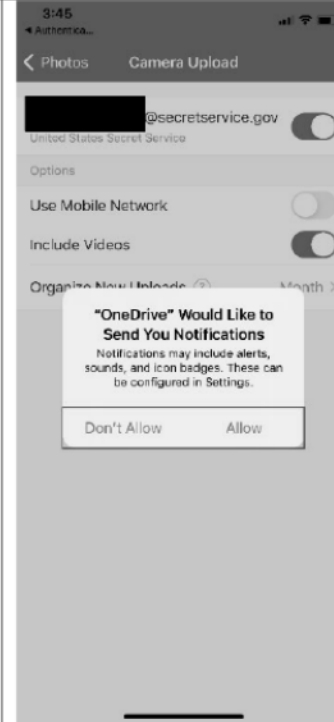
Rev. Jan 22 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to Teams via your mobile device.*

Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#). **Note: it is best to be connected to Wi-Fi to perform these transfers.***

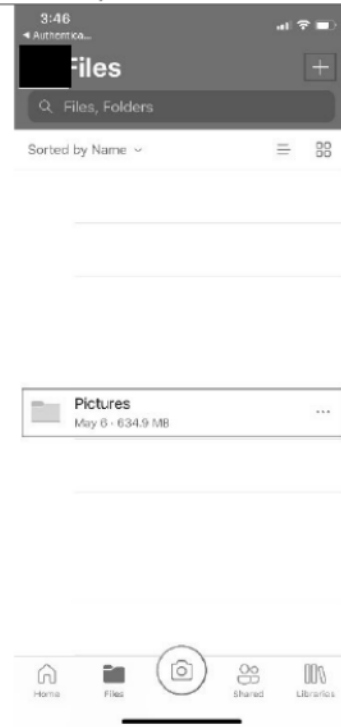
<p>Select image in upper left corner.</p>	<p>Select Photos.</p>	<p>Toggle on next to your @secretservice.gov account. Select Confirm.</p>	<p>Decide whether you want notifications. Wait for your photos/videos to complete the transfer.</p>
			

USSS Preserve Content Guide for iPhone & iPad

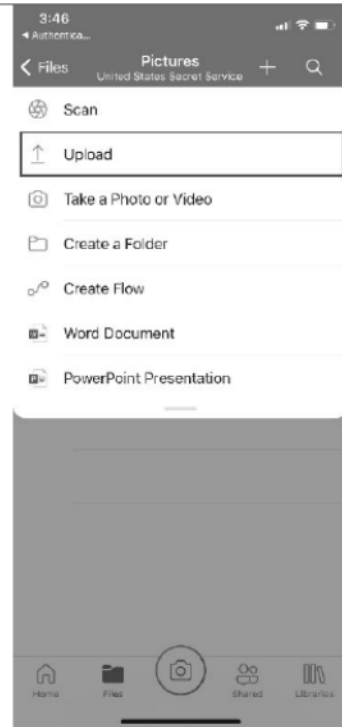
Selected items: **Note: it is best to be connected to Wi-Fi to perform these transfers.**

From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

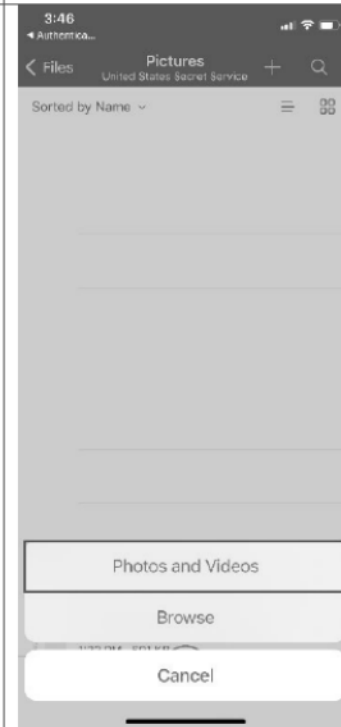
Select **Upload**.



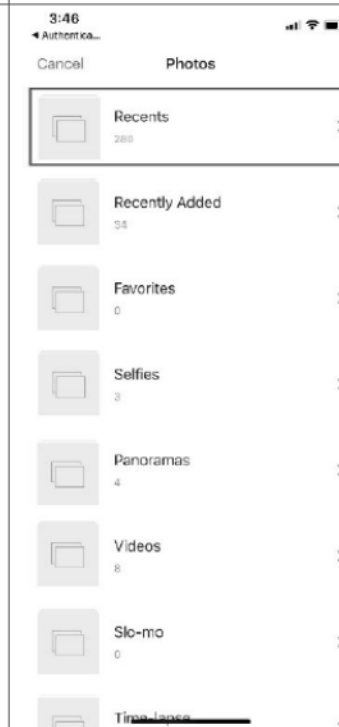
Select **Photos and Videos**.



Select **Recents**.



Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 22 2020 RLT

Check iMessages

Verify if you have any iMessages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

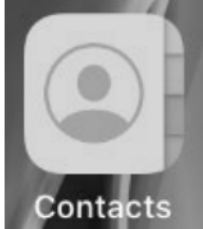
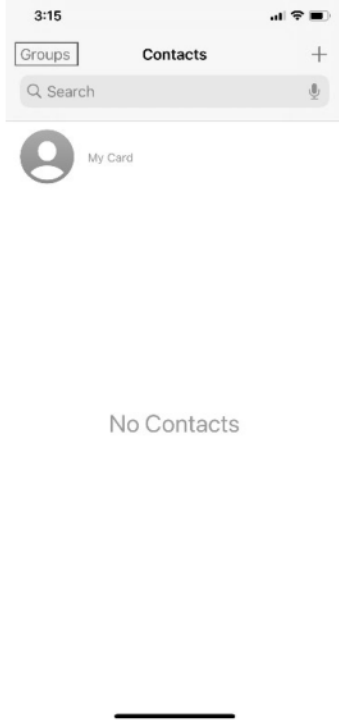
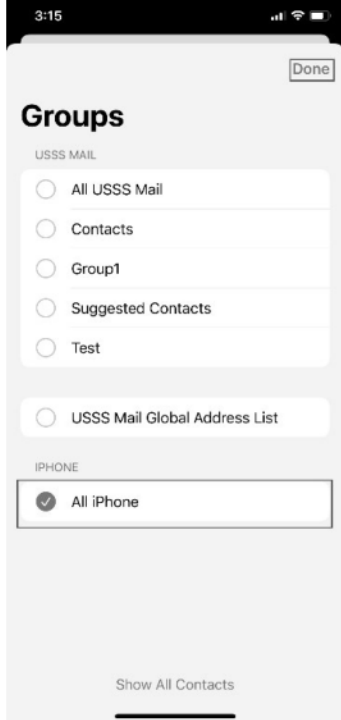
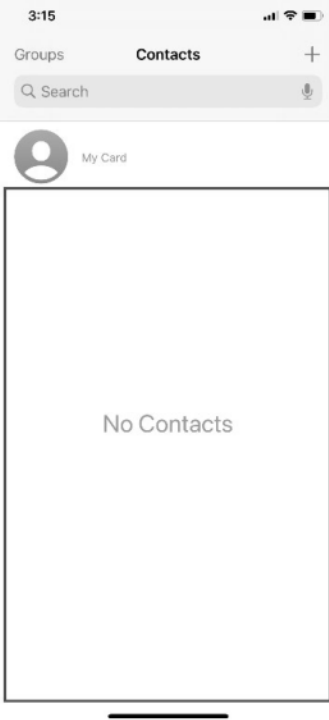
iMessages Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

Check Contacts

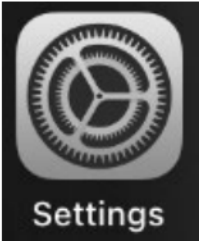


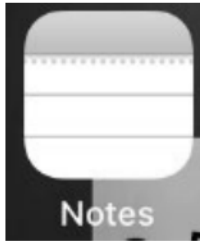

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure <i>only</i> All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be preserved. If so, add them to your contacts within Outlook from your PC.
			

USSS Preserve Content Guide for iPhone & iPad

Check Notes

Follow the steps below to determine if you have any notes saved locally on your mobile device.

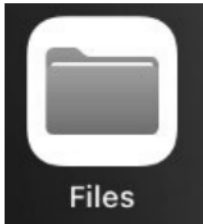

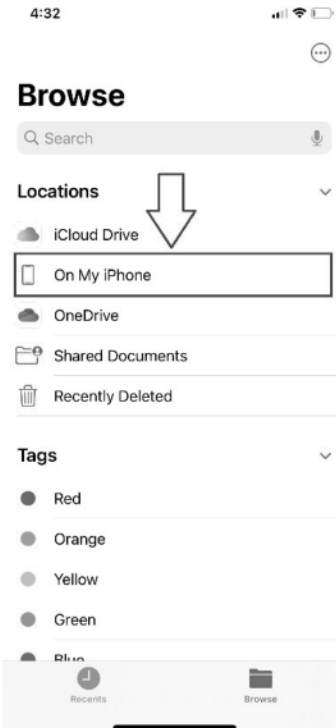
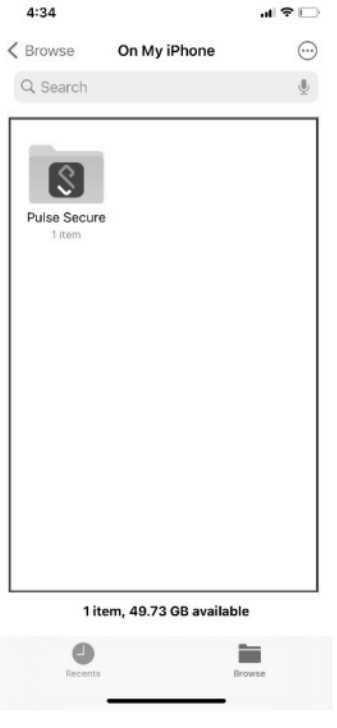
Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Notes.
				

There are numerous steps for saving these notes that you would have to determine which method is best for you. Screenshot your notes or save to OneDrive are just a couple of methods from your numerous options for preserving these notes.

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.
			

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

Introduction

The following guide has been provided for your use, to assist in determining if you have any content that needs to be preserved, prior to wiping your iPhone/iPad. If you know that there is nothing on your device that you wish to preserve, then you can proceed with wiping your device, otherwise please review the options provided below.

Table of Contents

[Check Photos](#)

[Check Messages](#)

[Check Contacts](#)

[Check Notes](#)

[Check Files](#)


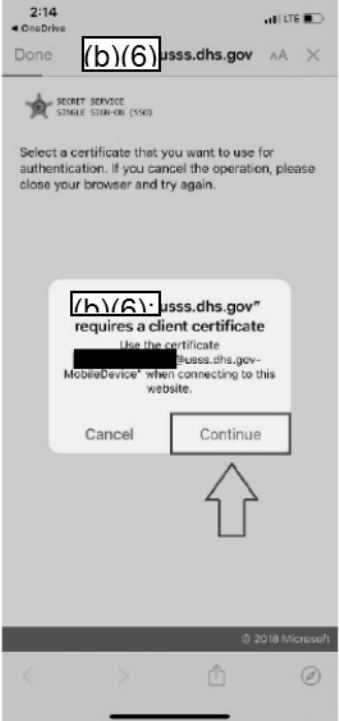
[FAQ](#)

USSS Preserve Content Guide for iPhone & iPad

Check Photos

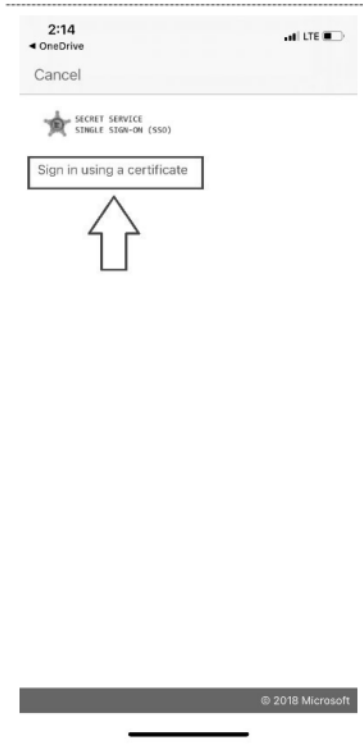
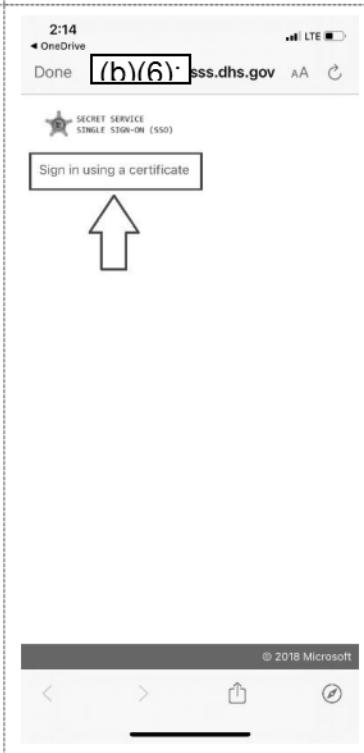
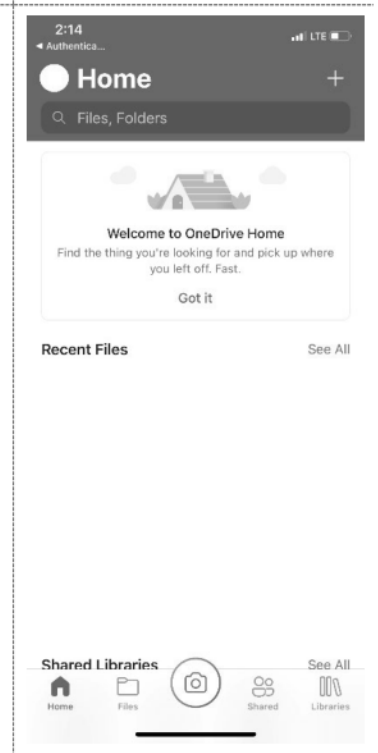
Verify if you have photos that you need preserved, you can either email the photos to yourself, or follow the steps below for utilizing Microsoft OneDrive.

Never O365 Authenticated: Follow these steps if you have never authenticated to Teams via your mobile device. If you have, continue to these steps [here](#).

Open Microsoft OneDrive.	Type in your @secretservice.gov credentials. Select Next .	Select Continue .	Select OK .	Select OK .	Open Microsoft OneDrive.	Select OK .
						

USSS Preserve Content Guide for iPhone & iPad

Never O365 Authenticated Continued....


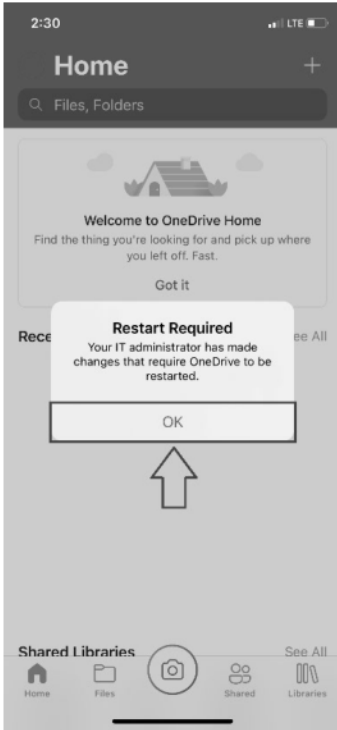



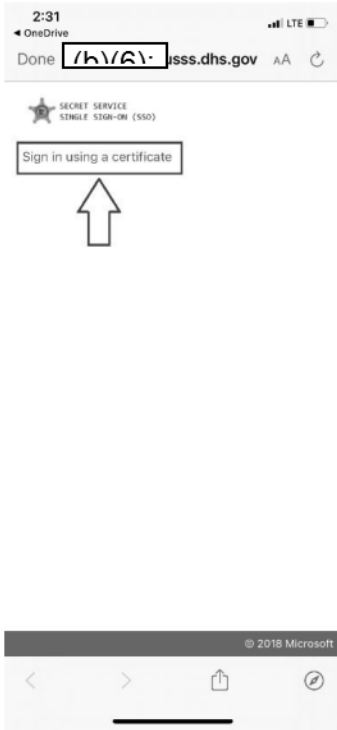
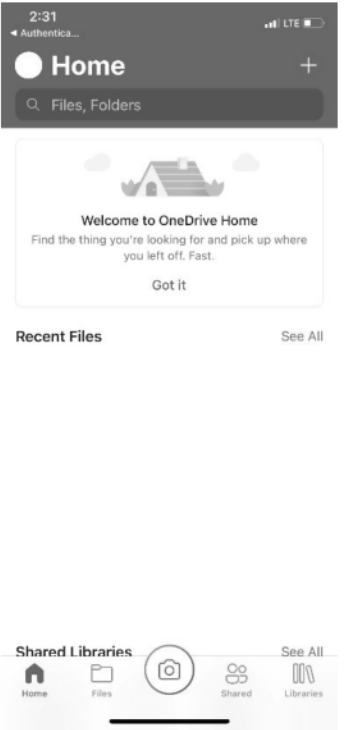
<p>Select Sign in using a certificate.</p> 	<p>Select Sign in using a certificate.</p> 	<p>You are now authenticated into OneDrive.</p> 
---	--	--

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

Already O365 Authenticated: *Follow these steps if you have authenticated to Teams via your mobile device.*

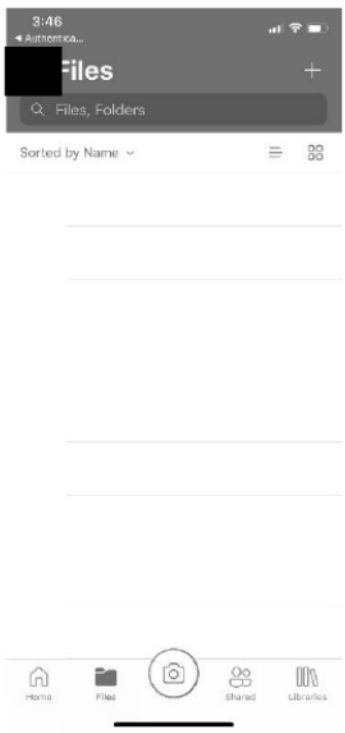

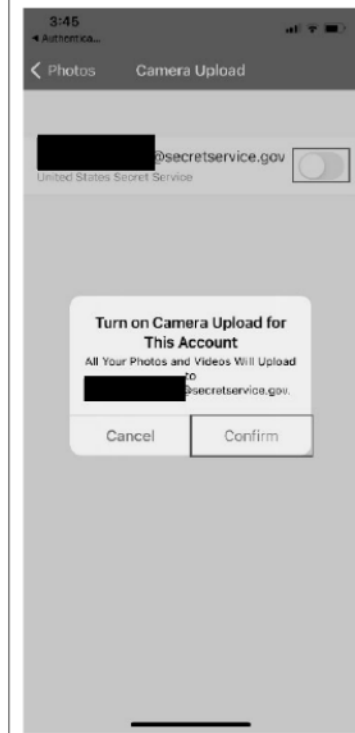
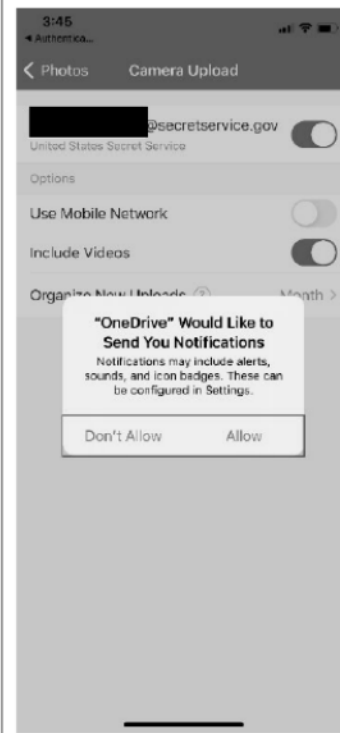
Open Microsoft OneDrive.	Select OK .	Open Microsoft OneDrive.	Select OK .	Select Sign in using a certificate .	Select Sign in using a certificate .	You are now authenticated into OneDrive.
						

USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

All Photos/Videos: *Follow these steps if you want to transfer all photos/videos. If you just wish to transfer selected item, continue to these steps [here](#). **Note: it is best to be connected to Wi-Fi to perform these transfers.***

Select image in upper left corner.	Select Photos.	Toggle on next to your @secretservice.gov account. Select Confirm .	Decide whether you want notifications. Wait for your photos/videos to complete the transfer.
			

USSS Preserve Content Guide for iPhone & iPad

Selected items: **Note: it is best to be connected to Wi-Fi to perform these transfers.**

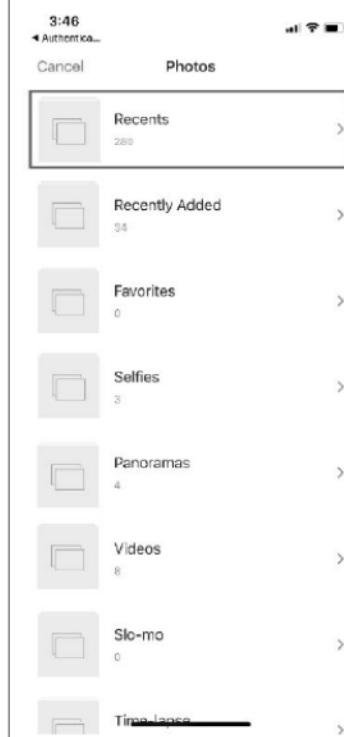
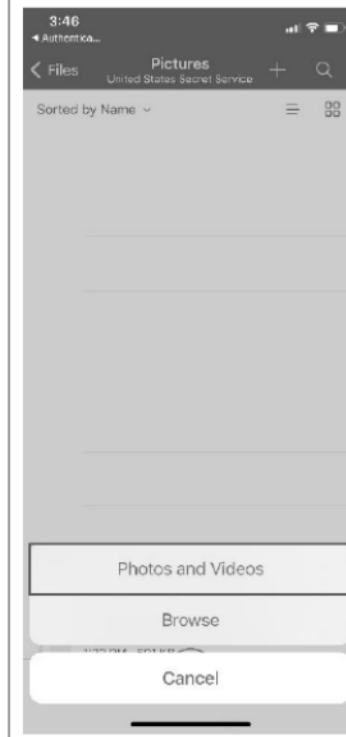
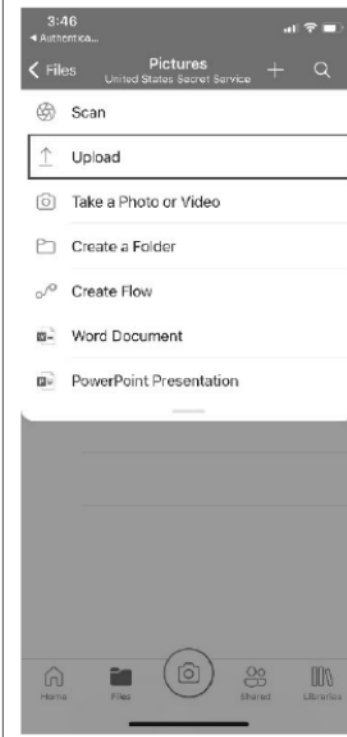
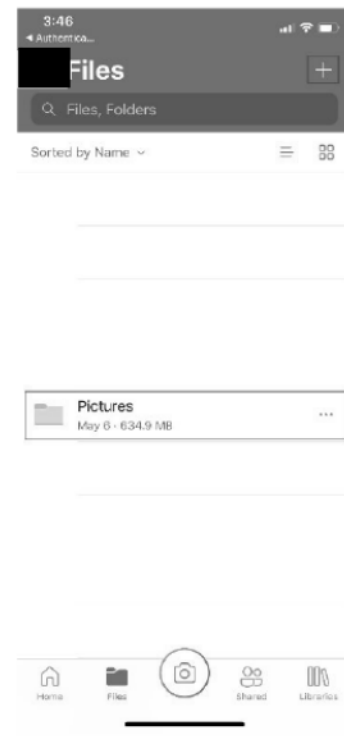
From OneDrive, either select the **Pictures** folder if one already exists, or create a folder by selecting the add button in the upper right hand corner. If you created a folder, select that folder.

Select **Upload**.

Select **Photos and Videos**.

Select **Recents**.

Select the files you want to transfer. Select **Done**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

Check Messages

Verify if you have any Messages that need to be preserved. Follow the steps below to take screenshots, then go to Check Photos [here](#), for guidance on preserving those photos. For preserving iMessage Groups, see remarks [here](#).

Screenshot Steps

1. For iPhone Xs – Press Volume Up and Power Button at the same time
2. For iPhone 8 and below _ Press Home Button and Power Button at the same time.

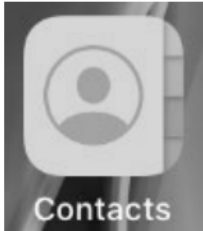
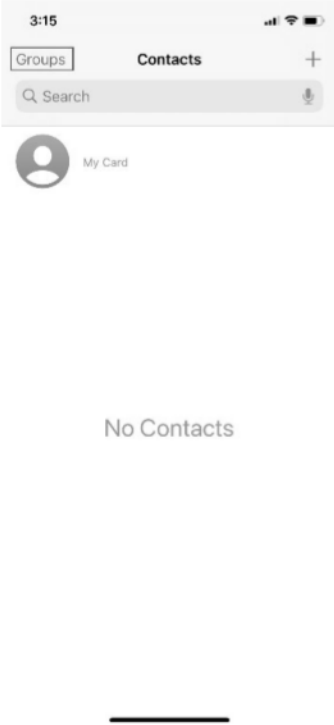
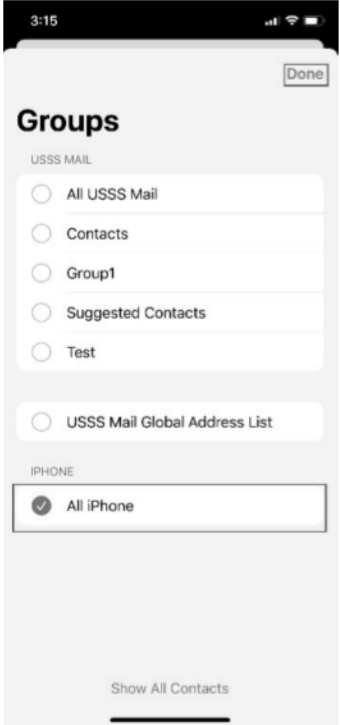

iMessage Groups

iMessage Groups cannot be backup-up and will not be retrievable once the device has been wiped. If you have iMessage Groups that you would like to recreate, OCIO has provided a guide for recreating your iMessage Groups within Shortcuts Application, which can be viewed [here](#). Otherwise you can document which contacts you currently have in your iMessage Groups and recreate them within your iMessage app, once re-enrolled. Another option is to have someone that still has the same iMessage group send a message once re-enrolled, which will apply the group to your iMessage app.

USSS Preserve Content Guide for iPhone & iPad

Check Contacts

Follow the steps below to determine if you have any contacts saved locally on your mobile device.

Open Contacts .	Open Groups .	Make sure <i>only</i> All iPhone is selected. Select Done .	Review contacts to determine if any of them need to be preserved. If so, <i>add them to your contacts within Outlook from your PC.</i>
			 <p data-bbox="1884 683 2206 1040">If you followed the step correctly for making sure <i>only</i> All iPhone was selected, then you will see contacts that are saved locally to your device. If you don't see any contacts, that means all of your contacts are already getting saved to Outlook.</p>

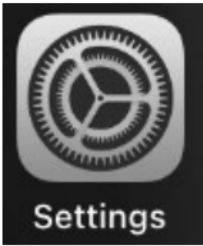




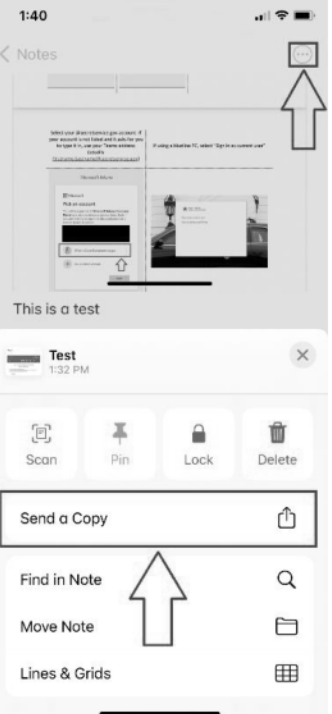
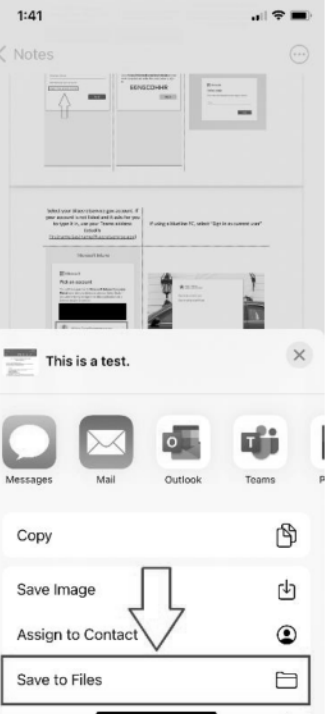
USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

Check Notes

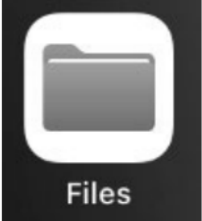

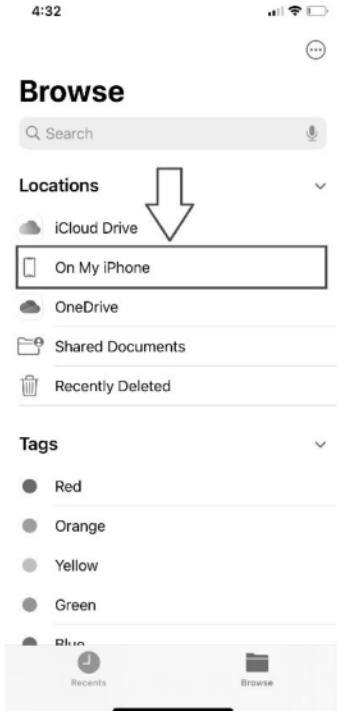

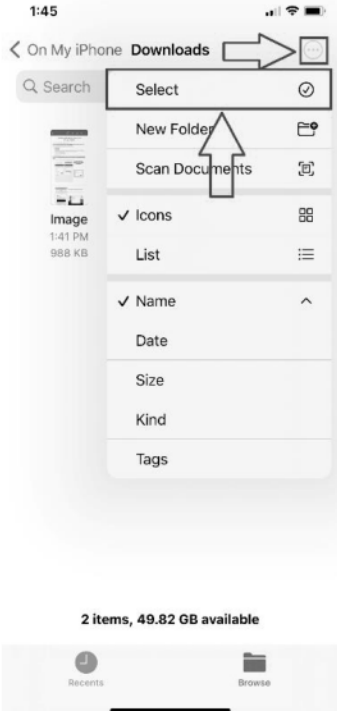
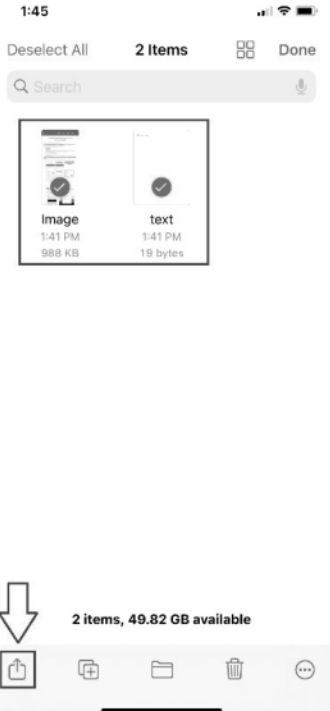
Follow the steps below to determine if you have any notes saved locally on your mobile device.

Open Settings .	Select Notes .	Change Default Account to On My iPhone .	Open Notes .	Determine if there are any Notes saved On My iPhone that need saved within Notes.	Open the Note that you want to preserve. Select Options in upper right hand corner. Select Send a Copy	Select Save to Files . Continue to Check Files steps here .
						

USSS Preserve Content Guide for iPhone & iPad

Check Files

Follow the steps below to determine if you have any files saved locally on your mobile device.

Open Files .	Select Browse in the lower right. Select Browse in the upper left.	Select On My iPhone .	Check Files and Folders, to see if you have any content that need preserved.	Selection Options in upper right hand corner. Select Select .	Select the files that you want to preserve. Select Share in the lower left hand corner.
					

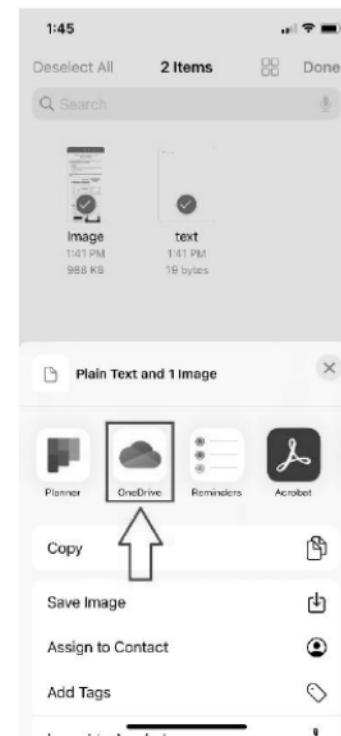
USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

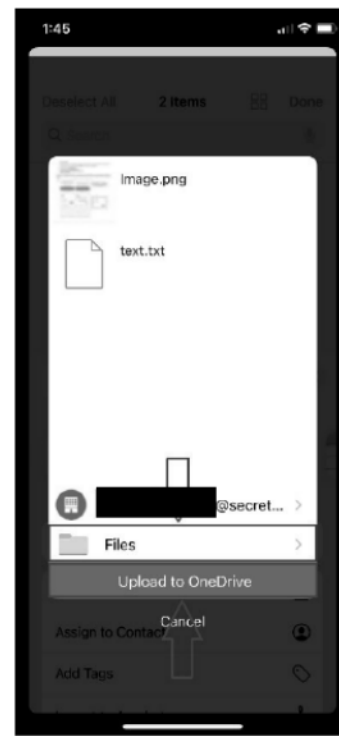
Rev. Jan 27 2020 RLT

Check Files Continued....

Select **OneDrive**.



Choose the folder that you want your files to be saved in. Select **Upload to OneDrive**.



USSS Preserve Content Guide for iPhone & iPad

[Table of Contents](#)

Rev. Jan 27 2020 RLT

FAQ

Please see below for Frequently Asked Questions that have been received regarding preserving content.

Can I backup my Photos?

Yes. Please follow the steps described [here](#).

Can I backup my Messages?

No. You can take screenshots of your messages and backup those screenshots. Please follow the steps described [here](#).

Can I backup my iMessage Groups?

No. You can document your iMessage Groups and recreate them. Please follow the steps described [here](#).

Can I backup my Contacts?

Yes, contacts sync automatically to your Outlook account. If your contacts are saved locally, you will have to follow steps described [here](#).

Can I backup my Notes?

Yes, notes sync automatically to your Outlook account. If your notes are saved locally, you will have to follow steps described [here](#).

Can I backup my Files?

Yes. Please follow the steps described [here](#).

Can I backup my documents in Adobe Reader?

Yes. They can be backed-up from the Files app. Steps for backing up documents from the Files app can be found [here](#).

Can I backup my files in iTAK?

Yes. They can be backed-up from the Files app. Steps for backing up documents from the Files app can be found [here](#).

From: CIO
To: USA
Subject: *****CORRECTION***** 145.000 Deployment of iPhone/iPad OneDrive Application
Date: Thursday, January 14, 2021 2:02:04 PM

***** Correction made to change date of Deployment*****

//ROUTINE//

FROM: Headquarters (OCIO - Office of the Chief Information Officer)
File: 145.000

TO: All USSS Employee's

SUBJECT: Deployment of iPhone/iPad OneDrive Application

The Office of the Chief Information Officer (OCIO) is rolling out the Microsoft (MS) Office365 "OneDrive" application, making it available to all Secret Service users via their issued USSS iPhones/iPads. This application will replace the current USSS OneDrive link on iPhones/iPads, which will still be available through Intranet.

The MS OneDrive application will be deployed to USSS iPhones/iPads on Friday, January 22, 2021. Once installed on your iPhone/iPad, you will find a new icon on your iPhone, named "OneDrive", which appears as a blue cloud with a white background. You should already have an application named "Authenticator" on your iPhone/iPad. Both are required for proper functionality of OneDrive on the iPhone/iPad.

Important First Time Sign-In Information

Users should follow the below instructions for a first-time sign-on of the OneDrive application after it has been installed on an iPhone/iPad. Your sign-in credentials should be automatically stored for subsequent sign-on into the application after your initial entry.

If you currently have an email address ending in @usss.dhs.gov:

Your OneDrive(0365) user ID will be the same as the first portion of your current email address, but instead of using @usss.dhs.gov you will use **@secretservice.gov** for the right-side part of the email address.

(b)(6); (b)(7)(C) will use

If your current email address ends in @associates.usss.dhs.gov:

Your OneDrive(0365) user ID will be the same as that of the first portion of your current email address, but with the addition of ".ctr" before the @ sign and you will also use **@secretservice.gov**

(b)(6); (b)(7)(C) will use

It is highly recommended that you take full advantage of the available information related to the software by viewing the Microsoft OneDrive instructional videos via this web link: [MS OneDrive Training](#). Please note that you may have to access an external website first such as Google, in order to authenticate your PIV creds and then to view these videos.

The training video content is very informative, comprehensive, and will likely cover questions you may have about the software and its use.

You can also utilize a Quick Start PDF reference guide to assist you with some of the "How To" questions for MS OneDrive. Access the Quick Start document here: [Microsoft OneDrive Quick-Start Guide](#)

If you try the OneDrive application on your current non-Apple device and it does not work, then you can access OneDrive via this web link:

<https://unitedstatessecretservice-my.sharepoint.com> You will be using the web-version of the application and your sign on information using the web link is the same as indicated above.

For any questions related to this information, please contact the OCIO

Service Desk at

(b)(6); (b)(7)(C)

Headquarters (CIO - Chief Information Officer)

Wilson/Nally

From: CIO
To: ITO; SMD; AOD; CIO
Subject: 145.000 Deployment of iPhone/iPad OneDrive Application
Date: Thursday, January 14, 2021 12:42:28 PM

//ROUTINE//

FROM: Headquarters (OCIO - Office of the Chief Information Officer)
File: 145.000

TO: Chief - Security Management Division
SAIC - Investigative Support Division
Chief - Administrative Operations Division
Attn: Property Management Division
SAIC - Information Technology Operations

SUBJECT: Deployment of iPhone/iPad OneDrive Application

The Office of the Chief Information Officer (OCIO) is rolling out the Microsoft (MS) Office365 "OneDrive" application, making it available to all Secret Service users via their issued USSS iPhones/iPads. This application will replace the current USSS OneDrive link on iPhones/iPads, which will still be available through Intranet.

The MS OneDrive application will be deployed to USSS iPhones/iPads on Friday, January 15, 2021. Once installed on your iPhone/iPad, you will find a new icon on your iPhone, named "OneDrive", which appears as a blue cloud with a white background. You should already have an application named "Authenticator" on your iPhone/iPad. Both are required for proper functionality of OneDrive on the iPhone/iPad.

Important First Time Sign-In Information

Users should follow the below instructions for a first-time sign-on of the OneDrive application after it has been installed on an iPhone/iPad. Your sign-in credentials should be automatically stored for subsequent sign-on into the application after your initial entry.

If you currently have an email address ending in @usss.dhs.gov:

Your OneDrive(0365) user ID will be the same as the first portion of your current email address, but instead of using @usss.dhs.gov you will use **@secretservice.gov** for the right-side part of the email address.

(b)(6); (b)(7)(C) will use

If your current email address ends in @associates.usss.dhs.gov:

Your OneDrive(0365) user ID will be the same as that of the first portion of your current email address, but with the addition of ".ctr" before the @ sign and you will also use **@secretservice.gov**

(b)(6); (b)(7)(C) will use

It is highly recommended that you take full advantage of the available information related to the software by viewing the Microsoft OneDrive instructional videos via this web link: [MS OneDrive Training](#). Please note that you may have to access an external website first such as Google, in order to authenticate your PIV creds and then to view these videos.

The training video content is very informative, comprehensive, and will likely cover questions you may have about the software and its use.

You can also utilize a Quick Start PDF reference guide to assist you with some of the "How To" questions for MS OneDrive. Access the Quick Start document here: [Microsoft OneDrive Quick-Start Guide](#)

If you try the OneDrive application on your current non-Apple device and it does not work, then you can access OneDrive via this web link: <https://unitedstatessecretservice-my.sharepoint.com> You will be using the web-version of the application and your sign on information using the web link is the same as indicated above.

For any questions related to this information, please contact the OCIO
Service Desk at (b)(6); (b)(7)(C)

Headquarters (CIO - Chief Information Officer)

Wilson/Nally

From: CIO
To: USA
Subject: 145.000 Mobile Device Management Migration
Date: Monday, January 25, 2021 3:37:47 PM

//ROUTINE//

FROM: Office of the Chief Information Officer File: 145.000
TO: All Offices
SUBJECT: Mobile Device Management Migration

Reference is made to the CIO Official Message, dated 1/14/2021, Deployment of iPhone/iPad OneDrive Application.

The Office of the Chief Information Officer (CIO) will begin migrating mobile devices to the Microsoft Intune Mobile Device Management (MDM) System on Wednesday, 1/27/2021. Migration of USSS iPhones and/or iPads will not occur all at once for every device, but through a systematic targeting of individual and pre-designated divisions or offices, in a methodical approach and over the course of several months. Prior to migration, individuals assigned to the specifically targeted divisions or offices for a particular date, will receive the following email communication:

USSS Mobile Device User:

You are receiving this message because your USSS issued iPhone and/or iPad device has been migrated to our new Intune Mobile Device Management (MDM) system. In order to complete this migration, you must enroll your device within this new system.

Enrollment of USSS iPhones and/or iPads in the new MDM system will erase all data on your mobile device to include contacts, iMessages, photographs, notes, and files. Follow the content preservation guide found [here](#) to prevent permanent data loss.

To self-enroll, complete the enrollment steps found [here](#). You will be given two weeks to self-enroll in the new MDM system. If you do not self-enroll within the given timeframe, your iPhone and/or iPad device(s) will be remotely wiped, and the OCIO will initiate the enrollment process automatically.

The CIO recommends that all personnel self-enroll at their earliest convenience once notified. Please plan in allowing 30 minutes for the enrollment process to complete.

If your device fails to enroll, submit a ticket to [the ITO Service Desk](#) or contact the ITO Service Desk telephonically at (b)(6); (b)(7)(C)

End-users will receive a second email notification reminding them to self-enroll one week prior to the mandatory enrollment date. Once an end-user is enrolled, notification reminders will cease.

Questions regarding mobile device enrollment may be directed to the [ITO Service Desk](#).

Headquarters (Office of the Chief Information Officer) Wilson/Nally

From: KEVIN NALLY (CIO)
To: (b)(6):
Subject: MDM -- InTune Batch Schedule Notification
Date: Wednesday, January 27, 2021 9:59:00 AM

From: CIO <CIO@OFFICIALMAIL.USSS.DHS.GOV>
Sent: Monday, January 25, 2021 3:38 PM
To: USA <usa@OfficialMail.ussd.dhs.gov>
Subject: 145.000 Mobile Device Management Migration

//ROUTINE//

FROM: Office of the Chief Information Officer File: 145.000
TO: All Offices
SUBJECT: Mobile Device Management Migration

Reference is made to the CIO Official Message, dated 1/14/2021, Deployment of iPhone/iPad OneDrive Application.

The Office of the Chief Information Officer (CIO) will begin migrating mobile devices to the Microsoft Intune Mobile Device Management (MDM) System on Wednesday, 1/27/2021. Migration of USSS iPhones and/or iPads will not occur all at once for every device, but through a systematic targeting of individual and pre-designated divisions or offices, in a methodical approach and over the course of several months. Prior to migration, individuals assigned to the specifically targeted divisions or offices for a particular date, will receive the following email communication:

USSS Mobile Device User:

You are receiving this message because your USSS issued iPhone and/or iPad device has been migrated to our new Intune Mobile Device Management (MDM) system. In order to complete this migration, you must enroll your device within this new system.

Enrollment of USSS iPhones and/or iPads in the new MDM system will erase all data on your mobile device to include contacts, iMessages, photographs, notes, and files. Follow the content preservation guide found [here](#) to prevent permanent data loss.

To self-enroll, complete the enrollment steps found [here](#). You will be given two weeks to self-enroll in the new MDM system. If you do not self-enroll within the given timeframe, your iPhone and/or iPad device(s) will be remotely wiped, and the OCIO will initiate the enrollment process automatically.

The CIO recommends that all personnel self-enroll at their earliest convenience once notified. Please plan in allowing 30 minutes for the enrollment process to complete.

If your device fails to enroll, submit a ticket to the [ITO Service Desk](#) or contact the ITO Service Desk telephonically at (b)(6): (b)(7)(C)

End-users will receive a second email notification reminding them to self-enroll one week prior to the mandatory enrollment date. Once an end-user is enrolled, notification reminders will cease.

Questions regarding mobile device enrollment may be directed to the [ITO Service Desk](#).

Below are the proposed batching in groups as the notification dates are fluid depending upon the

rate of success with users self-enrolling.

Every couple of days the metrics will be evaluated, to determine if another office can be added to the notification process, based on how well the migration is being accepted by users to self-enroll. (Keeping it at ~10% of the workforce in the enrollment process)

RTC & WFO begin today, subsequent batches are TENTATIVLY scheduled to start ~4-7 days later – but that’s dependent on how hard the desk gets hit with issue (if any). We can dynamically speed up the notifications if this goes well and users’ ability to self-enroll goes smoothly and at a good pace. Otherwise, we are able to back off and slow (or stop) the process if we see issues.

UD is able to begin now to enroll their folks. They are on their own schedule which (b)(6); (b)(7)(C) will monitor for progress. They have their two IT Specialists who will handle their schedule and keep us apprised. We will monitor their progress on MS InTune.

The 8th Floor can begin when they want to, as (b)(6); could give the white-glove treatment at his leisure to re-enroll devices up there, if you’d like to take that approach. We don’t have to send a notification to them, we can begin with Helder’s and other IT Spec’s assistance now, or we can keep them in the Phase 2 arena which will come at a later date as part of the larger push after we are well into having much of the Agency self-enrolled.

Office	user count	% of Total	Proposed Batch	Note
CIO	(b)(6); (b)(7)(C); (b)(7)(E)	2.4%		Already Done
UDW		9.5%		Will be handled by UD IT
UDO		5.0%		Will be handled by UD IT
UDS		3.4%		Will be handled by UD IT
UDF		2.3%		Will be handled by UD IT
UDV		1.8%		Will be handled by UD IT
RTC		4.4%	1	
WFO		3.8%	1	
NYC		3.0%	2	
PID		2.2%	2	
CID		2.2%	2	
MIA		1.8%	3	
LAX		1.6%	3	
CHI		1.5%	3	
FSD		1.2%	3	
DAL		1.0%	3	
ISD		1.0%	3	
GBD		0.9%	3	
SMD		0.8%	4	
TAD		0.8%	4	
PPD		6.2%	4	
TSD		3.0%	4	
VPD		3.0%	4	

SOD		2.1%	4
CSD		1.3%	4
OPD		1.0%	4
SSD		1.0%	4
HOU		0.8%	4
DPD		0.8%	4
PHL		0.8%	4
ATL		0.8%	4
NWK		0.8%	4
ERO		0.7%	4
WCD		0.7%	4
AOD		0.6%	4
BAL		0.6%	4
IGL		0.6%	4
BOS		0.5%	Phase 2
CLE		0.5%	Phase 2
FMD		0.5%	Phase 2
SFO		0.5%	Phase 2
DET		0.5%	Phase 2
DEN		0.5%	Phase 2
BPR		0.4%	Phase 2
LEG	(b)(6);	0.4%	Phase 2
CLT	(b)(7)(C);	0.4%	Phase 2
INV	(b)(7)(E)	0.4%	Phase 2
PRO		0.4%	Phase 2
CPD		0.4%	Phase 2
OPO		0.4%	Phase 2
ISP		0.4%	Phase 2
LIA		0.3%	Phase 2
OSP		0.3%	Phase 2
TPA		0.3%	Phase 2
JAX		0.3%	Phase 2
BHM		0.3%	Phase 2
CMR		0.3%	Phase 2
HNL		0.3%	Phase 2
ORL		0.3%	Phase 2
SAT		0.3%	Phase 2
SEA		0.3%	Phase 2
RIC		0.3%	Phase 2
LAS		0.3%	Phase 2
SDO		0.3%	Phase 2
HUM		0.3%	Phase 2
LOU		0.3%	Phase 2
PHX		0.3%	Phase 2
PIT		0.3%	Phase 2

CFO	(b)(6); (b)(7)(C); (b)(7)(E)	0.3%	Phase 2
CIN		0.3%	Phase 2
CSC		0.3%	Phase 2
HRR		0.3%	Phase 2
IND		0.2%	Phase 2
LIT		0.2%	Phase 2
KCM		0.2%	Phase 2
MSP		0.2%	Phase 2
NSH		0.2%	Phase 2
STL		0.2%	Phase 2
EES		0.2%	Phase 2
OKC		0.2%	Phase 2
MEM		0.2%	Phase 2
NEO		0.2%	Phase 2
IPD		0.2%	Phase 2
NCF		0.2%	Phase 2
SAF		0.2%	Phase 2
TNG		0.2%	Phase 2
BUF		0.2%	Phase 2
BUD		0.2%	Phase 2
SJU		0.2%	Phase 2
SAV		0.2%	Phase 2
TEC		0.2%	Phase 2
ABQ		0.2%	Phase 2
JAN		0.2%	Phase 2
WPL		0.2%	Phase 2
CLB		0.1%	Phase 2
ERM		0.1%	Phase 2
NHV		0.1%	Phase 2
WPB		0.1%	Phase 2
WPN		0.1%	Phase 2
AUS		0.1%	Phase 2
EAD	0.1%	Phase 2	
ABY	0.1%	Phase 2	
DAY	0.1%	Phase 2	
HRP	0.1%	Phase 2	
JFK	0.1%	Phase 2	
OMA	0.1%	Phase 2	
SII	0.1%	Phase 2	
CHN	0.1%	Phase 2	
CHS	0.1%	Phase 2	
EGE	0.1%	Phase 2	
FTM	0.1%	Phase 2	
KNX	0.1%	Phase 2	
LNG	0.1%	Phase 2	

MIL	(b)(6); (b)(7)(C); (b)(7)(E)	0.1%	Phase 2
NOR		0.1%	Phase 2
POR		0.1%	Phase 2
PRF		0.1%	Phase 2
RAL		0.1%	Phase 2
RIV		0.1%	Phase 2
SPR		0.1%	Phase 2
ATC		0.1%	Phase 2
BRL		0.1%	Phase 2
GRR		0.1%	Phase 2
LEX		0.1%	Phase 2
PAR		0.1%	Phase 2
SAN		0.1%	Phase 2
SLC		0.1%	Phase 2
TOL		0.1%	Phase 2
TUL		0.1%	Phase 2
VEN		0.1%	Phase 2
ESD		0.1%	Phase 2
GSC		0.1%	Phase 2
PRV		0.1%	Phase 2
RES		0.1%	Phase 2
SAC		0.1%	Phase 2
WNC		0.1%	Phase 2
CHA		0.1%	Phase 2
DSM		0.1%	Phase 2
ELP		0.1%	Phase 2
ETP		0.1%	Phase 2
FRE		0.1%	Phase 2
GRN		0.1%	Phase 2
ITG		0.1%	Phase 2
LON		0.1%	Phase 2
MCA		0.1%	Phase 2
MCH	0.1%	Phase 2	
MOB	0.1%	Phase 2	
MON	0.1%	Phase 2	
REN	0.1%	Phase 2	
ROM	0.1%	Phase 2	
SAG	0.1%	Phase 2	
SCR	0.1%	Phase 2	
TAL	0.1%	Phase 2	
TLR	0.1%	Phase 2	
TUS	0.1%	Phase 2	
WAC	0.1%	Phase 2	
WIL	0.1%	Phase 2	
ALB	0.1%	Phase 2	

FRA	(b)(6); (b)(7)(C); (b)(7)(E)	0.1%	Phase 2
LUB		0.1%	Phase 2
PME		0.1%	Phase 2
SJO		0.1%	Phase 2
SPO		0.1%	Phase 2
SYR		0.1%	Phase 2
TRE		0.1%	Phase 2
ECA		0.1%	Phase 2
OTW		0.1%	Phase 2
ROA		0.1%	Phase 2
ROC		0.1%	Phase 2
WIC		0.1%	Phase 2
BAN		0.0%	Phase 2
BCH		0.0%	Phase 2
GUA		0.0%	Phase 2
HAR		0.0%	Phase 2
HBS		0.0%	Phase 2
SMO		0.0%	Phase 2
BIL		0.0%	Phase 2
BOI		0.0%	Phase 2
DIR		0.0%	Phase 2
HGE		0.0%	Phase 2
PRT		0.0%	Phase 2
SOF		0.0%	Phase 2
SOU		0.0%	Phase 2
TLN		0.0%	Phase 2
ANC		0.0%	Phase 2
BOG		0.0%	Phase 2
BRS		0.0%	Phase 2
BUR		0.0%	Phase 2
COO		0.0%	Phase 2
DEP		0.0%	Phase 2
IRM	0.0%	Phase 2	
LIM	0.0%	Phase 2	
MDR	0.0%	Phase 2	
MEX	0.0%	Phase 2	
PAI	0.0%	Phase 2	
VAN	0.0%	Phase 2	
FSN/PAP	0.0%	Phase 2	
HKG	0.0%	Phase 2	
MAD	0.0%	Phase 2	

From: [Intune](#)
To:
Subject: Alert: Intune Migration
Date: Wednesday, January 27, 2021 11:09:33 AM
Importance: High

Good Morning

PLEASE READ THIS ENTIRE MESSAGE BEFORE BEGINNING SELF-ENROLLMENT

You are receiving this message because your USSS issued iPhone and/or iPad device has been migrated to our new Intune Mobile Device Management (MDM) system. In order to complete this migration, you must enroll your device within this new system.

Enrollment of USSS iPhones and/or iPads in the new MDM system will erase all data on your mobile device to include contacts, iMessages, photographs, notes, and files. Follow the content preservation guide found [here](#) to prevent permanent data loss.

There are enrollment steps that require you to be at a USSS blue line connected, or USSS VPN connected PC. To self-enroll, complete the enrollment steps found [here](#). You will be given two weeks to self-enroll in the new MDM system. If you do not self-enroll within the given timeframe, your iPhone and/or iPad device(s) will be remotely wiped, and the OCIO will initiate the enrollment process automatically.

The CIO recommends that all personnel self-enroll at their earliest convenience once notified. Please plan in allowing 30 minutes for the enrollment process to complete.

If your device fails to enroll, [submit a ticket to the ITO Service Desk](#) or contact the ITO Service Desk telephonically at (b)(6); (b)(7)(C)

Regards,

Office of the CIO

From: [Intune](#)
To:
Subject: Final Alert: Intune Migration
Date: Wednesday, February 3, 2021 10:59:33 AM
Importance: High

Good Morning

PLEASE READ THIS ENTIRE MESSAGE BEFORE BEGINNING SELF-ENROLLMENT

You are receiving this message because your USSS issued iPhone and/or iPad device has been migrated to our new Intune Mobile Device Management (MDM) system. In order to complete this migration, you must enroll your device within this new system.

Enrollment of USSS iPhones and/or iPads in the new MDM system will erase all data on your mobile device to include contacts, iMessages, photographs, notes, and files. Follow the content preservation guide found [here](#) to prevent permanent data loss.

There are enrollment steps that require you to be at a USSS blue line connected, or USSS VPN connected PC. To self-enroll, complete the enrollment steps found [here](#). This is your final week to self-enroll in the new MDM system. If you do not self-enroll within the given timeframe, your iPhone and/or iPad device(s) will be remotely wiped, and the OCIO will initiate the enrollment process automatically.

The CIO recommends that all personnel self-enroll at their earliest convenience once notified. Please plan in allowing 30 minutes for the enrollment process to complete.

If your device fails to enroll, [submit a ticket to the ITO Service Desk](#) or contact the ITO Service Desk telephonically (b)(6); (b)(7)(C)

Regards,

Office of the CIO

From: [Intune](#)
To:
Subject: LAST NOTIFICATION BEFORE IPHONE WIPE
Date: Friday, February 12, 2021 9:01:52 PM
Importance: High

Good Evening

PLEASE READ THIS ENTIRE MESSAGE BEFORE BEGINNING SELF-ENROLLMENT

You are receiving this message because your USSS issued iPhone and/or iPad device has been migrated to our new Intune Mobile Device Management (MDM) system. In order to complete this migration, you must enroll your device within this new system.

Enrollment of USSS iPhones and/or iPads in the new MDM system will erase all data on your mobile device to include contacts, iMessages, photographs, notes, and files. Follow the content preservation guide found [here](#) to prevent permanent data loss.

There are enrollment steps that require you to be at a USSS blue line connected, or USSS VPN connected PC. To self-enroll, complete the enrollment steps found [here](#). This is your final week to self-enroll in the new MDM system. If you do not self-enroll by Tuesday, February 16, 2021 at 1000 hours, your iPhone and/or iPad device(s) will be remotely wiped, and the OCIO will initiate the enrollment process automatically.

The CIO recommends that all personnel self-enroll at their earliest convenience once notified. Please plan in allowing 30 minutes for the enrollment process to complete.

If your device fails to enroll, submit a ticket to the [ITO Service Desk](#) or contact the ITO Service Desk telephonically at (b)(6); (b)(7)(C)

Regards,

Office of the CIO

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 11 2022 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

*Do **NOT** start the enrollment process **WITHOUT** being in front of a USSS blue line connected or USSS VPN connected PC. If you do, you will not be able to enroll your device. The only way to complete an enrollment, is if you are at a PC described above. Unfortunately, there is **NOTHING** the OCIO can do to enroll your iPhone/iPad, if you are not at a PC described above. Note: for iPad enrollments, an already enrolled iPhone can be used for the steps where it is described to use a blue line connected or VPN connected PC.*

*Do **NOT** enroll your device while connected to Hotspot. If you do, your enrollment will most likely fail and will have difficulty recovering it to a state that will allow for enrollments to continue on the device.*

*At **NO** point does the instructions below describe entering credentials on the iPhone/iPad, during the enrollment process. If you enter credentials on the enrolling iPhone/iPad during your enrollment, you are doing it wrong and your enrollment will fail.*

Backup

Backup content (if needed). A guide for preserving content for a device that needs wiped / re-enrolled can be found [here](#).

Video

A video of the enrollment process has been created. I strongly recommend that you review this video for the enrollment process. In order to view this video, please connect to the proxy first, by authenticating to www.google.com. Then proceed to the enrollment process video found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up **and are at a USSS blue line connected or USSS VPN connected PC to complete the enrollment process**, wipe your device to enroll in Intune. Go to “*Settings->General->Reset->Erase All Content and Settings*”

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, *immediately followed by an error message regarding “Guided Access”* – **this is expected and occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal. It is best not to let this screen turn off during this process.**

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select **“Sign in”**

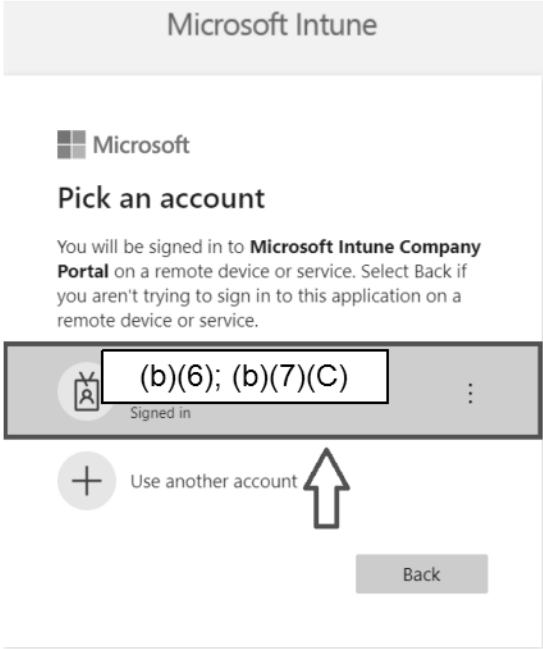
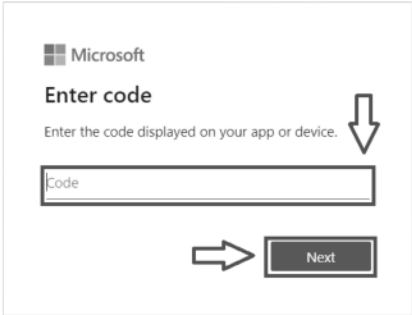
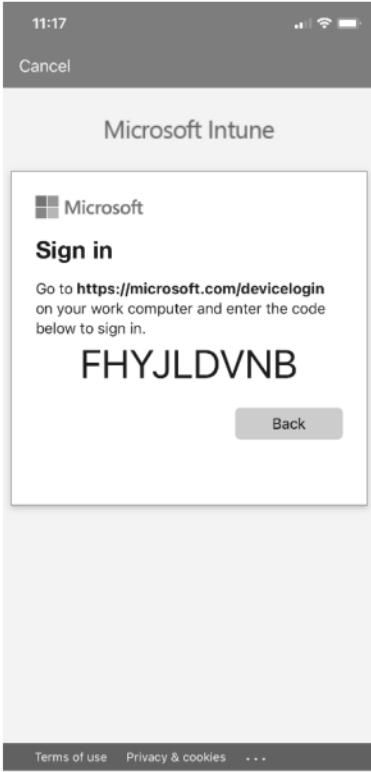
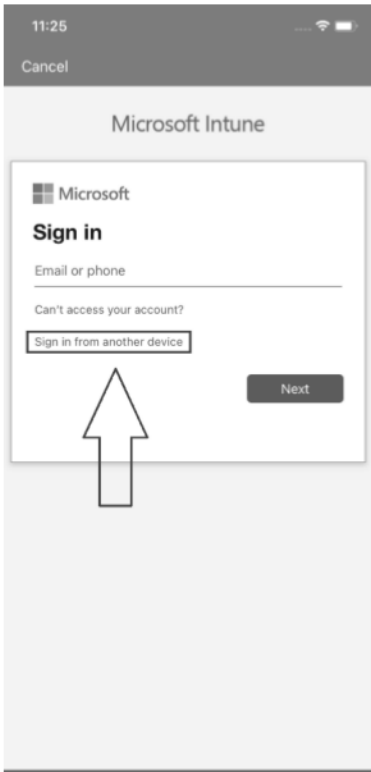
On the iPhone/iPad you are enrolling, **Select “Sign in from another device”**

It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.

On your USSS blue line connected or USSS VPN connected PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step **(This is not case sensitive)**.

On your USSS blue line connected or USSS VPN connected PC, select your @secretservice.gov account. If your account is not listed and it asks for you to type it in, use your Teams address (usually (b)(6); (b)(7)(C) @secretservice.gov)

On your USSS blue line connected or USSS VPN connected PC, select “Sign in as current user”



Enrollment Continued...

On your USSS blue line connected or USSS VPN connected PC, once successful, you will see the below message and will be done with the PC.

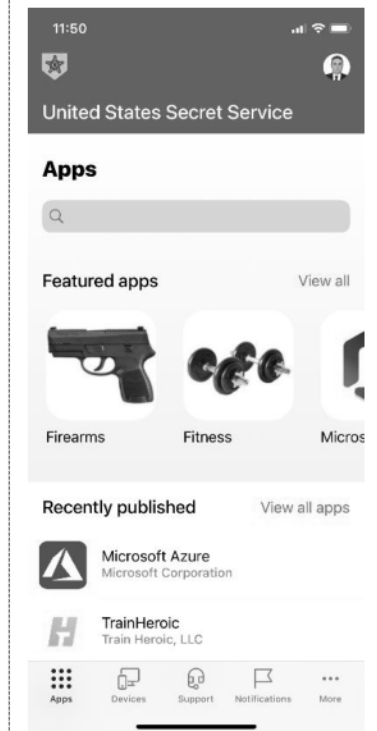
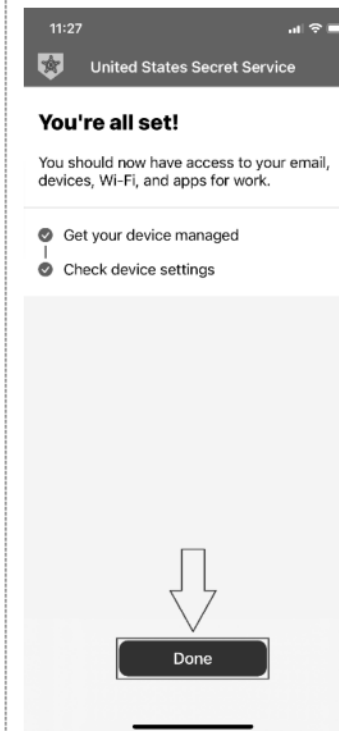
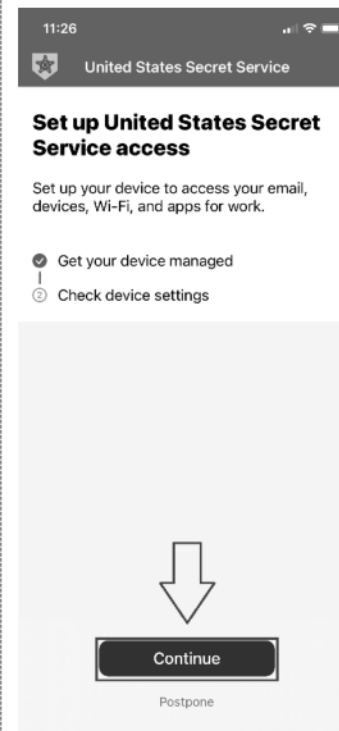
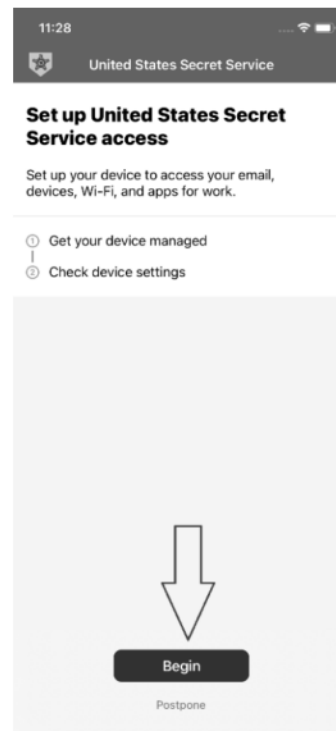
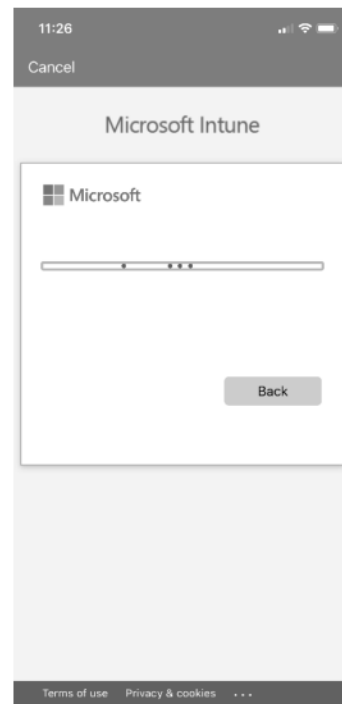
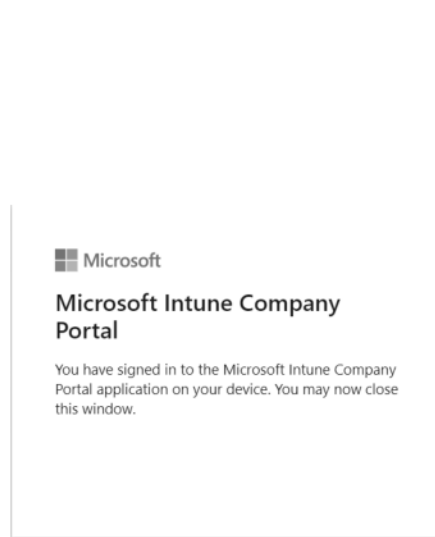
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

iPad Specific

By default iPad web-browser Safari has desktop mode turned on, which can cause some unexpected behavior for some sites.

While Desktop mode is enabled when attempting to access internal USSS sites (e.g. ePerson or Intranet), the user will be presented with a prompt to enter Username & Password. This issue can be resolved by:

Going to Settings > Safari > Request Desktop Website > Toggle OFF "All Websites".

Settings > Safari > Clear History and Website Data.

Try internal USSS site again.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).

- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iOS & iPadOS

Rev. Jan 8 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

Backup

Backup content (if needed). A backup guide can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up, wipe your device to enroll in Intune. Go to “Settings->General->Reset->Erase All Content and Settings”

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a ‘Welcome’ message, immediately followed by an error message regarding “Guided Access” – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select "Sign in"

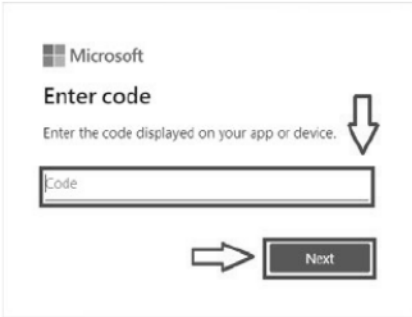
On the iPhone/iPad you are enrolling, **Select "Sign in from another device"**



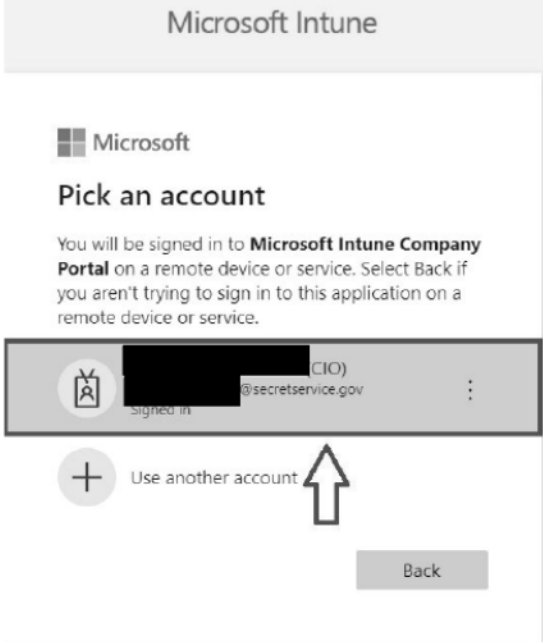
It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.



On your blue line PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step (This is not case sensitive).



Select your @secretservice.gov account. If your account is not listed and it asks for you to type it in, use your Teams address (usually [redacted]@secretservice.gov)



Select "Sign in as current user"



Enrollment Continued...

Once successful, you will see the below message and will be done with the PC.

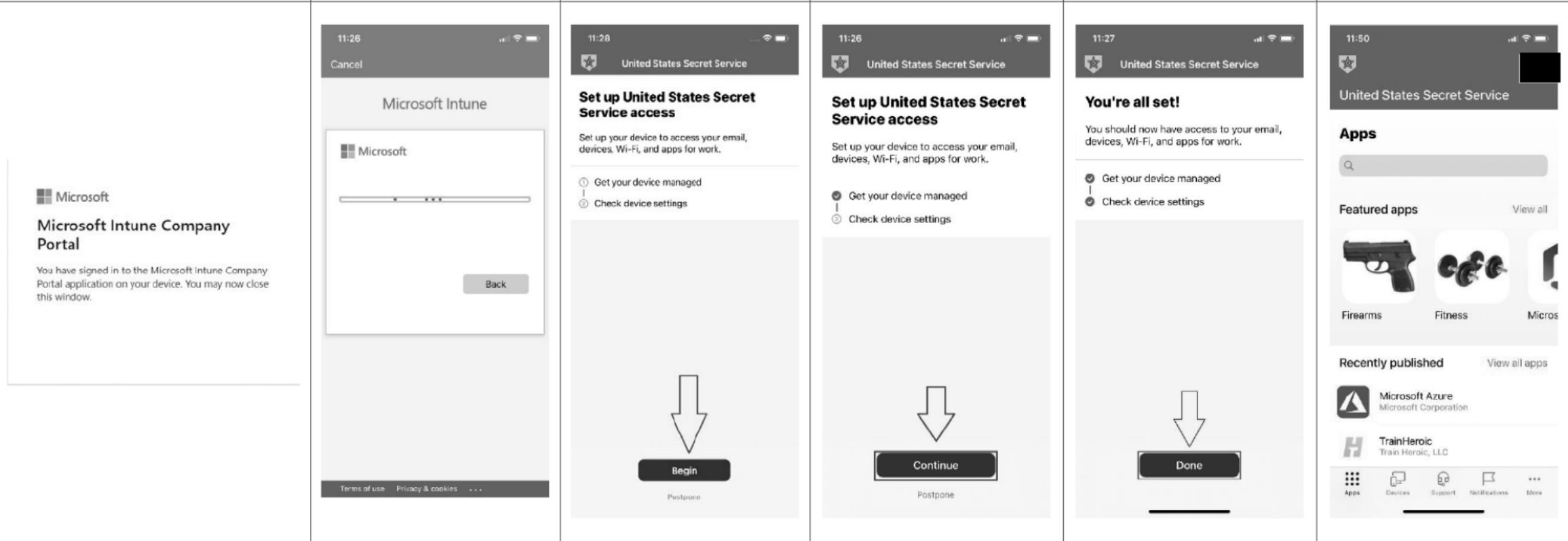
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select Check status and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-enter, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 14 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

Backup

Backup content (if needed). A backup guide can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up **and are near a Blueline device to complete the enrollment process**, wipe your device to enroll in Intune. *Go to "Settings->General->Reset->Erase All Content and Settings"*

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a 'Welcome' message, immediately followed by an error message regarding "Guided Access" – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select "Sign in"

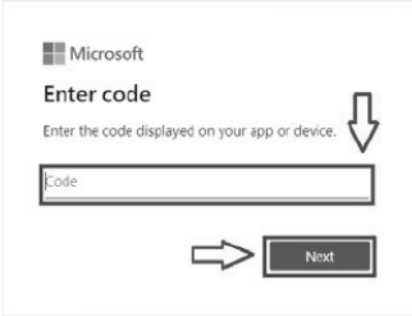
On the iPhone/iPad you are enrolling, **Select "Sign in from another device"**



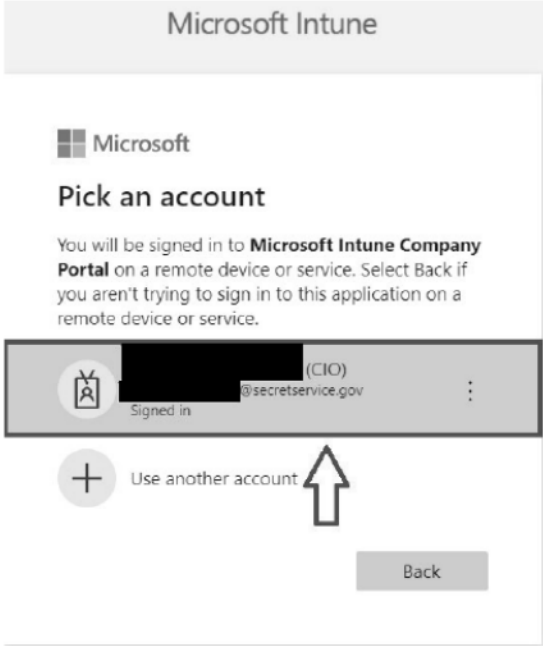
It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.



On your blue line PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step (This is not case sensitive).



Select your @secretservice.gov account. If your account is not listed and it asks for you to type it in, use your Teams address (usually [redacted]@secretservice.gov)



Select "Sign in as current user"



Enrollment Continued...

Once successful, you will see the below message and will be done with the PC.

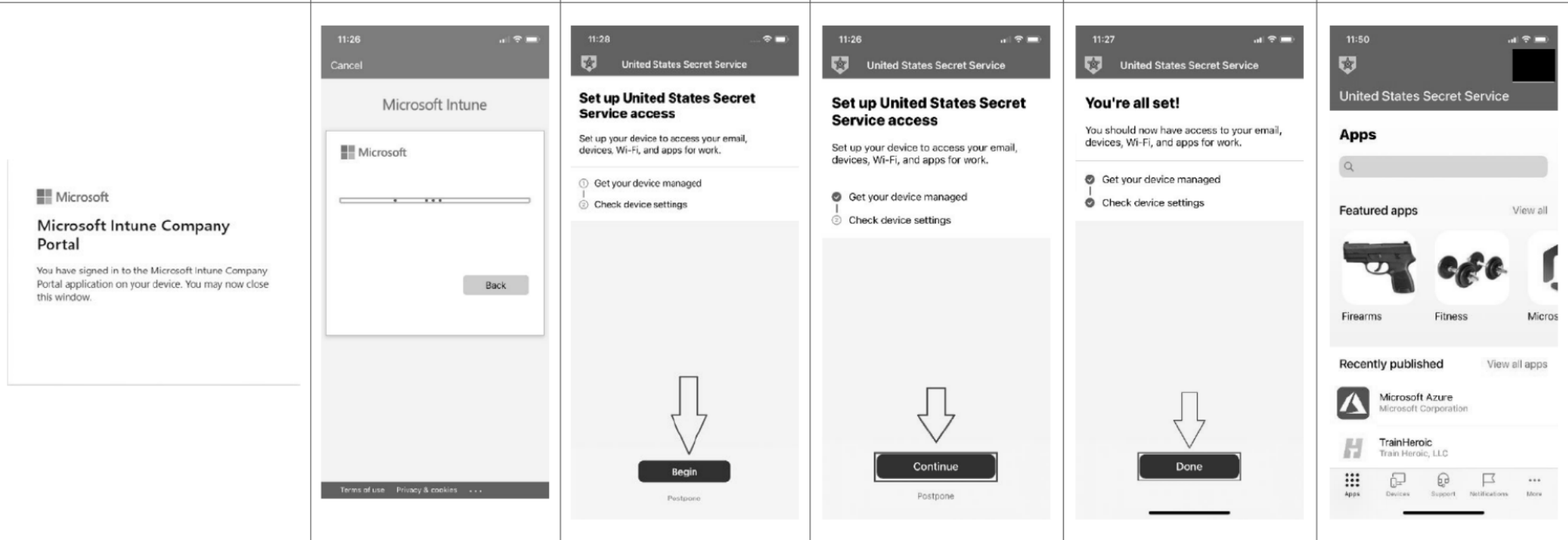
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select Check status and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-enter, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.

USSS Intune Enrollment Quick Start Guide for iPhone & iPad

Rev. Jan 15 2021 RLT

Disclaimer

If you do not follow the steps in this guide correctly, the enrollment of your device will most likely fail and/or functionality such as iMessage will not function.

Backup

Backup content (if needed). A guide for preserving content can be found [here](#).

Enrollment

Once you have confirmed that any content you may need to keep has been backed-up **and are near a Blueline device to complete the enrollment process**, wipe your device to enroll in Intune. *Go to "Settings->General->Reset->Erase All Content and Settings"*

At first Bootup the iOS/iPadOS device goes through the usual Setup Assistant:

- Choose Language
- Choose Country
- Set Up Manually
- Choose Wifi network, or Use Cellular Connection > It may take a few minutes to activate your iPhone/iPad
- Notification of Remote Management (**Select Next**) > Awaiting final configuration
- Terms & Conditions (**Select Agree**)
- iMessage & FaceTime (**Select Continue**)
- Location Service (**Select Enable Location Services**)
- (**Swipe up to get started**)

You will then be prompted with a 'Welcome' message, immediately followed by an error message regarding "Guided Access" – this occurs while the iPhone is downloading the Intune app to continue to the enrollment and is completely normal.

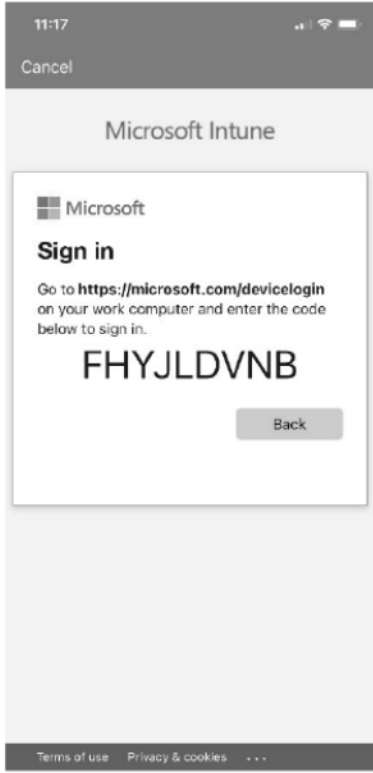
Enrollment Continued...

When Company Portal finishes installing it then auto launches. Select "Sign in"

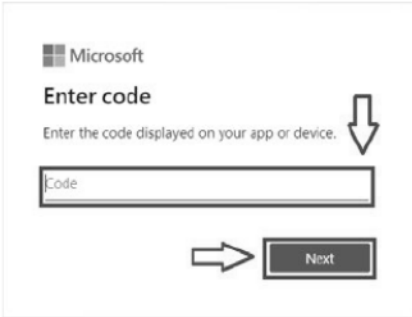
On the iPhone/iPad you are enrolling, **Select "Sign in from another device"**



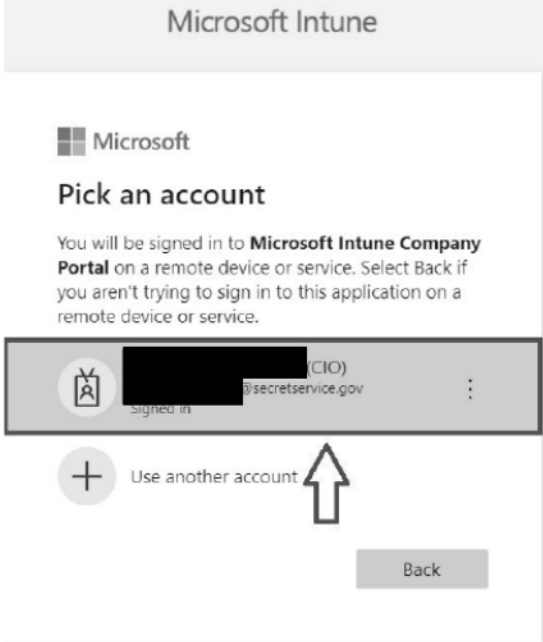
It will then display a website (<https://microsoft.com/devicelogin>) address and 9 digit code.



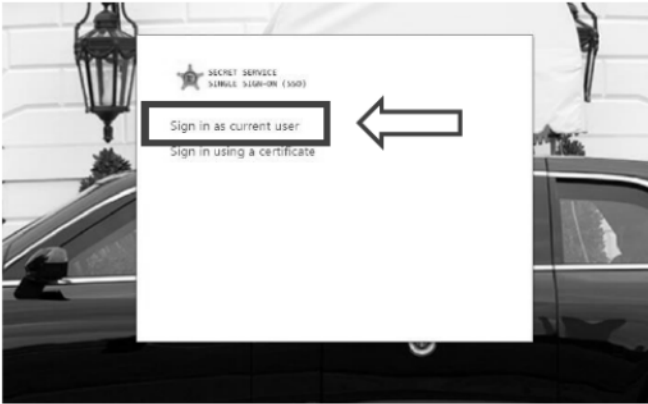
On your blue line PC, go to the website listed in the prior step. Enter the code you see on your phone from the prior step (This is not case sensitive).



Select your @secretservice.gov account. If your account is not listed and it asks for you to type it in, use your Teams address (usually [redacted]@secretservice.gov)



Select "Sign in as current user"



Enrollment Continued...

Once successful, you will see the below message and will be done with the PC.

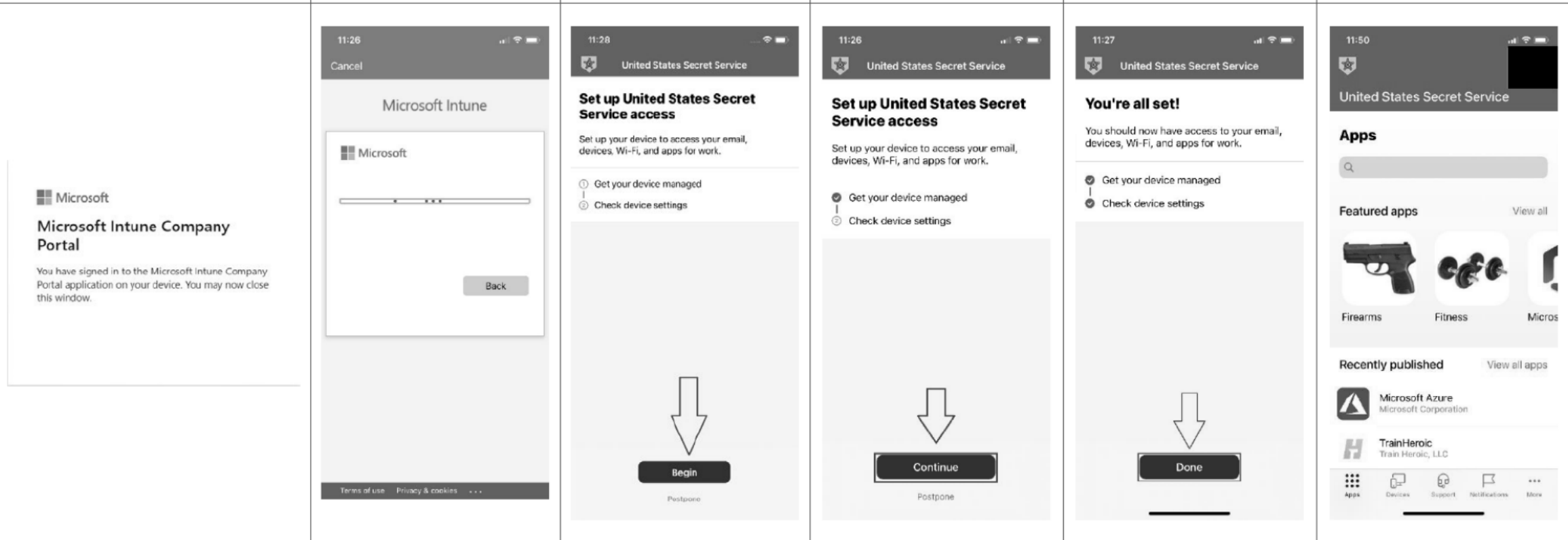
The iPhone will then display the below while moving on to the next steps.

At this step, select "Begin" and wait.

Select "Continue"

Select "Done"

You will then see something like the below.



Once the above is complete, the remaining configuration profiles will begin to be pushed to the device, such as email and apps. You will also be prompted to set a device unlock code.

Note: There is a requirement for the phone to be unlocked for cert/profiles to install. For those that allow their screen to lock during enrollment, you may need to sync from the company portal (check status) to allow for these profiles to finish installing.

Validation

In order to allow for the note mentioned above to complete, please start a validation process

- From the Company Portal app. Select the devices button in lower tray. Select **Check status** and wait for confirmation to complete.
- Check iMessage – Go to Settings > Messages and verify that iMessage is toggled on, otherwise you will need to wipe / re-enroll to enable this feature
- If you have already have set a passcode, check email – Verify you are now receiving email. Otherwise wait a couple of seconds and check status again from Company Portal app.
- Check if you are able to manually connect through the Pulse Secure app. *You may need to close out of the app and re-open, in order to see the connect option.*

FAQs

Where do I download applications?

Company Portal app. There is an option to **view all apps** available for download.

How do I re-enable myServices (eCC) for Authenticator App?

Guidance can be found [here](#).

I forgot my passcode, how can I unlock my device?

From a blueline device, go to the self-service portal [here](#) (you may have to enter or select your @secretsservice.gov credentials). Select options (**3 lines**) in upper left hand corner > Select **Devices** > Select your Device > Select **Reset Passcode**. Note you may have to exit out and go back into the self-service portal to confirm that you want to reset the passcode and see the status of the command. Microsoft Guidance can be found [here](#).

Troubleshoot

- iMessage is not enabled on my iPhone. You most likely didn't select **Continue** to enable iMessage during enrollment. Wipe and re-enroll your device. *Note: iMessage is not enabled on iPads.*
- In rare occasions, the device can get stuck on "Guided Access unavailable, please contact your administrator". Once you have given a significant amount of time for the Company Portal app to install and you have not progressed past this screen, you may need to perform a hard restart. Tap Volume Up > Tap Volume Down > Press and hold the power button until the screen turns dark and the Apple symbol appears (*Ignore Slide to power off*).
- "Company Portal temporarily unavailable" error is usually from someone entering their @secretsservice.gov credentials to attempt signing in via the device they are attempting to enroll vs selecting the "Sign in from another device" (*shown in the first image*).
- Reported email/VPN issues are normally resolved from either performing a device sync (Check Status) within the Company Portal app or Sync command from the Intune Admin Portal (Check Status from the device is usually more effective). This can happen as there is a requirement by Apple for the device to be unlocked in order for profiles to install. To perform a device sync, from the Company Portal select Device > Check Status.